ENCYCLOPEDIA OF
Espionage, Intelligence, and Security

ENCYCLOPEDIA OF
Espionage, Intelligence, and Security

This page intentionally left blank

ENCYCLOPEDIA OF
Espionage, Intelligence, and Security

K. LEE LERNER AND BRENDA WILMOTH LERNER, EDITORS

volume
I
A–E

Detroit • New York • San Diego • San Francisco • Cleveland • New Haven, Conn. • Waterville, Maine • London • Munich

Encyclopedia of Espionage, Intelligence, and Security

K. Lee Lerner and Brenda Wilmoth Lerner, editors

Project Editor
Stephen Cusack

Editorial
Erin Bealmear, Joann Cerrito, Jim Craddock, Miranda Ferrara, Kristin Hart, Melissa Hill, Carol Schwartz, Christine Tomassini, Michael J. Tyrkus, Peter Gareffa

Permissions
Lori Hines

Imaging and Multimedia
Dean Dauphinais, Leitha Etheridge-Sims, Mary K. Grimes, Lezlie Light, Luke Rademacher

Product Design
Kate Scheible

Manufacturing
Rhonda Williams

For more information, contact
The Gale Group, Inc.
27500 Drake Rd.
Farmington Hills, MI 48331-3535
Or you can visit our Internet site at http://www.gale.com

Cover Photos

Volume 1: Ethel and Julius Rosenberg following arraignment on charges of espionage, August 23, 1950. ©Bettmann/Corbis

Volume 2: SR-71 Blackbird, c. 1991. ©Corbis

Volume 3: Clean-up crews scour the American Media Inc. building in Boca Raton, Florida, after the discovery of anthrax spores, October 9, 2001. AP/Wide World Photos.

Library of Congress Cataloging-in-Publication Data

Encyclopedia of espionage, intelligence, and security / K. Lee Lerner and Brenda Wilmoth Lerner, editors.
p. cm.
Includes bibliographical references and index.
ISBN 0-7876-7546-6 (set : hardcover : alk. paper) — ISBN 0-7876-7686-1 (v. 1) — ISBN 0-7876-7687-X (v. 2) — ISBN 0-7876-7688-8 (v. 3)
1. Espionage—Encyclopedias. 2. Intelligence service—Encyclopedias. 3. Security systems—Encyclopedias. I. Lerner, K. Lee. II. Lerner, Brenda Wilmoth.
JF1525.I6E63 2004
327.12'03—dc21

2003011097

This title is available as an e-book.
ISBN 0-7876-7762-0

Contact your Gale sales representative for ordering information.

Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

Contents

This page intentionally left blank

Introduction

In composing *The Encyclopedia of Espionage, Intelligence, and Security (EEIS),* our goal was to shape a modern encyclopedia offering immediate value to our intended readers by emphasizing matters of espionage, intelligence, and security most frequently in the news.

EEIS is not intended as a classical "spy book," filled with tales of daring operations. Instead, within a framework of historical overviews, *EEIS* emphasizes the scientific foundations, applications of technology, and organizational structure of modern espionage, intelligence, and security. High school and early undergraduate students can use this book to expand upon their developing awareness of the fundamentals of science, mathematics, and government as they begin the serious study of contemporary issues.

EEIS is also intended to serve more advanced readers as a valuable quick reference and as a foundation for advanced study of current events.

EEIS devotes an extensive number of articles to agencies and strategies involved in emerging concepts of homeland security in the United States. Faced with a daunting amount of information provided by agencies, organizations, and institutes seeking to put their best foot forward, we have attempted to allocate space to the topics comprising *EEIS* based upon their relevance to some unique facet of espionage, intelligence, or security—especially with regard to science and technology issues—as opposed to awarding space related to power of the agency or availability of material.

A fundamental understanding of science allows citizens to discern hype and disregard hysteria, especially with regard to privacy issues. Spy satellites powerful enough to read the details of license plates do so at peril of missing events a few steps away. With regard to electronic intercepts, the capability to identify what to carefully examine—often a decision driven by mathematical analysis—has become as essential as the capacity to gather the intelligence itself. Somewhere between the scrutiny of Big Brother and the deliberately blind eye lie the shadows into which terrorists often slip.

With an emphasis on the realistic possibilities and limitations of science, we hope that *EEIS* finds a useful and unique place on the reference shelf.

It seems inevitable that within the first half of the twenty-first century, biological weapons may eclipse nuclear and chemical weapons in terms of potential threats to civilization. Because informed and reasoned public policy debates on issues of biological warfare and bioterrorism can only take place when there is a fundamental understanding of the science underpinning competing arguments, *EEIS* places special emphasis on the multifaceted influence and applications of the biological sciences and emerging biometric technologies. Future generations of effective intelligence and law enforcement officers seeking to thwart the threats posed by tyrants, terrorists, and the technologies of mass destruction might be required to be as knowledgeable in the terminology of epidemiology as they are with the tradecraft of espionage.

Knowledge is power. In a time where news can overwhelm and in fact, too easily mingle with opinion, it is our hope that *EEIS* will provide readers with greater insight to measure vulnerability and risks, and correspondingly, an increased ability to make informed judgments concerning the potential benefits and costs of espionage, intelligence, and security matters.

K. LEE LERNER & BRENDA WILMOTH LERNER, EDITORS
CORNWALL, U.K.
MAY, 2003

How to Use the Book

The *Encyclopedia of Espionage, Intelligence, and Security* was not intended to contain a compendium of weapons systems. Although *EEIS* carries brief overviews of specifically selected systems commonly used in modern intelligence operations, readers interested in detailed information regarding weapons systems are recommended

to *Jane's Strategic Weapon Systems*, or *Jane's Defense Equipment Library*.

Although *EEIS* contains overview of significant historical periods and events, for those readers interested in additional information regarding the history of espionage operations and biographies of intelligence personnel, the editors recommend Jeffrey T. Richelson's *A Century of Spies : Intelligence in the Twentieth Century* (Oxford University Press, 1995), Vincent Buranelli and Nan Buranelli's *Spy/Counterspy: An Encyclopedia of Espionage* (New York: McGraw-Hill, 1982), and Allen Dulles', *The Craft of Intelligence* (New York: Harper & Row, 1963).

The articles in *EEIS* are meant to be understandable by anyone with a curiosity about topics in espionage, intelligence, and security matters, and this first edition of the book has been designed with ready reference in mind:

- Entries are arranged alphabetically. In an effort to facilitate easy use of this encyclopedia, and to attempt order in a chaotic universe of names and acronyms the editors have adopted a "common use" approach. Where an agency, organization, or program is known best by its acronym, the entry related to that organization will be listed by the acronym (e.g. FEMA is used instead of Federal Emergency Management Agency). To facilitate use, the editors have included a number of "jumps" or cross-referenced titles that will guide readers to desired entries.
- To avoid a log jam of terms starting with "Federal" and "United States," titles were broken to most accurately reflect the content emphasized or subject of agency authority.
- **"See Also" references** at the end of entries alert the readers to related entries not specifically mentioned in the body of the text that may provide additional or interesting resource material.
- An extensive **Glossary** of terms and acronyms is included to help the reader navigate the technical information found in *EEIS*.
- The **Chronology** includes significant events related to the content of the encyclopedia. Often accompanied by brief explanations, the most current entries date represent events that occurred just as *EEIS* went to press.
- A **Sources** section lists the most worthwhile print material and web sites we encountered in the compilation of this volume. It is there for the inspired reader who wants more information on the people and discoveries covered in this volume.
- A comprehensive general **Index** guides the reader to topics and persons mentioned in the book. Bolded page references refer the reader to the term's full entry.
- The editors and authors have attempted to explain scientific concepts clearly and simply, without sacrificing fundamental accuracy. Accordingly, an advanced understanding of physics, chemistry, or biochemistry is not assumed or required. Students and other readers should not, for example, be intimidated or deterred by the complex names of biochemical molecules—where necessary for complete understanding, sufficient information regarding scientific terms is provided.
- To the greatest extent possible we have attempted to use Arabic names instead of their Latinized versions. Where required for clarity we have included Latinized names in parentheses after the Arabic version. Alas, we could not retain some diacritical marks (e.g. bars over vowels, dots under consonants). Because there is no generally accepted rule or consensus regarding the format of translated Arabic names, we have adopted the straightforward, and we hope sensitive, policy of using names as they are used or cited in their region of origin.
- EEIS relies on open source material and no classified or potentially dangerous information is included. Articles have been specifically edited to remove potential "how to" information. All articles have been prepared and reviewed by experts who were tasked with ensuring accuracy, appropriateness, and accessibility of language.
- With regard to entries regarding terrorist organizations, *EEIS* faced a serious dilemma. For obvious reasons, it was difficult to obtain balanced, impartial, and independently verifiable information regarding these organizations, nor could *EEIS* swell to incorporate lengthy scholarly analysis and counter-analysis of these organizations without losing focus on science and technology issues. As a compromise intended to serve students and readers seeking initial reference materials related to organizations often in the news, *EEIS* incorporates a series of supplemental articles to convey the information contained in the U.S. Department of State annual report to Congress titled, *Patterns of Global Terrorism,* 2001. These articles contain the language, assertions of fact, and views of the U.S. Department of State. Readers are encouraged to seek additional information from current U.S. Department of State resources and independent non-governmental scholarly publications that deal with the myriad of issues surrounding the nature and activities of alleged terrorist organizations. A number of governmental and non-governmental publications that deal with these issues are cited in the bibliographic sources section located near the index.

Key *EEIS* articles are signed by their authors. Brief entries were compiled by experienced researchers and reviewed by experts. In the spirit of numerous independent scientific watchdog groups, during the preparation of *EEIS* no contributors held a declared affiliation with any intelligence or security organization. This editorial policy not only allowed a positive vetting of contributors, but also assured an independence of perspective and an emphasis on the fundamentals of science as opposed to unconfirmable "insider" information.

When the only verifiable or attributable source of information for an entry comes from documents or information provided by a governmental organization (e.g., the U.S. Department of State), the editors endeavored to carefully note when the language used and perspective offered was that of the governmental organization.

Although some research contributors requested anonymity, no pseudonyms are used herein.

Acknowledgments

The editors wish to thank Herbert Romerstein, former USIA Soviet Disinformation Officer and Coordinator of Programs to Counter Soviet Active Measures, United States Information Agency, for his assistance in compiling selected articles.

The editors wish to thank Lee Wilmoth Lerner for his assistance in compiling technical engineering data for inclusion in EEIS.

The editors acknowledge the assistance of the members of the Federation of American Scientists for the provision of reports and materials used in the preparation of selected articles.

Although certainly not on the scale of the challenge to provide security for a nation with approximately 85 deep-draft ports, 600,000 bridges, 55,000 independent water treatment systems, 100 nuclear power plants, and countless miles of tunnels, pipelines, and electrical and communications infrastructure, the task of incorporating changes brought on by creation of the Department of Homeland Security—and the most massive reorganization of the United States government since World War II—as this book went to press provided a unique challenge to *EEIS* writers and advisors. The editors appreciate their dedication and willingness to scrap copy, roll up their sleeves, and tackle anew the smorgasbord of name and terminology changes.

As publishing deadlines loomed, EEIS was also well served by a research staff dedicated to incorporating the latest relevant events—especially information related to the search for weapons of mass destruction—that took place during war in Iraq in March and April of 2003.

EEIS advisors, researchers, and writers tenaciously attempted to incorporate the most current information available as *EEIS* went to press. The editors pass any credit or marks for success in that effort, and reserve for themselves full responsibility for omissions.

The editors gratefully acknowledge the assistance of many at St. James Press for their help in preparing *The Encyclopedia of Espionage, Intelligence, and Security*. The editors extend thanks to Mr. Peter Gareffa and Ms. Meggin Condino for their faith in this project. Most directly, the editors wish to acknowledge and thank the project editor, Mr. Stephen Cusack, for his talented oversight and for his tireless quest for secure engaging pictures for *EEIS*.

The editors lovingly dedicate this book to the memory of Wallace Schaffer, Jr., HM3, USNR, who died on January 8, 1968, in Thua Thien (Hue) Province, Vietnam.

"A small rock holds back a great wave."—Homer, *The Odyssey*.

This page intentionally left blank

Advisors and Contributors

Julie Berwald, Ph.D.
Geophysicist, writer on marine science, environmental biology, and issues in geophysics.
Austin, Texas

Robert G. Best, Ph.D.
Clinical cytogeneticist and medical geneticist who has written on a range of bioscience issues
Director, Division of Genetics
University of South Carolina School of Medicine

Tim Borden, Ph.D.
Doctorate in History from Indiana University, and is an inspector with the U.S. Bureau of Customs and Border Protection
Toledo, Ohio

Brian Cobb, Ph.D.
Bioscience writer, researcher
Institute for Molecular and Human Genetics
Georgetown University, Washington, D.C.

Cecilia Colomé, Ph.D.
Astrophysicist, translator, and science writer
Austin, Texas

Laurie Duncan, Ph.D.
Geologist, science writer, and researcher
Austin, Texas

William J. Engle, P.E.
Writer on contemporary geophysics issues and the impacts of science and technology on history
Exxon-Mobil Oil Corporation (Rt.) New Orleans, Louisiana

Antonio Farina, M.D., Ph.D.
Physician, researcher, and writer on medical science issues
Assistant Professor, University of Bologna, Italy

Christopher T. Fisher, Ph.D.
Assistant Professor, Department of African American Studies and the Department of History
The College of New Jersey, Ewing, New Jersey

Larry Gilman, Ph.D.
Electrical engineer and science writer
Sharon, Vermont

William Haneberg, Ph.D.
Former research scientist and professor, now an independent consulting geologist and science writer
Portland, Oregon

Brian D. Hoyle, Ph.D.
Science writer and Chief Microbiologist, Government of New Brunswick from 1993 to 1997
Nova Scotia, Canada

Joseph Patterson Hyder
Writer on the historical impacts of science and technology
University of Tennessee College of Law, Knoxville, Tennessee

Alexandr Ioffe, Ph.D.
Writer on the history of science and researcher with the Geological Institute of Russian Academy of Sciences in Moscow
Russian Academy of Sciences, Moscow

Judson Knight
Science writer, researcher, and editor
Knight Agency Research Services, Atlanta, Georgia

Michael Lambert, Ph.D.
Researcher at the Great Plains/Rocky Mountain Hazardous Substance Research Center and at the U.S. Naval Research Laboratory
Manhattan, Kansas

Adrienne Wilmoth Lerner
Writer of various articles on the history of science, archaeology, and the evolution of security-related law
University of Tennessee College of Law, Knoxville, Tennessee

Agnes Lichanska, Ph.D.
Science writer who has conducted research at the Department of Medical Genetics and Ophthalmology at Queen's University of Belfast (Northern Ireland)
University of Queensland, Brisbane, Australia

Eric v.d. Luft, Ph.D., M.L.S.
Writer on cultural, scientific, and intellectual history, and philosophy
Curator of Historical Collections
SUNY Upstate Medical University, Syracuse, New York

Martin Manning
Served on the Economic Security Team, Office of International Information Programs, U.S. Department of State
Bureau of Public Diplomacy
U.S. Department of State, Washington, D.C.

Kelli Miller
Served as news writer and producer for Inside Science *TV News at the American Institute of Physics (AIP) and as executive producer of* Discoveries & Breakthroughs Inside Science
Atlanta, Georgia

Caryn E. Neumann
Instructor and doctoral candidate in the Department of History at Ohio State University
Columbus, Ohio

Mike O'Neal, Ph.D.
Independent scholar and writer
Moscow, Idaho

Belinda M. Rowland, Ph.D.
Science and medical writer
Voorheesville, New York

Judyth Sassoon, Ph.D., ARCS
Science writer with research experience in NMR and X-ray crystallography techniques
Department of Biology & Biochemistry
University of Bath, United Kingdom

Morgan Simpson
Aerospace Engineer
National Aeronautical and Space Administration (NASA)
Kennedy Space Center, Cape Canaveral, Florida

Constance K. Stein, Ph.D.
Writer on medical and bioscience issues related to modern genetics
Director of Cytogenetics, Assistant Director of Molecular Diagnostics
SUNY Upstate Medical University, Syracuse, New York

Tabitha Sparks, Ph.D.
Marion L. Brittain fellow, Georgia Institute of Technology and Fellow, Center for Humanistic Inquiry, Emory University
Atlanta, Georgia

David Tulloch
Science and technology writer
Wellington, New Zealand

Michael T. Van Dyke, Ph.D.
Served as visiting assistant professor, Department of American Thought & Language
Michigan State University, East Lansing, Michigan

Stephanie Watson
Science writer specializing in the social impacts of science and technology
Smyrna, Georgia

Simon Wendt, Ph.D.
Ph.D. candidate in Modern History and History instructor
John F. Kennedy Institute for North American Studies, Free University of Berlin, Germany

List of Entries

A

B

C

D

E

F

G

H

I

IJI

IKI

ILI

IMI

N

O

P

Q

R

S

T

U

V

W

Z

This page intentionally left blank

A

Abu Nidal Organization (ANO)

Abu Nidal Organization (ANO) is identified by the United States Department of State as an international terrorist organization led by Sabri al-Banna. Split from the Palestine Liberation Army (PLO) in 1974, the ANO is comprised of various functional committees, including political, military, and financial committees.

The Abu Nidal Organization (ANO) also operates as, or is known as; Fatah Revolutionary Council, Arab Revolutionary Brigades, Black September, and Revolutionary Organization of Socialist Muslims.

Organization activities. The ANO has carried out terrorist attacks in 20 countries, killing or injuring almost 900 persons. Targets have included the United States, the United Kingdom, France, Israel, moderate Palestinians, the PLO, and various Arab countries. Major attacks included the Rome and Vienna airports in December 1985, the Neve Shalom synagogue in Istanbul, and the Pan Am Flight 73 hijacking in Karachi in September 1986, along with the City of Poros day-excursion ship attack in Greece in July, 1988. The ANO is suspected of assassinating PLO deputy chief Abu Iyad and PLO security chief Abu Hul in Tunis in January, 1991. ANO assassinated a Jordanian diplomat in Lebanon in January, 1994, and has been linked to the killing of the PLO representative there. As of May 2002, the ANO has not attacked Western targets since the late 1980s. ANO leader Abu Nidal was found dead in Baghdad, Iraq in August 2002. Following Nidal's death and subsequent disruption of ANO by Operation Iraqi Freedom in 2003, the fate of the organization remained uncertain.

Membership in the ANO is estimated at a few hundred plus a limited overseas support structure. Al-Banna relocated to Iraq in December 1998, where the group maintains a presence. ANO has had an operational presence in Lebanon including in several Palestinian refugee camps. Financial problems and internal disorganization have reduced the group's activities and capabilities. Authorities shut down the ANO's operations in Libya and Egypt in 1999. The ANO has demonstrated ability to operate over wide areas, including the Middle East, Asia, and Europe. They have also received considerable support, including safe haven, training, logistic assistance, and financial aid from Iraq, Libya, and Syria (until 1987), in addition to close support for selected operations.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Abu Sayyaf Group (ASG)

The Abu Sayyaf Group (ASG) is the most violent of the Islamic separatist groups operating in the southern Philippines. Some ASG leaders have studied or worked in the Middle East and reportedly fought in Afghanistan during the Soviet war. The group split from the Moro National Liberation Front in the early 1990s under the leadership of

Abdurajak Abubakar Janjalani, who was killed in a clash with Philippine police on 18 December, 1998. His younger brother, Khadaffy Janjalani, has replaced him as the nominal leader of the group, which is composed of several semi-autonomous factions.

Organization activities. The ASG engages in kidnappings for ransom, bombings, assassinations, and extortion. Although from time to time it claims that its motivation is to promote an independent Islamic state in western Mindanao and the Sulu Archipelago, areas in the southern Philippines heavily populated by Muslims, the ASG now appears to use terror mainly for financial profit. The group's first large-scale action was a raid on the town of Ipil in Mindanao in April 1995. In April of 2000, an ASG faction kidnapped 21 persons, including 10 foreign tourists, from a resort in Malaysia. Separately in 2000, the group abducted several foreign journalists, three Malaysians, and a United States citizen. On 27 May 2001, the ASG kidnapped three U.S. citizens and 17 Filipinos from a tourist resort in Palawan, Philippines. Several of the hostages, including one U.S. citizen, were murdered.

A few hundred ASG fighters make up the core group, but at least 1000 individuals motivated by the prospect of receiving ransom payments for foreign hostages allegedly joined the group in 2000–2001.

The ASG was founded in Basilan Province, and mainly operates there and in the neighboring provinces of Sulu and Tawi-Tawi in the Sulu Archipelago. It also operates in the Zamboanga peninsula, and members occasionally travel to Manila and other parts of the country. The group expanded its operations to Malaysia in 2000 when it abducted foreigners from a tourist resort.

The ASG is largely self-financed through ransom and extortion, but they may also receive support from Islamic extremists in the Middle East and South Asia. Libya publicly paid millions of dollars for the release of the foreign hostages seized from Malaysia in 2000.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Abwehr

■ ADRIENNE WILMOTH LERNER

The Abwehr was the German military intelligence organization from 1866 to 1944. The organization predates the emergence of Germany itself, and was founded to gather intelligence information for the Prussian government during a war with neighboring Austria. After initial successes, the organization was expanded during the Franco-Prussian War in 1870. Under the direction of Wilhelm Stieber, Abwehr located, infiltrated, and reported on French defensive positions and operations. The Prussians claimed victory, largely because of the success of Abwehr agents. In 1871, Prussia united with other independent German states to form the nation of Germany. The new country adopted much of the former Prussian government and military structure, including the Abwehr.

The intelligence agency was again tested at the outbreak of World War I in 1914. German agents worked to pinpoint the location and strength of the Allied forces, helping the German forces to invade and progress through northern France before stalemated trench warfare began. New military technology changed the nature of espionage. Agency director Walther Nicolai recognized the need for a modernized intelligence force and reorganized the department to include experts in wire tapping, munitions manufacturing, shipping, and encryption. The agency tapped enemy communications wires, intercepting and deciphering Allied dispatches with measured accomplishment. The Abwehr sent several agents to spy on the manufacture of poison gas in France, and tracked munitions production and shipping in Britain. The organization sent saboteurs to disrupt the shipment of arms from America to Allied forces in Europe. Several ships were sunk in transit after being identified by agents as smuggling arms. German agents, often acting on information collected by Abwehr, set fire to several American weapons factories and storage facilities. While the Abwehr was generally successful, the loss of the German codebook to British intelligence somewhat undermined the agency's ultimate efficacy during the war.

After World War I, the Abwehr ceased operation under the terms of the Versailles Treaty. The intelligence service was re-established in 1921. When the Nazis gained control of Germany in the 1930s, some members of the intelligence agency began to spy on their own government. The Nazis created a separate intelligence organization, the *Sicherheitsdienst*, or Security Service, headed by Reinhard Heydrich. In 1935, the new Abwehr director, Wilhelm Canaris, and Heydrich reached an agreement about the roles of each agency, but both trained and maintained their own espionage forces. Canaris reorganized the Abwehr into three branches: espionage, counter-espionage, and saboteurs. He appointed three distinguished Abwehr agents to lead the branches, but only on condition that they were not members of the Nazi party.

This aroused the suspicion of rival Security Service. The two agencies came into conflict on several occasions, and as Heydrich gained power, he persuaded the government to investigate members of the Abwehr for espionage and treason. Several members of the Abwehr were arrested in 1939. Though a handful of the agency's highest ranking officials were active as double-agents or as members of the Resistance, the organization as a whole continued its espionage operations on behalf of the German government.

At the outbreak of World War II, Abwehr resumed operations similar to those carried out during World War I. The agency was in charge of tracking troops and munitions transports, tapping wires and intercepting radio messages, and infiltrating foreign intelligence and military units. Abwehr placed two operatives inside the British intelligence agency for two years, and developed a highly successful encryption device called the Enigma machine. Agents tracked and monitored various resistance movements in occupied Europe, and even sabotaged military and government strongholds behind Allied lines.

Canaris made the United States one of Abwehr's primary targets even before America's entry into the conflict. By 1942, German agents were operating from within all of America's top armaments manufacturers. Abwehr scored perhaps its greatest victories in the area of industrial espionage, as agents managed to steal the blueprint for every major American airplane produced for the war effort.

One of the Abwehr's responsibilities during World War II was the extraction of information from prisoners of war. While Abwehr agents remained largely in control of seeking strategic information from British, French, and American prisoners, the Nazi government issued a special directive to various branches of the military regarding Russian prisoners of war. The Commissar Order, as it became known, instructed the Army to handle Russian prisoners as harshly as they deemed necessary for the retrieval of military information. At one time, German concentration camps held more that 1.5 million Russian prisoners. Canaris himself raised several objections to this policy, largely on the grounds that it undermined the authority and efficacy of his agency and could cripple the German war effort.

In 1944, Heinrich Himmler, head of the Gestapo, the Nazi secret police, assumed control of Abwehr after an unsuccessful assassination attempt on Adolf Hitler and several other high ranking Nazi officials. Himmler suspected that the plot was the work of agents inside the government, most especially the Abwehr. The July Plot also exposed the work of those Abwehr agents who had intentionally leaked sensitive information to the Allies. Several agents, including Canaris, were charged with treason and executed. The Abwehr was then dissolved.

SEE ALSO

Bletchley Park
Cipher Machines
Germany, Intelligence and Security
World War I: Loss of the German Codebook

Accelerated Strategic Computing Initiative (ASCI).

SEE *Lawrence Livermore National Laboratory (LLNL).*

Achille Lauro.

SEE *Palestine Liberation Front (PLF).*

Acoustic Bullets.

SEE *Audio Amplifiers.*

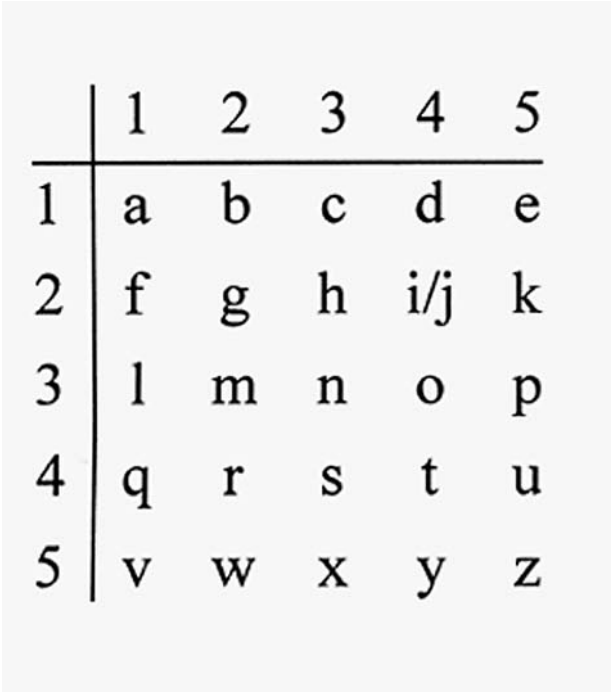
ADFGX Cipher

JUDSON KNIGHT

The ADFGX cipher, sometimes referred to as the ADFGVX cipher, is one of the most famous codes in the entire history of cryptography. Introduced by the Germans in World War I, it is based on an ancient idea of associating letters with positions on a grid. Variations on the code have made communication possible across the walls of prison cells, and further intricacies added through the technique of transposition have made the code unbreakable without the aid of a computer.

Greek historian Polybius (fl.c. 200 B.C.) introduced what became known as the Polybius square, a 5 x 5 grid that used the 24 letters of the Greek alphabet. Each letter had a unique position identifiable by a coordinate system that numbered the rows and columns. For example, *A* was one column to the right of the point of origin, and one row down, so its coordinate would be 11. In the English alphabet, two letters are combined in a single square so that the 26 letters fit into the 25-square grid. Supposing *I* and *J* are combined, then *K* would be at position 25—two rows down, and five squares over.

Over the centuries that followed, the Polybius square made possible a system of taps or knocks whereby prisoners could pass messages to one another across walls. Applied by groups ranging from Russian anarchists to American prisoners of war in Vietnam, the system has been described by writers as diverse as Arthur Koestler in *Darkness at Noon,* Aleksandr Solzhenitsyn in *The Gulag*



	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

A polybius cipher square showing a grid that assigns a code number to each letter of the alphabet. In this square, for example, the letter M would be coded as number 32.

Archipelago, and Senator John S. McCain in *Faith of Our Fathers.* It has undergone countless variations based on the needs of the users—for example, a 6 x 6 grid for the 33 letters of the Russian alphabet—but the basic principle remains the same. According to the English-language grid described earlier, for instance, *K* would be rendered by two rapid knocks or taps, a short break, and then five rapid knocks or taps.

The ADFGX Cipher in World War I. The ADFGX cipher, developed by German army radio officer Fritz Nebel (1891–1967), made its appearance on March 5, 1918, when the Germans used it in a wireless transmission on the western front. Instead of the numerals 1 through 5 along a side of the Polybius square, Nebel's cipher applied the letters *A, D, F, G,* and *X,* which he chose because their equivalents in Morse code were so dissimilar that confusion was unlikely. (For example, *A* is one dot and two dashes, while *D* is one dash and two dots.) Three months later, on June 1, the German army added the letter *V* to make a sixth row and column. The 6 x 6 grid of the ADFGVX cipher allowed the inclusion of the 10 numerals from 0 to 9, like its predecessor.

The brilliance of the ADFGX cipher lay in the fact that, unlike ordinary codes, the frequency of letters such as *E* was not easy to recognize. Furthermore, the code could become even more challenging by applying a system of transposition. Suppose a message is written out in ADFGVX format—that is, as a series of two-letter combinations using just those six letters. That string of letters is then placed in a matrix under the letters of a chosen keyword, such as *KAISER,* which an army in wartime would typically change every day, Then the letters of the keyword are placed in alphabetical order—in this case, spelling *AEIKRS,* with the corresponding columns moved as well. After being transposed in this manner, the message is transcribed by reading down along each column, making it impossible for anyone who does not know the keyword to translate the message.

A modern computer would be capable of unscrambling such a transmission, even in a situation involving an unknown keyword, but the Allies in World War I were initially unable to break Nebel's code. However, French artillery captain Georges-Jean Painvin (1886–1980) did succeed in deciphering the code. Though his work was good only for a single day, it enabled the allied armies to counter the German offensive of June 9, 1918.

FURTHER READING:

BOOKS:

Haldane, Robert A. *The Hidden War.* New York: St. Martin's Press,1978.

Konheim, Alan, G. *Cryptography: A Primer.* New York: Wiley,1981.

Rosen, Kenneth H., and John G. Michaels. *Handbook of Discrete and Combinatorial Mathematics.* Boca Raton, FL: CRC Press, 2000.

SEE ALSO

Codes and Ciphers
Cryptology, History

Advanced Photon Source (APS).

SEE *Argonne National Laboratory.*

AEC (Atomic Energy Commission).

SEE *DOE (United States Department of Energy).*

Aegis Air Defense System .

SEE *Ballistic Missile Defense Organization, United States.*

Afghanistan.

SEE *Enduring Freedom, Operation.*

Aflatoxin

JUDYTH SASSOON

Aflatoxins belong to a group of toxins called mycotoxins, which are derived from fungi. In particular, aflatoxins are produced by the soil-born molds *Aspergillus flavus* and *Aspergillus parasiticus* that grow on the seeds and plants. At least 13 aflatoxins have been identified including B1, B2, G1, G2, M1 and M2. The B aflatoxins fluoresce blue and the G aflatoxins fluoresce green in the presence of ultraviolet light. The M aflatoxins are present in milk products. Aflatoxin B1 is the most ubiquitous, most toxic and most well studied of the aflatoxins. *Aspergillus* spp. contamination occurs as a result of environmental stresses on plants such as heat, dryness, humidity or insect infestation. It can also occur if plants are harvested and stored in hot, humid environments. As a result, people who live in the regions of the world most prone to these conditions, sub-Saharan Africa and southeast Asia are at highest risk for aflatoxin poisoning.

Aflatoxins were first discovered in England in 1960 when more than 10,000 turkeys and ducks died within a few months. The disease contracted by these animals was called Turkey X disease and its cause was traced to *Aspergillus flavus* contamination of peanut meal that had originated in Brazil. The toxin was named for the short hand of its causative agent: *A. fla* .

Aflatoxins are the most toxic, naturally occurring carcinogens known. Aflatoxin B1 is an extremely hepatocarcinogenic compound, causing cancer of the liver in humans. Aflatoxin B1 exposure results in both steatosis (an accumulation of fat) and necrosis (cell death) of liver cells. Symptoms of aflatoxicosis are gastrointestinal including vomiting and abdominal pain. Other symptoms can include convulsions, pulmonary edema, coma and eventually death. Aflatoxins also pose a threat to developing fetuses and they are transferred from mother to infant in breast milk. Aflatoxins B1, G1 and M1 are carcinogenic in animals.

Aflatoxin poisoning occurs from ingestion of crops that have been infested with *Aspergillus* spp. or from eating animal products from animals that have ingested these crops. High concentrations of aflatoxins are most often found in plants with very nutritive seeds such as maize, nuts and cereal grains in Africa and rice in China and Southeast Asia. In the United States, peanuts are routinely tested for aflatoxin concentrations, and contamination has also occurred in corn, rice, and cereal grains.

Most consider aflatoxins extremely dangerous and suggest that in human food is only acceptable with no detectable concentration. The maximum allowable concentration of aflatoxins set by the United States FDA is 20 parts per billion (ppb). Foreign markets usually reject grains with concentrations of 4 to 15 ppb. Acceptable levels of aflatoxins for animal consumption are up to 100 ppb. Because of the strict regulations regarding the permissible concentration of aflatoxin, exporting countries often reserve contaminated grains for consumption within their own country. Because *Aspergillus* spp. is usually colorless and does not break down during cooking, it is difficult to know whether or not people are consuming contaminated food.

Evidence exists that Iraq used aflatoxins in biological weapons. In December of 1990, Iraq produced 2,200 liters of aflatoxin, 1,580 liters of which were used in biological warheads. In particular, 16 R400 bombs and 2 Al Hussein (SCUD) warheads were filled with the toxin.

FURTHER READING:

ELECTRONIC:

Aflatoxins—Home Page, "Aflatoxins: Occurrence and Risk" <http://www.ansci.cornell.edu/plants/toxicagents/aflatoxin/aflatoxin.html> (March 17, 2003).

Agriculture Network Information Center, "Plant Disease Announcements" <http://www.agnic.org/pmp/alpha.html> (March 11, 2003).

World Heath Organization: "Hazardous Chemicals in Human and Environmental Health"<http://www.who.int/pcs/training_material/hazardous_chemicals/section_1.htm#1.2> (March 11, 2003).

SEE ALSO

Biological Warfare
Food Supply, Counter-Terrorism
Toxicology

Africa, Modern U.S. Security Policy and Interventions

JUDSON KNIGHT

United States policy in Africa since World War II has generally been non-interventionist, in the sense that U.S. troops have seldom actually engaged in military or quasi-military activities on the African continent. Exceptions, however, do exist, most notable among them being a limited commitment (both of troops and of covert operatives) during the Congo civil war in the early 1960s, the bombing of Libya in 1986, and the humanitarian mission to Somalia in 1993. More often, the United States has provided assistance to African movements, such as anticommunist guerrillas in Angola during the 1970s and 1980s. America has also used diplomatic and economic pressure, both against South African apartheid in the

Children follow a United States soldier patrolling the Green Line, a heavily contested area in the Somali civil war of the 1980s, during Operation Restore Hope in 1992. ©PETER TURNLEY/CORBIS.

1980s and criminal activities in Nigeria during the twenty-first century.

Background

After the 1998 embassy bombings in Kenya and Tanzania, the United States conducted bombing raids over both Afghanistan and Sudan, attempting to neutralize Osama bin Laden and his al Qaeda terror network. The fact that the same terrorist group later caused the 2001 bombings in New York City and Washington, D.C., serves to illustrate the fact that events in Africa are not removed from impacting American security and policy. As of July, 2003, the U.S. made a limited troop commitment to secure stability in Liberia and considered a more extensive involvement.

In choosing their policy priorities for Africa, American leaders managed a fine line between appearing interventionist or imperialist on the one hand, and insensitive to Africans' misery on the other. Generally, U.S. policy in Africa has been guided by assessments of the strategic importance of a given nation, its existing alignment or non-alignment with U.S. interests, and the stability of its government.

With the exception of Liberia and Ethiopia, every nation in Africa—more than 50 in all—was at one time a European colony. This is true even in North Africa, whose people are linguistically and culturally distinct from their neighbors to the south. At the beginning of the twentieth century, France held much of west and central Africa; Britain southern and eastern Africa, as well as parts of West Africa; Belgium what is now the Congo, and Portugal a few notable colonies, among them Angola and Mozambique. Germany and Italy, latecomers to African colonialism, controlled some of the sites less rich in natural resources.

In the period between 1945 and 1975, virtually every nation in Africa gained independence, with the Portuguese—first Europeans to colonize in Africa—becoming the last to relinquish colonies. High hopes attended independence, but with few exceptions (a notable one being Botswana), the history of modern Africa has been an unrelieved tale of cruelty, corruption, mismanagement, and rampant disease and poverty. Funds given to help the African people have often ended up in the Swiss bank accounts of dictators, and money intended to build schools and feed children has instead been used to fund civil wars.

The Congo, Rwanda, and Africa's "First World War"

The Congo exemplified this problem. In 1960, Belgium granted its former colony independence, but this proved only the beginning of new troubles. Civil war ensued, and initially the United States, as a participant in a United Nations (UN) peacekeeping force, seemed to back Prime Minister Patrice Lumumba. But as Lumumba drifted increasingly into the Soviet orbit, the Central Intelligence Agency (CIA) considered means of assassinating him, in the words of the local CIA station chief, "to avoid another Cuba." Meanwhile, the United Stated provided assistance to army officer Joseph Désiré Mobutu, whose troops captured and killed Lumumba.

Although conditions in the Congo were difficult under Lumumba, they were at least as bad under Mobutu, who became unquestioned leader of the nation in 1966. He renamed the country Zaire and himself Mobutu Sese Seko Kuku Ngbendu wa za Banga, which means "the all-powerful warrior who, because of his endurance and inflexible will to win, will go from conquest to conquest, leaving fire in his wake." For the next three decades, Mobutu, supported by the United States and the World Bank, looted his country, building vast palaces for himself and fattening the pockets of his cronies while the majority of his people lived without electricity, running water, or basic medical care.

Mobutu was overthrown in 1997 by Laurent Kabila, who proved just as corrupt, and who was killed by his own bodyguards in 2001. By then, the Congo had become embroiled in events described collectively as "Africa's First World War." The opening salvo of that larger conflict—a series of conflicts involving Rwanda, the Congo (which returned to its original name in 1997), and other nations—was the infamous Rwandan genocide in 1994.

The conflict involved age-old disputes between the Hutu and Tutsi peoples, who together constitute most of the population in Rwanda, Burundi, and neighboring states. After Rwanda's Hutu dictator, Major General Juvenal Habyarimana, died in a plane crash on April 6, 1994, his supporters blamed the Tutsi-controlled Rwandan Patriotic Front (RPF), and launched a campaign of genocide that resulted in more than 800,000 deaths over a period of a few weeks. By July, the RPF had driven the remnants of the Habyarimana government, along with some 1 million refugees, into neighboring Zaire. This influx served to so destabilize the Mobutu regime that it helped provide the opportunity for Kabila's takeover.

Somalia, Ethiopia, and Angola: Marxism, Anarchy, and Intervention

The United States was criticized, both at home and abroad, for not intervening in Rwanda, an extremely poor and landlocked nation with almost no strategic importance to Washington. It is possible that had America intervened, it would have been condemned for interfering in other nations' internal affairs. Such was the case in Somalia just a few months earlier, when U.S. attempts to provide humanitarian assistance so inflamed resentment that even after the terrorist attacks of September, 2001, Muslim critics of U.S. policy would cite Somalia as an example of American imperialism.

Located on the horn of Africa, Somalia also achieved its independence in 1960, and also succumbed to dictatorship, in this case under Major General Mohamed Siad Barre. After overthrowing the government in 1969, Siad Barre launched the country on a disastrous experiment in Soviet-style socialism, complete with posters in the capital city of Mogadishu that featured his face alongside those of Karl Marx and V. I. Lenin. In a country where the principal form of organization is by clan, modern political forms of any kind were foreign, and it would have been difficult to find a more inadequate prescription for Somalia's challenges than Siad Barre's Marxist Leninism.

Ironically, the takeover of neighboring Ethiopia by Communists in 1974 proved Siad Barre's undoing. In the chaos that befell Ethiopia after the downfall of longtime emperor Haile Selassie, Somalia went to war with its neighbor over the Ogaden Desert, and by September, 1977, had all but won. At that point, however, the Soviets switched their allegiance to Ethiopia's Marxist government.

The Soviets' change of allegiance created a strange alliance between Siad Barre and the United States. The proxy war in the Horn of Africa nearly became an entanglement involving U.S. troops, as Zbigniew Brzezinski, National Security Advisor under President James E. Carter, briefly considered deploying the U.S. carrier *Kitty Hawk* to the region in March 1978. The United States and Somalia concluded military agreements in 1980 that allowed U.S. access to naval ports at Mogadishu and other cities.

The military alliance with the United States did not result in any meaningful changes in Siad Barre's style of rule, and over the next decade, his influence slowly declined until he was ousted in 1991. By then, with the Cold War all but finished, the United States—which had strategic naval bases farther south in Kenya—had no particular interest in preventing Somalia from sliding toward anarchy. Then, in 1992, during the last weeks of his administration, President George H. W. Bush committed 25,000 U.S. troops to a UN force involved in distributing famine relief supplies.

Bush was influenced by the fact that the UN had performed well during the crises surrounding the Persian Gulf War of 1990–91, but the experience in Somalia was not to be as successful. By 1993, U.S. forces had become caught in the middle of conflicts between local warlords, and on October 3, 18 U.S. Rangers were killed in a firefight on the streets of Mogadishu. Prior to this debacle, Secretary of Defense Les Aspin had outlined an agenda of

"nation-building" in a nation that had no true government, and in the aftermath of the Mogadishu disaster, Aspin resigned.

Ethiopia and Somalia were just a few of the nations that attempted to apply the Marxist formula to their problems during the 1970s. Numerous other nations aligned with Moscow, but few did so as openly as the former Portuguese colonies of Angola and Mozambique. The United States provided help to the rebels fighting in both countries, though aid to Angola was much greater. In 1985, President Ronald Reagan, under pressure from both the Department of Defense and the CIA, transferred some $15 million in antiaircraft and antitank missiles to the rebel movement.

The United States commitment to Angola was in part a response to the fact the Soviets and Cubans had become heavily involved on the side of the government, but it was also a product of the magnetism exerted by the rebels' charismatic leader, Jonas Savimbi. In 1966, Savimbi had formed the National Union for the Total Independence of Angola, known by the initials of its name in Portuguese, UNITA. First he fought against the Portuguese, then against the MPLA (Popular Movement for the Liberation of Angola) when it took control of the government after the Portuguese left. Because the MPLA was aligned with Moscow, Savimbi gained support from a wide array of nations opposed to the Soviet Union: the United States, China, and South Africa. Savimbi managed to convince American conservatives that he was an anti-communist, just as he presented himself to the Chinese as a Maoist. To the regime that maintained the system of apartheid in South Africa, Savimbi's victory would help keep blacks from getting the idea that they should gain a share of whites' wealth.

In reality, the war was not about ideology, but about control of the nation's diamond resources and other natural wealth. The Communist regime of José Eduardo dos Santos was corrupt and cruel, but Savimbi matched its record. In 1989, even Mobutu tried to step in and pressure him to accept a ceasefire. In 1992, with the Cold War over, Savimbi lost U.S. funding. He spent the remainder of his life fighting the government and opposition in his party, looting the populace, and resisting efforts toward peace. Six weeks after his death in February, 2002, the two sides signed a ceasefire agreement.

Liberia and South Africa: Oppression and Economics

In deciding to intervene, whether by military, economic, or diplomatic means, prudent leaders tend to favor a conservation of resources. An example was America's response to chaos in Liberia in 1990. The West African nation, founded by freed American slaves in 1847, has proven no more stable or successful than any of its neighbors that had been colonies. Nor has the American influence yet fostered a greater degree of respect for human rights: ironically, the freed slaves, known as Americo-Liberians, virtually enslaved the native Liberians, who lived under conditions of forced labor and extreme poverty.

Finally, in 1980, Sgt. Samuel K. Doe led a revolt against President William Tolbert, ending 133 years of oppression. Doe, however, proved a tyrant, and he benefited from some $500 million in U.S. aid even as the quality of life for the Liberian populace continued to decline. When rebels overthrew Doe in 1990, the United States quietly evacuated its diplomatic personnel and other citizens from the troubled nation.

In part because the nation-state is a western construct imposed on Africa, life in post-colonial times has often been characterized by the oppression of one ethnic group by another: first Hutu by Tutsi, then the reverse, first native Liberians by Americo-Liberians, then the reverse, and so on. As most of these situations involved native African ethnic groups, they have attracted little attention in the outside world. By contrast, the regime of apartheid that prevailed in South Africa for more than four decades after 1948, involving as it did oppression of a black majority by a white minority, invoked sharp criticism throughout the western world.

Although many Americans had long condemned apartheid, the issue did not become a part of American popular culture until 1985, as entertainers and college students took up the cause. Activists pressured the Reagan administration to deal aggressively with South Africa, and to isolate the nation economically. In fact the United States did impose a number of economic restrictions on South Africa, but not to a degree demanded by activists. The solutions that worked with recalcitrant U.S. states during desegregation in the 1960s would not necessarily be as successful with an independent nation in the 1980s. Reagan reasoned that while apartheid did not comport with U.S. values, South Africa was of far greater value to the United States than many of its most outspoken critics—among them Zimbabwe, home to the notorious dictatorship of Robert Mugabe.

Reagan's administration used a combination of limited economic and diplomatic pressure, while allowing South Africans—who at least had a framework of European-style representational government—to work out their own differences. In the end, opposition leader Nelson Mandela was released from prison, apartheid fell, and Mandela became the president of a new South Africa.

Other Interventions and Non-Interventions

In terms of economic intervention, Sierra Leone and Chad may offer positive examples of what the world community can do to affect policy in Africa. In 2000, the UN imposed a ban on the purchase of diamonds from Sierra Leone, sales of which had been used in large part to fund that nation's civil war. Two years later, the 11-year war ended in a ceasefire.

Also in 2000, construction began on a pipeline through Chad, an extremely poor country in which oil had been discovered. Rather than permit a repeat of past mistakes, a consortium of companies (including America's Exxon and Mobil), along with the World Bank, devised a strategy to prevent the nation's rulers from misusing funds. Agreements included stipulations that 80% of all oil revenues would be spent on improving health, education, and welfare for the populace. Another 10% would go into escrow accounts for future generations, 5% would be directed toward the local populations in the area of the oil fields, and only 5% would be placed in the hands of the government to do with as it pleased.

Nigeria: counterfeiting and advance-fee scams. Another economic and legal battleground—one where problems remain is Nigeria. One of the leading nations in Africa in terms of size and potential wealth, with its oil riches, Nigeria is only slightly more stable than its neighbors, and criminal activity is rampant. The country is particularly notorious for its counterfeiting operations and its business scams.

Nigerian counterfeiting involves not banknotes, but consumer and industrial goods, including garments and textiles, electronics, spare parts, pharmaceuticals, personal products, and even soft drinks. The reason, in part, is that intellectual property owners, frustrated with the national bureaucracy, have done little to put a stop to counterfeiting efforts there. Additionally, owners of rights to these products are often unaware of counterfeiting activities in Nigeria. The Nigerian government has injunctions against these crimes, but has been largely ineffective in pursuing them.

In 1999, years of military rule in Nigeria ended, and U.S. officials took advantage of this opportunity to strengthen law enforcement efforts there. In July, 2002, the two countries signed an agreement for increased law-enforcement cooperation. Part of the agreement was a grant of $3.5 million from the United States, intended to help Nigeria modernize its police force and provide additional resources to the country's special fraud unit, which targets 419 known scams.

FURTHER READING:

BOOKS:

Campbell, Kurt M., and Michele A. Fluornoy. *To Prevail: An American Strategy for the Campaign against Terrorism.* Washington, D.C.: CSIS Press, 2001.

Haass, Richard, and Meghan L. O'Sullivan. *Honey and Vinegar: Incentives, Sanctions, and Foreign Policy.* Washington, D.C.: Brookings Institution Press, 2000.

Kissinger, Henry. *Years of Renewal.* New York: Simon and Schuster, 1999.

Roberts, Brad. *U.S. Foreign Policy after the Cold War.* Cambridge, MA: MIT Press, 1992.

ELECTRONIC:

African Issues. U.S. Department of States. <http://usinfo.state.gov/regional/af/> (April 29, 2003).

Congo Crisis. Maxwell Air Force Base. <http://www.au.af.mil/au/aul/bibs/congo/congo.htm> (April 29, 2003).

USAID in Africa. U.S. Agency for International Development. <http://www.usaid.gov/regions/afr/> (April 29, 2003).

SEE ALSO

Americas, Modern U.S. Security Policy and Interventions
Egypt, Intelligence and Security
IMF (International Monetary Fund)
International Narcotics and Law Enforcement Affairs (INL), United States Bureau
Kenya, Bombing of United States Embassy
Libya, Intelligence and Security
Libya, U.S. Attack (1986)
Middle East, Modern U.S. Security Policy and Interventions
Morocco, Intelligence and Security
South Africa, Intelligence and Security
Sudan, Intelligence and Security

Agent Orange

Agent Orange is a defoliant, that is, a chemical that kills plants and causes the leaves to fall off the dying plants. The name was a code devised by the United States military during the development of the chemical mixture. The name arose from the orange band that marked the containers storing the defoliant.

Agent Orange was an equal mixture of two chemicals; 2, 4–D (2,4, dichlorophenoxyl acetic acid) and 2, 4, 5–T (2, 4, 5-trichlorophenoxy acetic acid). Another compound designated TCDD (which stands for 2, 3, 7, 8-tetrachlorodibenzo-para-dioxin) is a by-product of the manufacturing process, and remains as a contaminant of the Agent Orange mixture. It is this dioxin contaminant that has proven to be damaging to human health.

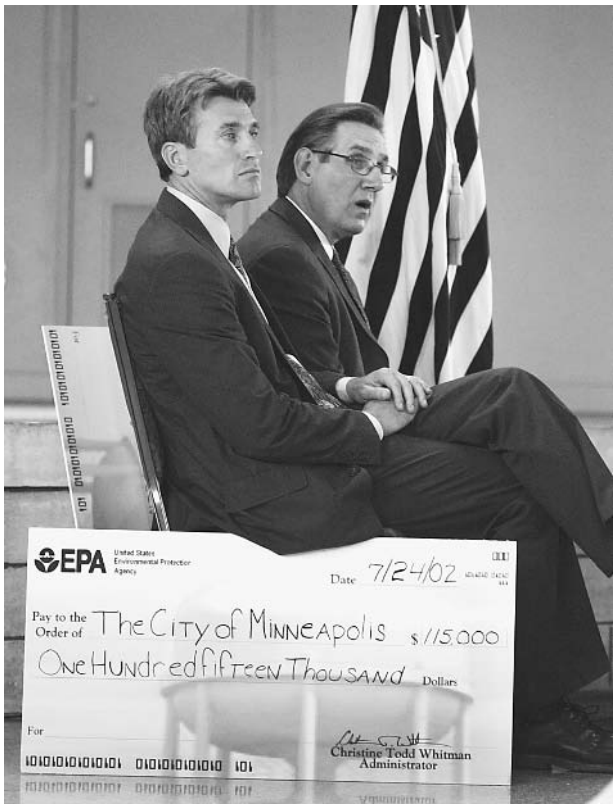
Agent Orange was devised in the 1940s. It was widely used during the 1960s during the Vietnam War. The dispersal of a massive amount of Agent Orange throughout the tropical jungles of Vietnam (an estimated 19 million gallons were dispersed) was intended to deprive the Viet Cong of jungle cover in which to hide.

By 1971, the use of Agent Orange in Vietnam had ended. Even today, however, the damage caused to the vegetation of the region by the spraying of Agent Orange is still visible. Agent Orange applications affected foliage of a diversity of tropical ecosystems of Vietnam, but the most severe damage occurred in the forested coastal areas.

Agent Orange was sprayed over 14 million acres of inland tropical forest. A single spray treatment killed about 10% of the tall trees comprising the forest canopy.

Because Agent Orange herbicide remains in the soil for some time, the contaminant TCDD is quite persistent in soil, with a half-life of three years. (In that period of time, one half of the dioxin originally applied would still be present in the soil.)

Evidence also suggests that the defoliant, and in particular the TCCD dioxin component, is a health threat to soldiers who were exposed to Agent Orange during their tour of duty in Vietnam. Tests using animals have identified TCCD as the cause of a wide variety of maladies. In the mid 1990s, the "Pointman" project was begun in New Jersey, which scientifically assessed select veterans in order to ascertain if their exposure to Agent Orange had damaged them. The project is ongoing. In the meantime, veterans organizations continue to lobby for financial compensation for the suffering they assert has been inflicted on some soldiers by Agent Orange.



Minneapolis Mayor R. T. Ryback, left, and St. Paul Mayor Randy Kelly, right, listen during a 2002 meeting where Christine Whitman, head of the Environmental Protection Agency, presented each city with checks for $115,000 in EPA grants for water security planning. AP/WIDE WORLD PHOTOS.

■ FURTHER READING

BOOKS:

Gough, M. *Agent Orange: The Facts.* New York: Perseus Books, 1986.

National Academy of Sciences. *Veterans and Agent Orange: Health Effects of Herbicides Used in Vietnam.* Washington, DC: National Academy Press, 1994.

Schuck, P. H. H. *Agent Orange on Trial: Mass Toxic Disasters in the Courts.* Boston: Harvard University press, 1990.

AI (Army Intelligence).

SEE *INSCOM (United States Army Intelligence and Security Command).*

Air America.

SEE *Vietnam War.*

Air and Water Purification, Security Issues

■ BRIAN HOYLE

Both water and air are particularly vulnerable to contamination by some bacteria and protozoa, and by their toxic products. Chemicals can also be dispersed in water and by air. A recent example occurred in 1995, when the Japanese cult Aum Shinrikyo released sarin gas into the Tokyo subway system. The poisonous gas attack killed 12 people and sickened 5,000.

Technologies exist to kill the microorganisms that might be present (disinfection) or to completely remove the microbes and chemicals from the air or water (purification). These technologies, however, are usually designed to remove naturally occurring or polluting contaminants.

Groundwater or surface water treatment focuses on providing water that is fit to drink. Typically, the water is filtered to remove large debris. Some jurisdictions also pass the water through microfilters that remove objects as small as viruses from the treated water. Most drinking water is treated with chlorine or chlorine-containing compounds to kill any bacteria. Other treatments that are gaining widespread acceptance include the use of ultraviolet light, ozone, and other chemicals such as bromine. Water can also be purified by techniques involving reverse osmosis and steam distillation, although these techniques are not typically used, as they are expensive and purify relatively small volumes of water at one time.

Treatment and monitoring ensure that the water emerging from the treatment plant is safe to drink and that

it remains that way all the way to the consumer's tap. However, these measures are not intended to thwart a deliberate act of sabotage. Many of the water treatment and distribution systems in use around the world were built decades ago. Domestic terrorism was virtually unknown at that time, and protective measures were seldom part of the system's design. For example, surface water supplies are often unguarded and exposed (unfenced, etc.).

For large surface water supplies, the volume of water alone makes the possibility of deliberate contamination remote. For example, it has been estimated that the contamination of the Crystal Springs Reservoir that supplies some of the water for San Francisco, California with enough hydrogen cyanide to harm anyone who drinks a glass of water would require over 400,000 metric tons of the poison. Similarly, huge amounts of bacteria or viruses would be required.

Poisoning smaller water sources, particularly after the water has left the treatment plant, is a more realistic possibility. Even if the water has been chlorinated, disease causing microorganisms such as *Giardia* and *Cryptosporidium* are resistant to chlorine, as are bacterial toxins.

More than 100,000 communities in the United States obtain their water from a community well, without the benefit of chlorination or other treatment. Deliberate contamination of these systems could put millions of people at risk.

Another security risk with water supplies involves the nature of monitoring the water. As of 2002, most monitoring techniques for living and nonliving contaminants requires up to 24 hours. "Real time" tests are not routinely available. Thus, contamination would not be detected until long after people had consumed the water.

Air is vulnerable to contamination with a variety of bacteria, viruses, and fungi that are light enough to become dispersed in air currents. When inhaled, the microbes can cause infections. Chemicals and toxins can also float in the air, to be inhaled or settle onto exposed skin.

Air purification has long been possible using filters. Bacteria, viruses, and even some inorganic chemicals can be retained on specialized filters. These filters are mainly suitable for laboratories or relatively small, specifically designed ventilation systems. In large indoor environments such as malls or sizeable office buildings, and in the open air, air purification is virtually impossible.

Contamination of the open air poses a similar problem as the contamination of a large volume of water, namely the amount of poisonous agent that is required. For example, estimates are that hundreds of pounds of anthrax spores would be needed to achieve a massive contamination of the population of a large city.

The release of toxic agents into a more limited area such as an office building is more plausible. Some buildings that are deemed to be a security risk, or which are used for research with highly infectious microbes, are equipped with safeguards to prevent the spread of airborne infectious agents or poisons. Air treatment, ventilation filters, alarms, and the ability to isolate contaminated zones are usually part of the designed safeguards.

FURTHER READING:

BOOKS:

Drell, S. D. *The New Terror: Facing the Threat of Biological and Chemical Weapons.* Stanford, CA: Hoover Institute Press, 1999.

Henderson, D. A., "The Looming Threat of Bioterrorism." *Science* no. 283 (1999): 1279–1282.

Kowalski, W. J., W. P. Bahnfleth, and T. S. Whittam. "Filtration of Airborne Microorganisms: Modeling and Prediction." *ASHRAE Transactions* 105 (1999): 4–17.

O'Toole, T. "Smallpox: An Attack Scenario." *Emerging Infectious Diseases* 5 (1999): 540–546.

SEE ALSO

Air Plume and Chemical Analysis
Biological Warfare
Environmental Issues Impact on Security
Microbiology: Applications to Espionage, Intelligence and Security
Water Supply: Counter Terrorism

Air Force Intelligence, United States

JUDSON KNIGHT

The intelligence-gathering efforts of the U.S. Air Force long predate its establishment as a separate military service in 1947. The Air Force has conducted extensive aerial surveillance, as well as air technical intelligence (ATI) operations—that is, the study of foreign aircraft themselves—since the end of World War I. As time has gone on, equipment and techniques have become more sophisticated, and involvement more widespread. Today's Air Combat Command includes a number of intelligence agencies.

Background. The U.S. Air Force has its roots in the Aeronautical Section of the U.S. Signal Corps, founded in 1907, and renamed the Aviation Section in 1914. This became the U.S. Army Air Service in 1918, and the Army Air Corps in 1926. In 1941, on the eve of World War II, the Department of the Army renamed its air section the United States Army Air Force. Two years after the end of World War II, the National Security Act of 1947 for the first time established the Air Force as a separate military service.

Throughout the twentieth century, the air services took part in aerial intelligence, particularly during the Cold

An image ready analyst from the AIA (Air Intelligence Agency) at Lackland Air Force Base, Texas, examines the imagery on a light table taken by a U-2 spy plane. AP/WIDE WORLD PHOTOS.

War and thereafter. In the 1950s, the United States launched one of its most successful spy aircraft, the U-2. Despite the shootdown of pilot Francis Gary Powers over the Soviet Union in 1960, as well as the passage of time and the aging of the craft, the U-2 remained in service during the 1990s. In addition to a number of surveillance craft such as the SR-71 Blackbird, deployed the Vietnam War, the Air Force made extensive use of satellites and unmanned, remotely piloted vehicles.

The Air Force and its predecessors also took a great deal of interest in ATI, which involves the study of aircraft, parts, and accessories. ATI has helped the United States, not only in the building of better aircraft, but also in targeting enemy defense plants for bombing runs. A by-product of ATI work has also been advances in other areas, including computer systems in general, and automatic language translation technology in particular.

Air intelligence today. Most air intelligence work today is under the leadership of Air Combat Command (ACC). Headquartered at Langley, Virginia, ACC operates fighter, bomber, reconnaissance, battle-management, rescue, and theatre airlift aircraft, along with command, control, communication, and intelligence systems. Under its leadership are a number of intelligence-related Air Force activities, most notable of which are the Air Intelligence Agency (AIA) and the Air Force Technical Applications Center (AFTAC).

Established in October 1993, AIA grew out of the Air Force Intelligence Service, established in June 1972. AIA, which is tasked with intelligence collection, security, support for treaty monitoring, and electronic warfare, is headquartered at Kelly Air Force Base (AFB) in Texas. It consists of several components, including the 67th Information Operations Wing and the 690th Information Operations Group at Kelly, as well as the 70th Intelligence Wing at Barksdale AFB in Louisiana. Its three centers are the National Air Intelligence Center at Wright-Patterson AFB in Ohio, the Air Force Information Warfare Center at Kelly, and AFTAC, which it supports administratively, at Patrick AFB in Florida. In the mid-1990s, AIA included 12,600 active-duty personnel, along with 1,900 reservists and 2,400 civilians.

AFTAC is the sole Department of Defense agency operating and maintaining a global network of nuclear

event detection sensors, the U.S. Atomic Energy Detection System (USAEDS). When the USAEDS detects a disturbance in the ground, water, atmosphere, or space, AFTAC laboratories undertake an analysis of the event to discover whether its causes relate to nuclear testing or deployment. It then reports its findings to national command authorities through Air Force headquarters. In the mid-1990s, AFTAC developed the U.S. National Data Center, which makes use of various ground and satellite centers for the monitoring of nuclear activities and treaty compliance worldwide.

FURTHER READING:

BOOKS:

Boyne, Walter J. *Beyond the Wild Blue: A History of the United States Air Force, 1947–1997.* New York: St. Martin's Press, 1997.

Clancy, Tom. *Fighter Wing: A Guided Tour of an Air Force Combat Wing.* New York: Berkley Books, 1995.

Gann, Ernest Kellogg. *The Black Watch: The Men Who Fly America's Secret Spy Planes.* New York: Random House, 1989.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

ELECTRONIC:

U.S. Air Combat Command. <http://www2.acc.af.mil/> (April 13, 2003).

U.S. Air Force Intelligence and Related. Federation of American Scientists. <http://www.fas.org/irp/agency/usaf/> (April 13, 2003).

U.S. Air Intelligence Agency. <http://aia.lackland.af.mil/> (April 13, 2003).

SEE ALSO

Air Force Office of Special Investigations, United States
DoD (United States Department of Defense)
J-Stars
Photographic Interpretation Center (NPIC), United States National
Photography, High-Altitude
USSTRATCOM (United States Strategic Command)

Air Force Office of Special Investigations, United States

The Air Force Office of Special Investigations (AFOSI) is the principal investigative service of the United States Air Force. Established in 1948, AFOSI is charged with investigating and preventing criminal activities by United States Air Force personnel, as well as by individuals outside the air force whose actions threaten the service's equipment, personnel, activities, or security. Its ranks, which numbered nearly 2,500 in 2002, include active-duty Air Force personnel, reservists, and civilians.

Then United States Secretary of the Air Force W. Stuart Symington formed AFOSI on August 1, 1948, as the result of recommendations by the United States Congress that the air force (created in 1947) consolidate its investigative activities. Symington patterned the new office after the Federal Bureau of Investigation (FBI), and appointed Special Agent Joseph Carroll, assistant to FBI director J. Edgar Hoover, as the first AFOSI chief. Symington and Carroll developed an investigative service designed to provide unbiased information and operate independent of top air force command. To this end, the AFOSI included civilian personnel from the beginning.

AFOSI is based on a fourfold mission, intended to protect the air force from dangers within and without. As stated by AFOSI itself, that mission is to (1) Detect and provide early warning of worldwide threats to the Air Force; (2) Identify and resolve crime impacting Air Force readiness or good order and discipline; (3) Combat threats to Air Force information systems and technologies; and (4) Defeat and deter fraud in the acquisition of Air Force prioritized weapons systems.

Fulfillment of the AFOSI mission. The majority of AFOSI activities are directed toward the fulfillment of the second directive listed above. Among the crimes addressed by AFOSI investigators are murder, robbery, rape, drug use and trafficking, black-market activities, and other unlawful acts committed by or against air force personnel. Economic crime, or fraud, is an area of investigation that places particularly large demands on AFOSI resources.

Additionally, the service is concerned with detecting and protecting against outside threats, activities that require investigation of espionage, terrorism, technology transfer, and computer infiltration. In line with the first directive in its mission, AFOSI personnel provide personal protection to senior air force leaders and other officials.

Within the ranks of AFOSI are also personnel with specialized missions and skills who fulfill functions ranging from that of polygrapher to computer expert to behavioral scientist. Other AFOSI agents operate within one of three antiterrorism teams, based at Lackland Air Force Base (AFB) in Texas; Ramstein AFB in Germany; and Hickham AFB in Hawaii.

Organization, personnel, and training. In addition to AFOSI headquarters, the organization has eight field investigation regions. Of these, seven are tied with major air force commands: materiel (Region 1), air combat (Region 2), air mobility (Region 3), air education and training (Region 4), United States Air Forces in Europe (Region 5), Pacific Air Forces (Region 6), and Air Force Space Command (Region 8). In line with the original vision of AFOSI as an independent unit, these regions report to AFOSI headquarters and

not to the relevant air force commanders. Finally, there is Region 7, which provides counterintelligence and security-program management under the direction of the Secretary of the Air Force.

As of 2002, AFOSI included more than 160 units worldwide. Its ranks numbered 2,475, with members drawn from active-duty Air Force personnel, reservists, and civilians. The vast majority—1,890 persons—were special agents bearing credentials at the federal level. Each year, the AFOSI, one of the most popular career-field choices in the United States Air Force, welcomed 230 new special agents drawn from active-duty officers and enlisted members, reservists, and civilians.

All members receive 11 weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, alongside trainees for other federal law enforcement services. They follow this with another six weeks of training specific to the AFOSI mission. After a one-year probationary period in the field, members typically receive additional training in their given specialties.

■ FURTHER READING:

BOOKS:

DOD Investigation Programs: Background Data. Washington, D.C.: United States General Accounting Office, 1989.

Wilson, William. *Dictionary of the United States Intelligence Services: Over 1500 Terms, Programs, and Agencies.* Jefferson, NC: McFarland, 1996.

ELECTRONIC:

Air Force Office of Special Investigations. <http://www.dtic.mil/afosi/> (December 29, 2002).

SEE ALSO

Air Force Intelligence, United States

Air Marshals, United States

United States air marshals are the first police force of the federal government created solely to protect against terrorism. Though they existed in limited numbers prior to the September 11, 2001, terrorist attacks, the signing of the Aviation and Transportation Security Act (ATSA) on November 19 of the same year completely changed the nature of the air marshal program. The ATSA created the air marshals' new employer, the Transportation Security Administration (TSA), and within a little more than a year, several thousand air marshals were on the job. Air marshals perform their job discreetly, and many aspects of the program are deliberately kept secret so as to increase its effectiveness.

The Changing Face of Flight

At the end of 2001, the federal air marshal program had 33 armed officers, and a budget of about $4 million. A year later, the number of employees had swelled into the thousands—U.S. officials are reticent, for security reasons, to indicate the number of air marshals that have been deployed—with a budget of more than $1 billion. The rapid pace of growth was symptomatic of a larger change in the face of air travel after the September 11th attacks. In the aftermath, the federal government placed security screeners under government employment, and planned to put in place a new computerized passenger-profiling system. These were visible signs that the ordinary traveler could hardly fail to notice. Most of all, travelers were confronted with long lines to enter terminals, and with new security rules. Only persons with a ticket were permitted past security checkpoints and into departure gates, and even the most seemingly innocuous items, such as tweezers, were subject to confiscation by security screeners. By January, 2003, all passengers were additionally required to bring luggage intended to be checked into the hold of the aircraft to a screening point for x-ray or other scanning.

The invisible air marshals. In contrast to these visible signs of change, there was one change passengers were not likely to notice: the addition of air marshals. In fact, if a marshal's presence on a routine flight was noticed, that meant he (more than 95% of air marshals are male) was not doing his job correctly. A key element of the marshal program is its invisibility, and this is so for a number of reasons, not least of which is the fact that not every flight has a marshal aboard.

At any given moment at the height of business hours, there are approximately 6,000 commercial flights in the air somewhere in the United States. Every day, 25,000 aircraft take off and land, and though the ranks of the marshal program have swelled since September 11, it is not possible to have a marshal on every flight. Officials estimate that even for the highest-priority flights (the determination of which is made by analyzing a number of factors, such as major events that may attract tourist attention), only about 15% had an air marshal on board in the first year after September 11.

The air marshal's work. Federal air marshals, known as FAMs, go through a specific procedure when assigned to a flight. They dress in civilian clothes, and before boarding, present their credentials to a ticket agent, who gives them a ticket. Since September, 2001, ticket agents have been trained in this procedure, and are aware of the security precautions involved, which include not drawing any attention to the fact that an FAM is present.

After receiving his ticket, the FAM enters the terminal by special means that allow him to bypass a security

A federal air marshal trainee shoots live rounds during a training session in Egg Harbor Township, New Jersey. Thousands of armed, undercover air marshals have joined the service since the September 11, 2001, terrorist attacks and are flying carefully chosen missions, sometimes on an hour's notice because of new terrorist threats. AP/WIDE WORLD PHOTOS.

check, because he is armed. Once aboard the plane, the crew has knowledge that a marshal is on board, and therefore, he is permitted access to discreetly check all areas of the plane. Federal air marshals are trained to have a variety of ordinary cover stories available to discourage suspicion about repeated movements in different areas of the aircraft, should they become necessary. The Federal air marshal program motto is *Invisus, Inauditus, Impavidus*—unseen, unheard, unafraid.

Hazards of the job. In the first year after September 2001, FAMs made a dozen arrests, none of them related to terrorism. They filed about a thousand reports of suspicious activities on planes, but these numbers have shown signs of decreasing as time as passed. Apparently, in the early months, FAMs tended to be overly cautious or overly reactive to potentially dangerous situations, but experience has made them more judicious.

Early assessments of the FAM program suggest that perhaps the greatest routine occupational hazard is a decrease in concentration due to the monotony of being a repeated airline passenger. Flying tends to be taxing enough for civilians who do it regularly, but the FAM does not have the option of going to sleep. Nor is he free to lose himself completely in a book or magazine article, or an in-flight movie, though he may take part in such activities as a means of blending in. On the one hand, the FAM must try to appear completely ordinary, and on the other, he must be on the alert at all times. Concerned about the effects of flight fatigue on air marshals, the TSA in January, 2003, announced plans to temporarily reassign some FAMs. In order to gain some relief from the boredom and exhaustion of flight, some of these agents would serve in airport terminals, providing surveillance. This announcement elicited considerable criticism, particularly from airport security officials, who complained that the FAMs were most needed in the skies, and that airports were already overstaffed with security personnel.

Issues of training and expertise have also raised concerns about the FAM program. Prior to September 2001, FAMs received 12 weeks' worth of training, but afterward, officials of the Federal Aviation Administration (FAA) and later TSA found themselves faced with a demand to hire and train some 800 FAMs a month. As a result, new recruits found themselves on the job with less than seven weeks' training. Those with previous federal law-enforcement experience might be deployed after as little as a single week of compacted instruction.

In May 2002, as the Senate was considering legislation to allow pilots to carry handguns, TSA director John Magaw testified that the expertise of FAMs was such that pilots did not need to carry guns. However, TSA officials later acknowledged that new recruits had not been required to undergo the rigorous shooting tests required of air marshals prior to September, 2001.

Given the fact that the program had experienced a sudden upsurge in its personnel rolls—equivalent to that of an army mobilizing after a declaration of war—inefficiencies were virtually inevitable. The challenge with which directors of the FAM program were confronted after September, 2001, would have been daunting for any agency, public or private, and thus, the program requires more time before its full effectiveness can be accurately assessed.

FURTHER READING:

PERIODICALS:

Donnelly, Sally B. "Grounding the Air Marshals." *Time.* 161, no. 4 (January 27, 2003): 17.

Lombardi, Kate Stone. "Air Travel Under a More Watchful Eye." *New York Times.* (January 26, 2003): WC1.

Schneider, Greg, and Sara Kehaulani Goo. "For Air Marshals, a Steep Takeoff." *Washington Post.* (January 2, 2003): A1.

Wald, Matthew L. "New Rule to Limit Boarding Passes from Gate." *New York Times.* (December 10, 2002): A24.

ELECTRONIC:

"Armed Air Marshals for UK Flights." British Broadcasting Corporation (BBC) News. <http://news.bbc.co.uk/1/h1/uk_politics/2590309.stm> (March 5, 2003).

Transportation Security Administration. <http://www.tsa.gov/public/> (March 5, 2003).

SEE ALSO

Aviation Security Screeners, United States
Civil Aviation Security, United States
FAA (United States Federal Aviation Administration)
September 11 Terrorist Attacks on the United States
Transportation Department, United States

Air Plume and Chemical Analysis

BRIAN HOYLE

An air plume is a layer of warm air that immediately surrounds a person's body. It has also been referred to as a human thermal plume.

The skin's surface temperature is typically 33° Celsius, which is approximately nine degrees warmer than the surrounding air at a typical room temperature. The temperature difference causes heat to be lost from the entire surface of the skin to the surrounding air.

Because warm air rises, the plume rises up the body and flows off the top of the head and shoulders, instead of radiating outward to the surrounding air from all parts of the body. As the air moves up and away from a person, tiny bits of the skin and chemicals that were present on the skin's surface can also be carried upward. The presence of clothing has no effect on the upward movement of the air.

The presence of clothing also does not block the migration of chemicals from items being carried in the clothing. Particles of an explosive in a pocket, for example, will be able to pass through the pores of the fabric to the immediate vicinity of the skin. There, they will encounter the air plume and migrate upward with the airflow.

The chemicals that are carried in the air plume can be detected using sophisticated detection equipment. The chemical analysis of an air plume can detect explosives and even the aromas emitted by microorganisms.

The analysis of an air plume has grown out of studies that relied on the use of what is termed a *schlieren* system. The word schlieren is German for streaks, and describes the appearance of air in a special optical system. Schlieren optics measure air flow based on the scattering of light due to differences in density at the interface between moving air and relatively motionless air.

Scientists interested in imaging the schlieren patterns produced by people modified the small optical system so that it could be accommodated in a larger device. The device is similar in appearance to the walk through X-ray machines that are now commonplace in airport security areas.

When a subject walks through the portal, the air plume is drawn into an analysis chamber positioned in the portal's archway. Any particles present are collected in a trap. As well, the vapors in the air plume can be condensed onto the trap. Chemical analysis is performed using a machine called an ion trap mobility spectrometer.

The trapping of particles and condensation of the vaporous air plume concentrates any compounds that are present. The trapped sample is delivered to a chamber that converts the sample molecules to ions. Typically, bombarding the sample atoms with electrons accomplishes this conversion. When an electron collides with a sample ion, an electron is dislodged from the sample atom, producing a positively charged ion. As voltage is applied along the length of the chamber, the positively charged sample ions move toward the negatively charged cathode. Separation of the ions occurs based upon their different sizes and masses. For example, smaller ions move down the chamber faster than larger ions. As ions arrive at the cathode, a current is produced. The current can be amplified to produce a detectable signal. The different signals can be plotted to produce a spectrum. The different peaks in the spectrum can be related

to known ions to determine the ionic composition of the sample.

The pattern of the spectrum produced by the nitrate (NO) groups in an explosive such as 2,4,6–dinitrotoluene (TNT) is characteristic of the arrangement of the NO groups within the chemical structure, and is different from the pattern produced by other NO-containing explosives like nitroglycerine, ethylene glycol dinitrate nitroglycerin, cyclotrimethylenetrinitramine, and pentaerythritoltetranitrate.

The spectrometer is extremely sensitive and fast. Chemicals that are present in only a few parts per billion will be detected in about 10 seconds. Thus, even a very small amount of explosive carried in a pocket would register in the spectrometer.

Currently, the chemical analysis of the air plume is geared towards the detection of explosives. The incorporation of other sensors, such as the "electronic nose" that can detect and identify some bacteria based on the unique chemical vapors given off by the cells will enable biological analysis of air plumes in addition to chemical analysis. Incorporating a metal detector into the device could enable one device to be used to screen for conventional, chemical, and biological weapons.

■ FURTHER READING:

BOOKS:

Settles, Gary S. *Schlieren and Shadowgraph Techniques.* Heidelberg: Springer-Verlag, 2001.

PERIODICALS:

Crabb, C. "Biosensors Enliven the Science of Detection." *Chemical Engineering* August (1998): 35–39.

Settles, G.S., and W.J. McCann. "Potential for Portal Detection of Human Chemical and Biological Contamination." *SPIE Aerosense* no. 4378 (2001): paper 01.

SEE ALSO

Air and Water Purification, Security Issues
Biosensor Technologies
Gas Chromatograph-Mass Spectrometer

Aircraft Carrier

■ JUDSON KNIGHT

Sometimes characterized as "floating cities," aircraft carriers are a potent symbol of America's strength as a superpower. Although nations ranging from the United Kingdom and Russia to Peru and Thailand have their light carrier and helicopter carriers, the large carriers of the United States are without parallel in ability and firepower. Carriers provide an important means of force projection from the continental United States to any theatre, no matter how hostile, and offer a floating platform for missions that include both combat and intelligence-gathering. As President William J. Clinton said during a visit to the carrier *Theodore Roosevelt* in the 1990s, "When word of crisis breaks out in Washington, it's no accident that the first question that comes to everyone's lips is, 'where is the nearest carrier?'"

Components in the Carrier Concept

The carrier is one of the leading means for force projection, or the ability to project an aggregation of military personnel from the continental United States (or another theatre) in response to military requirements. As long as it operates in international waters, a carrier needs no permission to conduct landings or overflights. These floating military bases constitute sovereign U.S. territory capable of moving over the oceans—70% of Earth's surface—in the service of U.S. interests.

Carriers make possible a variety of options. They may be used to insert forces ashore; on the other hand, their presence is so intimidating that they may be used simply to "show the flag," or remind hostile powers of the U.S. presence. They are capable of attacking airborne, sea borne, or land targets, and engage in sustained operations in support of other forces—for example, the ground forces deployed for Operation Iraqi Freedom in 2003.

Battle groups and air wings. National command authorities do not deploy carriers alone. Rather, the carrier is the center of a battle group, a force of a half-dozen or more ships. The carrier battle group, or CVBG, may be used to protect merchant or military shipping; to provide protection to a Marine amphibious source en route to, or arriving in, an objective area; or to establish a naval presence in support of national security interests

Members of a battle group may include at least one destroyer and one frigate, two attack submarines, two guided missile cruisers, one guided missile destroyer, and a logistical support ship. Destroyers and frigates are primarily for anti-submarine warfare, while attack submarines, as their name implies, attack both enemy submarines and ships. Both guided missile cruisers and destroyers are multi-mission surface combatants, the first type armed with Tomahawk cruise missiles for long-range strike capability, and the second equipped for anti-aircraft warfare. The logistical support ship is usually a combined ammunition, oiler, and supply vessel.

Additionally, the carrier—by definition—serves as a home base for a number of aircraft, known as the carrier air wing. These typically include three squadrons of F/A-18 Hornets, which are all-weather fighter and attack aircraft, and one squadron of F-14 Tomcats, made for fleet air defense and precision strikes against ground targets. Along with these are one squadron of S-3B Vikings, the primary overhead/mission tanker, which is equipped for day and

A flight deck crew gives the launch signal as an F/A-18-C Hornet is catapulted off the flight deck of the carrier USS *Kitty Hawk* in the Persian Gulf as part of over 3,000 American sorties flown during Operation Iraqi Freedom. AP/WIDE WORLD PHOTOS.

night surveillance, electronic countermeasures, command/control/communications warfare, and search and rescue; one squadron of EA-6B Prowlers, which jams enemy radar, electronic data links, and communications; one squadron of E-2C Hawkeyes, all-weather tactical warning and control system aircraft; and one squadron of SH-60 Seahawks, twin-engine utility or assault helicopters.

Overview of a Modern Carrier

U.S. aircraft carriers fall into several groupings, the largest of which is the Nimitz class. Largest warships in the world, these measure 1,092 feet (332.9 m) from bow to stern, and 252 feet (76.8 m) across. As large as it is, the large U.S. carrier still does not provide enough room for takeoff and landing by conventional means; therefore, the carrier deck includes a number of items for these purposes, as well as for the storage of aircraft below decks.

The aircraft do not remain on the carrier's deck when not in use; rather, they rest in a cavernous hangar beneath the deck, to which they can be summoned by means of four deck-edge elevators, each of which is capable of moving two aircraft at a time. For taking off, aircraft are attached to catapults, which give them the necessary acceleration to go from a standing position to 165 miles per hour (265.5 kph) in just two seconds. The flight crew of the Nimitz-class aircraft carrier is capable of launching two aircraft and landing one every 37 seconds in daylight, or one per minute at night.

The flight crew itself is a choreographed team, or rather a group of teams, each distinguished by jackets of different colors that signify functions. To the pilot in the air, the most critical colors on the deck are the amber and red lights of the Fresnel lenses on deck. Depending on the angle of the light, the pilot knows if he is too low or too high, while red flashing lights automatically signal a wave-off, meaning that the pilot cannot land at that time. When landing, a plane catches an arresting cable using its tailhook, a hook bolted to an 8-foot (2.4 m) bar attached to the rear part of the aircraft. The tailhook can bring a plane from a speed of 150 miles an hour (241.4 klph) to a complete stop within just 320 feet (97.5 m).

Primary Flight Control, or "Pri-Fly," is the control tower for flights. Above it on the "island," the part of the carrier that sticks up above the flight deck, is the bridge, the command and control center of the carrier as a whole. On the bridge is always an officer of the deck (OOD), designated by the ship's commanding officer, who serves a four-hour watch. The OOD is responsible for all facets of the safety and operation of the ship, among which are navigation, ship handling, communications, and routine tests, and inspections. Also on the bridge are the helmsman, who steers the ship, and numerous other personnel.

Powered by two nuclear reactors with four geared steam turbines and four shafts, the Nimitz-class carrier is capable of spending at least half a year at sea, and more than a decade without refueling. Its ship's company exceeds 3,000, with almost 2,500 more on the air wing. Below decks is an entire city, complete with vast warrens of living spaces, dining halls that serve nearly 20,000 meals a day, a radio and television station, a barber shop, a library, gymnasium, a hospital and dentist office, shops, and a post office.

Evolution of the Carrier

At 11:01 a.m. on January 18, 1911, the U.S. Navy's Eugene Ely landed a Curtiss pusher aircraft on a specially built platform aboard the USS *Pennsylvania.* Thus, was born the concept of the aircraft carrier. On March 20, 1922, the Navy commissioned the *Langley,* its first carrier, built from a converted collier called the *Jupiter.* Later that year, as a result of the 1922 Washington Naval Limitation Treaty, which limited battleship inventories, Congress authorized the conversion of the unfinished battleships *Lexington* and *Saratoga.* In June 1934, the *Ranger,* the first ship built as an aircraft carrier, was commissioned.

During the interwar period, the aircraft carrier benefited from a number of innovations, most of them British in origin. For example, the Royal Navy introduced the idea of arresting wire (originally necessary because the flimsy World War I-era planes might blow overboard), as well as elevator lifts for stowing craft. Later innovations in catapults and landing lights would also come from the United Kingdom. The British and Americans were not the only forces building aircraft carriers; like the Americans, the Japanese, who had signed the Washington naval agreement, converted unfinished battleships to carriers.

Carriers figured heavily in World War II, particularly during operations in the Pacific theatre. The Japanese launched their attack on U.S. forces at Pearl Harbor in December, 1941, from carriers, and in May, 1942, the United States struck back decisively in the Battle of the Coral Sea, the first naval battle in which opposing fleets fought without their ships coming in sight of one another. A month later, the Battle of Midway proved one of the turning points in the war, and reinforced the concept of naval air support.

Postwar changes. By the end of World War II, the United States had commissioned more than 34 carriers, with several more made operational late in 1945. But it had also lost several such vessels, including the first two, the *Langley* and the *Lexington.* Following the war, the introduction of guided missiles revolutionized the nature of the carrier battle group, while nuclear fission replaced diesel power for the most advanced carriers.

Several British innovations—the angled landing strip, which made it possible for a jet to land far from parked aircraft, as well as the mirrored landing site and steam catapults—made it possible to build carriers capable of launching powerful aircraft and managing complex air missions. But as the Cold War progressed, it became clear that only extraordinary carriers could support the vessels' emerging threefold purpose: to deliver air strikes against targets on sea and land; to protect other ships at long range; and to support antisubmarine operations through their battle groups. Only a true world power could afford to build carriers big enough to perform all three tasks—a distinction that, in effect, separated the United States from the rest of the world.

With the launch of its 59th carrier, *Forrestal,* in 1959, the United States introduced the era of the very large carrier. The *Forrestal* included rectangular extensions on the rear part of the flight deck, which greatly expanded the deck area. Designers had also moved the elevators off to the side, so that they could be used even as aircraft were taking off and landing.

Two years later, in 1961, the Navy introduced the first nuclear-powered carrier, the *Enterprise.* It is no accident that the world's most well-known fictional spaceship, from the 1960s television show *Star Trek,* was also called the *Enterprise.* During that era, the standard of excellence among carriers—the epitomy of technological superiority anyone was likely to encounter in real life—was the *Enterprise,* which carried 100 aircraft, displaced 75,700 tons (68,674 tonnes), and moved at speeds higher than 30 knots (55.6 kph). With eight nuclear reactors, it could travel for three years before being replaced.

As impressive as it was, the *Enterprise* would be eclipsed by the *Nimitz* (commissioned in May 1975) and the rest of its class. Instead of eight reactors, these required only two, whose uranium cores needed to be replaced once every 13 years. The carriers displaced 81,600 tons, but had much smaller propulsion systems, and thus, could store much more aircraft fuel.

As of 2003, the United States had launched a total of 75 carriers, with two more under construction. Its 12 active carriers included the *Enterprise* and the *Kitty Hawk* class (the *Kitty Hawk* and *Constellation*), all launched in 1961; the *John F. Kennedy,* launched in 1968; and eight carriers of the Nimitz class: *Nimitz, Dwight D. Eisenhower* (1977), *Carl Vinson* (1982), *Theodore Roosevelt* (1986), *Abraham Lincoln* (1989), *George Washington* (1992), *John C. Stennis* (1995), and *Harry S. Truman* (1998). Additionally, the *Ronald Reagan* was under construction, with launch planned for the middle of the decade, while construction was to begin on the *George H. W. Bush,* with completion planned for 2009. (Both are Nimitz-class carriers.)

Other nations and light carriers. The United States has decommissioned about as many carriers—63—as the rest of the world had afloat in 2003. Nations with carriers included the United Kingdom, France, Russia, China, Italy, Japan, Spain, India, Brazil, Chile, Peru, China, and Thailand. The leading carrier power, other than the United States, was—not surprisingly, given the many previous

British achievements in carrier design—the United Kingdom. In part to facilitate the building of smaller and more economical carriers, the British in the late 1960s developed the Harrier jet, which takes off almost vertically. As of 2003, its fleet included three small carriers of the *Invincible* class, built for vertical/short takeoff and landing (V/STOL), each capable of carrying eight Harriers and from 10 to 12 helicopters.

France built the *Charles de Gaulle,* a nuclear-powered vessel that could carry 40 planes, as well as the *Jeanne d'Arc* helicopter carrier. The latter type of ship, midway of a carrier and a cruiser, provided a means of giving several nations carrier capabilities. Such was the case with the Russian Federation, which had a large helicopter carrier, the *Gorshkov,* along with a semi-active multi-role carrier, the *Kutznetsov.* As the Soviet Union, Russia was slow to develop carriers, in part because it lacked sufficient ports worldwide. By the late 1960s, however, the Soviets had begun to build aviation cruisers of the *Moskva* class. These have all been decommissioned since then, however. The world's other superpower, China, has a small naval carrier force, consisting primarily of the *Shichang* multi-role support ship.

Other notable naval powers include Italy, which had six carriers, helicopter carriers, or amphibious assault ships either in operation or under construction in 2003. These included the *Andrea Doria,* scheduled for completion in 2007. Built along the V/STOL model, the *Andrea Doria* would hold eight Harriers or 12 helicopters. Other navies with aircraft carriers, helicopter carriers, helicopter destroyers, or amphibious assault ships included Japan, Brazil, India, Spain, Thailand, and Peru.

FURTHER READING:

BOOKS:

Clancy, Tom. *Carrier: A Guided Tour of an Aircraft Carrier.* New York: Berkley Books, 1999.

Kaufman, Yogi. *City at Sea.* Annapolis, MD: Naval Institute Press, 1995.

Musciano, Walter A. *Warbirds of the Sea: A History of Aircraft Carriers and Carrier-Based Aircraft.* Atglen, PA: Schiffer Publishing, 1994.

Polmar, Norman. *The Naval Institute Guide to the Ships and Aircraft of the U.S. Fleet.* Annapolis, MD: Naval Institute Press, 1993.

Preston, Anthony. *Carriers.* New York: Gallery Books, 1993.

Wooldridge, E. T. *Carrier Warfare in the Pacific: An Oral History Collection.* Washington, D.C.: Smithsonian Institution Press, 1993.

ELECTRONIC:

Haze Gray and Underway World Aircraft Carrier Lists. <http://www.hazegray.org/navhist/carriers/> (April 13, 2003).

U.S. Navy—The Aircraft Carriers. U.S. Navy Office of Information. <http://www.chinfo.navy.mil/navpalib/ships/carriers/> (April 13, 2003).

SEE ALSO

Aviation Intelligence, History
E-2C
Libya, U.S. Attack (1986)
National Command Authority
Persian Gulf War
World War I
World War II

Airline Security

ADRIENNE WILMOTH LERNER

Following the September 11 terrorist attacks on the United States, airline and airport security reform was a key aspect of international anti-terrorist efforts. Although some nations, such as Great Britain and Israel, had created strong passenger and luggage screening protocols before 2001, there were few international standards for airport security. Concern about the possible future use of airplanes in terrorist attacks and hijacking events provoked widespread changes in United States airport security and passenger screening operations.

United States Aviation and Transportation Security Act

On November 18 and 19, 2001, the United States Congress passed the Airport Security Federalization Act and the Aviation and Transportation Security Act. The laws sought to standardize pre-flight passenger and cargo screening by federalizing security service and screening personnel in the nation's airports. The Aviation and Transportation Security Act created the Federal Transportation Security Administration (TSA) to supervise security operations for sea and air transportation. The TSA hires and trains Federal airport screeners, who under the new law must all be American citizens. Though the acts govern only United States airports, many of the new initiatives and procedures outlined in the legislation have been routine in many foreign airports for several years.

The Aviation and Transportation Security Act also prescribed several fundamental changes in screening and flight protocol beyond the federalization of personnel. As of December 31, 2002, bomb detection devices, which can detect explosive residue, must screen checked baggage. CT Scanning devices and increased hand searching of luggage were among other encouraged reforms.

Passenger screening also increased in scope and effectiveness. Access to airport departure and arrival gates and concourses is now restricted to ticketed passengers.

The renovated American Airlines security checkpoint, part of a $300 million improvement project, is seen in the American Airlines Terminal 4 of the Los Angeles International Airport. AP/WIDE WORLD PHOTOS.

In addition to the metal detectors already in place in many airports, more careful checks of electronic devices, such as laptop computers and cellular phones, and carry-on luggage, became standard. The Computer Assisted Passenger Prescreening System, a data base system used in conjunction with the Advance Passenger Information System (APIS), provides searchable biographical and security information on air travelers.

New security measures included modifications to aircraft. Fortified cockpit doors, required to remain closed during flight, prevent easy access from the cabin to the cockpit. Pilots and flight crew can now monitor the aircraft cabin with video monitors and recording devices. The Department of Transportation further requires all planes and passenger trains to be equipped with emergency notification systems that are capable of communicating with airport, national, and local "911" emergency services.

Airports themselves are now required to be secured areas. Fences prevent unauthorized entry onto runways and staging areas. Automobiles cannot be left unattended within 300 yards of the airport terminal. Since the September 11, 2001, terrorist attacks on the United States, the number of security personnel and law enforcement officers on duty in the nation's airports has increased. Some special security details employ K-9 units with chemical and bomb sniffing dogs.

The new screening process. Airport security reform mandated several procedural changes that are evident to travelers. Items that were once commonly allowed in carry-on luggage, such as razors and scissors, are now banned in luggage that will be stored in the cabin of a plane. Airports and airlines in the United States now employ a more stringent pre-flight screening process for passengers, as well as luggage.

The first step in the new screening process is to establish, and positively confirm, the identity of the traveler. Travelers must furnish identification that matches itineraries or tickets. If a passenger is traveling to a foreign destination, airlines and security personnel conduct an unseen screening of passengers via the Advance Passenger Information System (APIS), a database that stores biographical information on airline travelers.

After checking-in with the airline, the passenger, and any carry-on luggage, is required to go through a detailed, physical screening. Identification is checked and confirmed for a second time. Travelers must pass successfully through

pulse induction standing or wand metal detectors, while x-ray machines screen baggage. Electronic devices, such as cellular phones, laptop computers, and personal digital assistants (PDAs), are all required to be turned on and shown to security personnel for inspection, or taken out of luggage and screened separately by x-ray. Advanced x-ray machines that transmit images in three colors permit federal screeners to identify organic, inorganic, and metal, items inside of a traveler's baggage. If security personnel are unable to clearly define the contents of a piece of luggage, or suspect prohibited items, then they open the luggage and conduct a hand search. Only passengers and luggage that successfully pass inspection are permitted to proceed to airline departure gates.

Once at the departure gate, airline personnel are required to conduct random security searches as passengers board the plane. These searches are usually brief, but thorough, and involve a hand search of the contents of carry-on luggage. Some passengers are also asked to answer questions regarding their travel plans. These pre-flight searches have received criticism from some who claim that racial and ethnic profiling is the predominant factor in choosing which passengers to search. Others have claimed that the pre-flight screening violates privacy and causes fear with other passengers because the searches are performed in plain sight of fellow travelers. Proponents of the random pre-flight searches assert that they are indeed, random, unless a traveler is flagged by APIS.

As a passenger boards the plane, machines scan boarding cards in order to compile a final passenger manifest. Airline cabin or ground crew then transmits the passenger list to federal aviation and individual airline officials. During the boarding process, passenger identification is sometimes checked for a third and final time.

Baggage that the passenger surrenders to the airline for storage in the cargo hold during flight, or checked baggage, undergoes a different screening process, separate of the passenger. First, baggage is matched to its owning traveler. If the passenger does not board the flight, then the baggage is not loaded onto the plane. This is more easily accomplished with the use of printed, individual, barcode tags affixed to luggage.

Checked baggage screening is geared around the detection of explosive or incendiary devices. X ray machines or computer tomography (CT) scanners screen the content of baggage. CT scanners permit a bag to be x-rayed individually, yet efficiently, and from all sides. The screener also calculates the density and mass of objects within the luggage, checking the data with a database of known mass/densities of dangerous or explosive substances. CT scanners are slower than standard palate x-ray systems that survey several bags at a time, however their screening is more thorough.

The future of airline security. Despite general acceptance of most airline and airport security reforms, some programs remain controversial. Some have criticized the incorporation of law enforcement profiling techniques into routine passenger screening practices, claiming that persons of Middle Eastern ethnicity are more often under suspicion, searched, and detained by security personnel.

The controversy surrounding profiling escalated when officials in the Department of Homeland Security and the Department of Defense proposed the introduction of the Total Information Awareness (TIA) system, a searchable database that stores personal information including financial and medical records. Though the TIA was intended to be used by federal law enforcement officials to collate data and find terrorist networks, Congress severely circumscribed the controversial program in 2003, prohibiting its use for domestic security operations. TIA was later renamed the Terrorist Information Awareness system

With the creation of the United States Department of Homeland Security (DHS), many agencies responsible for airline safety and airport security, including the TSA, were assumed into the new government department. The DHS has combined national anti-terrorist efforts with earlier regulations specifically regarding airports and airlines. The incorporation of the Early Alert System, a color-coded warning system meant to indicate the variable likelihood of terrorist attacks, marked the most notable change in security procedures. As threat levels are elevated, security procedures are heightened. At the Orange and Red levels, airports employ a wider secured perimeter, different flight paths around urban areas, and increased security personnel.

Although TSA is now a part of the Department of Homeland Security, the Department of Transportation and the Federal Aviation Administration (FAA) continue to aid the progress of reforming United States airline security policy through safety recommendations and review of airline practices.

■ FURTHER READING:

ELECTRONIC:

Transportation Safety Administration. <http://129.33.119.130/public/index.jsp> (12 March 2003).

United States Department of the Treasury. U.S. Customs Service. <http://www.customs.ustreas.gov/>(05 January 2003).

SEE ALSO

Air Marshals, United States
APIS (Advance Passenger Information System)
Canada, Counter-terrorism Policy
France, Counter-terrorism Policy
Germany, Counter-terrorism Policy
Israel, Counter-terrorism Policy
September 11 Terrorist Attacks on the United States
United Kingdom, Counter-terrorism Policy
United States, Counter-terrorism Policy

Al-Aqsa Martyrs Brigade

The al-Aqsa Martyrs Brigade comprises an unknown number of small cells of Fatah-affiliated activists that emerged at the outset of the current intifadah to attack Israeli targets. It aims to drive the Israeli military and settlers from the West Bank, Gaza Strip, and Jerusalem and to establish a Palestinian state.

Organization activities. Al-Aqsa Martyrs Brigade has carried out shootings and suicide operations against Israeli military personnel and civilians and has killed Palestinians that it believed were collaborating with Israel. At least five United States citizens, four of them dual Israeli-U.S. citizens, were killed in these attacks. Intelligence reports claim the group probably did not target U.S. citizens during these attacks. In January 2002, the group claimed responsibility for the first suicide bombing carried out by a female.

The strength of the Al-Aqsa Martyrs Brigade is unknown, and operates mainly in the West Bank and has claimed attacks inside Israel and the Gaza Strip.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Alex Boncayao Brigade (ABB)

The Alex Boncayao Brigade (ABB), the breakaway urban hit squad of the Communist Party of the Philippines New People's Army, was formed in the mid-1980s. The ABB was added to the Terrorist Exclusion list in December 2001. The AAB is responsible for more than 100 murders and believed to have been involved in the murder in 1989 of U.S. Army Col. James Rowe in the Philippines. In March, 1997, the group announced it had formed an alliance with another armed group, the Revolutionary Proletarian Army (RPA). In March, 2000, the group claimed credit for a rifle grenade attack against the Department of Energy building in Manila and strafed Shell Oil offices in the central Philippines to protest rising oil prices. ABB has approximately 500 members and the largest RPA/ABB groups are on the Philippine islands of Luzon, Negros, and the Visayas.

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Al-Gama'a al-Islamiyya (Islamic Group, IG)

Al-Gama'a al-Islamiyya (Islamic Group, IG) is Egypt's largest militant group, active since the late 1970s, and appears to be loosely organized. IG has an external wing with supporters in several countries worldwide. The group issued a cease-fire in March 1999, but its spiritual leader, Shaykh Umar Abd al-Rahman, sentenced to life in prison in January, 1996, for his involvement in the 1993 World Trade Center bombing and incarcerated in the United States, rescinded his support for the cease-fire in June, 2000. IG has not conducted an attack inside Egypt since August, 1998. Senior members signed Osama Bin Ladin's fatwa in February, 1998, calling for attacks against the

United States. The organization is unofficially split in two factions, one that supports the cease-fire led by Mustafa Hamza and one led by Rifa'i Taha Musa, calling for a return to armed operations. Taha Musa in early 2001 published a book in which he attempted to justify terrorist attacks that would cause mass casualties. Musa disappeared several months thereafter, and there were conflicting reports as to his current whereabouts. The primary goal of the IG is to overthrow the Egyptian government and replace it with an Islamic state, but disaffected IG members, such as those potentially inspired by Taha Musa or Abd al-Rahman, may be interested in carrying out attacks against the U.S. and Israeli interests.

Organization activities. The IG has conducted armed attacks against Egyptian security and other government officials, Coptic Christians, and Egyptian opponents of Islamic extremism before the cease-fire. From 1993 until the cease-fire, al-Gama'a launched attacks on tourists in Egypt, most notably the attack in November, 1997, at Luxor that killed 58 foreign tourists. The IG also claimed responsibility for the attempt in June, 1995, to assassinate Egyptian President Hosni Mubarak in Addis Ababa, Ethiopia. The IG has never specifically attacked a U.S. citizen or facility, but has threatened United States interests.

At its peak, the IG probably commanded several thousand hard-core members and a like number of sympathizers, but its present size is unknown. The 1999 cease-fire and security crackdowns following the attack in Luxor in 1997, and more recently, tightened security efforts following the September 11, 2001, terrorist attacks in the United States probably have resulted in a substantial decrease in the group's numbers.

IG operates mainly in the Al-Minya, Asyu't, Qina, and Sohaj Governorates of southern Egypt. They also appear to have support in Cairo, Alexandria, and other urban locations, particularly among unemployed graduates and students, and have a worldwide presence, including the United Kingdom, Afghanistan, Yemen, and Austria.

The oragnization's external sources of support, if any, are unknown. The Egyptian government believes that Iran, Osama Bin Ladin, and Afghan militant groups support the organization. The IG may also obtain some funding through various Islamic non-governmental organizations.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Al-Ittihad al-Islami (AIAI)

Al-Ittihad al-Islami (AIAI) also operates as, or is known as, the Islamic Union.

AIAI is Somalia's largest militant Islamic organization. AIAI rose to power in the early 1990s following the collapse of the Siad Barre regime. AIAI aims to establish an Islamic regime in Somalia and force the secession of the Ogeden region of Ethiopia. AIAI participates in primarily insurgent-style attacks against Ethiopian forces and other Somali factions. The group is believed to be responsible for a series of bomb attacks in public places in Addis Ababa in 1996 and 1997, as well as the kidnapping of several relief workers in 1998. AIAI sponsors Islamic social programs, such as orphanages and schools, and provides pockets of security in Somalia. AIAI strength is estimated at some 2,000 members, plus additional reserve militias.

The AIAI operates primarily in Somalia, with limited presence in Ethiopia and Kenya. AIAI has received funds from Middle East financiers, Western diaspora remittances, weapons deliveries from Sudan, and—prior to Operation Enduring Freedom—conducted training in Afghanistan with ties to al-Qaeda (also spelled al-Qaida).

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins

Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya

Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya also operates as, or is known as, the Libyan Islamic Fighting Group, Fighting Islamic Group, Libyan Fighting Group, and/or Libyan Islamic Group.

Emerged in 1995 among Libyans who had fought against Soviet forces in Afghanistan, the organization declared the government of Libyan leader Muammar Qadhafi un-Islamic and pledged to overthrow it. Some members maintain a strictly anti-Qadhafi focus and organize against Libyan government interests, but others are aligned with Osama Bin Laden's al-Qaeda (also frequently spelled al-Qaida) organization or are active in the international mujahidin network. Al-Jama'a claimed responsibility for a failed assassination attempt against Qadhafi in 1996 and engaged Libyan security forces in armed clashes during the mid to late 1990s. Currently, the organization engages in few armed attacks against Libyan interests either in Libya or abroad.

Al-Jama'a, operates in Libya, but since late 1990s many members have fled to various Middle Eastern and European countries. The group obtains some funding through private donations, various Islamic non-governmental organizations, and criminal acts.

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins

Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Al-Jihad

Al-Jihad (also known as Egyptian Islamic Jihad, Jihad Group, and Islamic Jihad) is an Egyptian Islamic extremist group active since the late 1970s. Al-Jihad merged with Osama Bin Ladin's al-Qaida organization in June, 2001, but may retain some capability to conduct independent operations. Al-Jihad continues to suffer setbacks worldwide, especially after tightened Egyptian security in the aftermath of the September 11, 2001 terrorist attacks in the United States. Al-Jihad's primary goals are to overthrow the Egyptian government and replace it with an Islamic state, and to attack U.S. and Israeli interests in Egypt and abroad.

Organization activities. Al-Jihad specializes in armed attacks against high-level Egyptian government personnel, including cabinet ministers, and car-bombings against official U.S. and Egyptian facilities. The original Jihad was responsible for the assassination in 1981 of Egyptian President Anwar Sadat. The organization claimed responsibility for the attempted assassinations of Interior Minister Hassan al-Alfi in August 1993 and Prime Minister Atef Sedky in November 1993. As of May, 2002, Al-Jihad has not conducted an attack inside Egypt since 1993 and has never targeted foreign tourists there. Al-Jihad is responsible for the Egyptian embassy bombing in Islamabad in 1995; in 1998 an Al-Jihad attack against U.S. Embassy in Albania was thwarted.

The actual size of Al-Jihad is unknown, but the organization has at least several hundred hardcore members. Al-Jihad operates in the Cairo area, but most of its network is outside Egypt, including Yemen, Afghanistan, Pakistan, Lebanon, and the United Kingdom, and its activities have been centered outside Egypt for several years.

The Egyptian government claims that Iran supports Al-Jihad. Its merger with al-Qaeda also boosts Osama Bin Ladin's support for the group. Al-Jihad also may obtain some funding through various Islamic non-governmental organizations, cover businesses, and criminal acts.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Allied Democratic Forces (ADF)

The Allied Democratic Forces (ADF) is a diverse coalition of a few hundred fighters from the National Army for the Liberation of Uganda (NALU), Islamists from the Salaf Tabliq group, Hutu militiamen, and fighters from ousted regimes in Congo. The conglomeration of fighters formed in 1995 in opposition to the government of Ugandan President Yoweri Museveni. The ADF seeks to use the kidnapping and murder of civilians to create fear in the local population and undermine confidence in the government. The group is suspected to be responsible for dozens of bombings in public areas. A Ugandan military offensive in 2000 destroyed several ADF camps, but ADF attacks continued in Kampala in 2001.

ADF operates in western Uganda and eastern Congo. ADF has received funding, supplies, and training from the government of Sudan and perhaps from sympathetic Hutu groups.

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Al-Qaeda (also known as Al-Qaida)

Responsible for the September 11, 2001, terrorist attacks upon the United States, Al-Qaeda (also known as Al-Qaida) was established by Osama bin Ladin (also spelled Usama Bin Ladin or Osama bin Laden) in the late 1980s to bring together Arabs who fought in Afghanistan against the Soviet Union. Al-Qaeda helped finance, recruit, transport, and train Sunni Islamic extremists for the Afghan resistance. Al-Qaeda's current goal is to establish a pan-Islamic Caliphate by working with allied Islamic extremist groups to overthrow regimes it deems "non-Islamic" and expelling Westerners and non-Muslims from Muslim countries. Al-Qaeda has issued statement under banner of "The World Islamic Front for Jihad against the Jews and Crusaders" in February 1998, saying it was the duty of all Muslims to kill U.S. citizens—civilian or military—and their allies anywhere in the world. The World Islamic Front for Jihad merged with Egyptian Islamic Jihad (Al-Jihad) in June 2001.

Organization activities. On September 11, 2001, 19 al-Qaeda suicide attackers hijacked and crashed four U.S. commercial jets, two into the World Trade Center in New York City, one into the Pentagon near Washington, D.C., and a fourth into a field in Shanksville, Pennsylvania, leaving about 3,000 individuals dead or missing. Al-Qaeda also directed the October, 12, 2000 attack on the U.S.S. *Cole* in the port of Aden, Yemen, killing 17 U.S. Navy crewmembers, and injuring another 39. Al-Qaeda also admitted responsibility for the bombings in August 1998 of the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, that killed at least 301 individuals and injured more than 5,000 others. Al-Qaeda claims to have shot down U.S. helicopters and killed U.S. servicemen in Somalia in 1993 and to have conducted three bombings that targeted U.S. troops in Aden, Yemen, in December 1992.

Al-Qaeda is linked to unrealized plans to assassinate Pope John Paul II during his visit to Manila in late 1994; a plan to kill President Clinton during a visit to the Philippines in early 1995; the planned midair bombing of a dozen U.S. trans-Pacific flights in 1995; and plans to set off a bomb at Los Angeles International Airport in 1999. They

An Air Force RQ-1 Predator pilotless aircraft, capable of launching Hellfire air-to-ground missiles in CIA operations similar to the pin-point missile strike that killed Qaed Salim Sinan al-Harethi, a top al-Qaeda operative, in Yemen on November 4, 2002. AP/WIDE WORLD PHOTOS.

also plotted to carry out terrorist operations against U.S. and Israeli tourists visiting Jordan for millennial celebrations in late 1999. (Jordanian authorities thwarted the planned attacks and put 28 suspects on trial.) In December, 2001, suspected al-Qaeda associate Richard Colvin Reid attempted to ignite a shoe bomb on a transatlantic flight from Paris to Miami.

Al-Qaeda may have several thousand members and associates in cells located around the world, and also serves as a focal point or umbrella organization for a worldwide network that includes many Sunni Islamic extremist groups, some members of al-Gama'a al-Islamiyya, the Islamic Movement of Uzbekistan, and the Harakat ul-Mujahidin.

Al-Qaeda has cells worldwide and is reinforced by its ties to Sunni extremist networks. Coalition attacks on Afghanistan since October 2001 have dismantled the Taliban—once al-Qaeda's protectors—and led to the capture, death, or dispersal of al-Qaeda operatives. Al-Qaeda members at large, including as of April 2003, Osama bin Ladin, have vowed to attempt to carry out future attacks against U.S. interests.

Bin Ladin, member of a billionaire family that owns the Bin Ladin Group construction empire, is said to have inherited tens of millions of dollars that he uses to help finance the group. Al-Qaeda also maintains moneymaking front businesses, solicits donations from like-minded supporters, and illicitly siphons funds from donations to Muslim charitable organizations. U.S. efforts to block al-Qaeda funding has hampered their ability to obtain money.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations

Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Americas, Modern U.S. Security Policy and Interventions

JUDSON KNIGHT

In 1823, the Monroe Doctrine provided a framework for United States security policy in the Americas by declaring the Western Hemisphere under a U.S. "sphere of influence". This served to warn away European colonial powers, while providing justification for U.S. intervention in the affairs of nations throughout Central and South America and the Caribbean. The Monroe Doctrine, along with other statements of policy by modern U.S. presidents, served as a basis for actions against Communist influence in Cuba, Nicaragua, Grenada, and other countries. As the Cold War drew to a close, U.S. action in Latin America, including the invasion of Panama in December 1989, tended to focus on anti-drug activities.

U.S. Policy and Interventions, 1823–1946

President James Monroe issued his famous doctrine in a speech before Congress. In response to rumors of a planned Franco-Spanish action to restore Spain's empire in the New World, Britain had made overtures to the United States for a joint policy opposing international intervention in the Americas. Former presidents Thomas Jefferson and James Madison urged Monroe to accept the British offer. However, Monroe's secretary of state, future president John Quincy Adams, advised him instead to make a unilateral statement of U.S. interests in the Americas—interests so great that outside intervention would meet with swift military action.

The Monroe Doctrine was to be a basis for a range of activities, from direct military intervention to support of friendly regimes, and from protection of Latin American nations against European aggression to humanitarian assistance for the peoples of Latin American countries. It was also the basis for American isolationism with regard to events overseas. Significantly, the United States, whose first international action was against Libyan pirates during Jefferson's administration, would not again be involved in overseas military activity until the Spanish-American War of 1898—itself fought primarily over Cuba and Puerto Rico. Even in 1917, the nation entered World War I partly on the basis of information that Germany intended to foment an attack against the United States through Mexico.

Mexico was the target of the first U.S. military action in the Americas, whereby the nation acquired much of what is now the southwestern United States in 1846. During the 1850s, the United States intervened repeatedly in Nicaragua, which U.S. adventurer William Walker ruled as a private colony for two years. The 1855–57 occupation by mercenaries under Walker, who was from Tennessee, later sparked southern hopes of a Confederate empire in Latin America.

Following the Spanish-American War, the United States gave Cuba its independence, but included in the Cuban constitution the Platt Amendment (1901), whereby it reserved the right to intervene in Cuba. In 1903, Washington backed the revolt of Panama against Colombia, which enabled the United States to begin building the Panama Canal. The years from 1904 to 1945 saw literally dozens of covert or military interventions in Cuba, the Dominican Republic, Guatemala, Haiti, Honduras, Mexico, Nicaragua, and Panama. These involved protection of U.S. facilities and personnel, U.S. businesses such as the United Fruit Company in Guatemala, and pro-American governments.

Particularly notable was the action against Mexican guerrilla leader Pancho Villa, whose 1916 raid on the city of Columbus, New Mexico, killed 17 Americans, the greatest loss of civilian life due to foreign action on U.S. soil between 1812 and 2001. American troops, led by General John Pershing, pursued Villa, but failed to catch up with him before they were diverted to Europe.

U.S. forces repeatedly intervened in Nicaragua to shore up pro-American governments, and, in 1926, to fight back a putative Bolshevik conspiracy. This was the leftist nationalist movement of Augusto César Sandino, whose name a later generation of guerrillas would adopt for their movement. The United States in 1929 created a military academy to train Nicaragua's National Guard, under the leadership of Anastazio Somoza García. In 1934, Somoza had Sandino assassinated, and in 1936, he assumed the presidency. His family would control the nation until the Sandinistas took power in the late 1970s.

As these events were taking place in Nicaragua, the United States was intervening in another nation destined to become communist, Cuba. In 1933, President Franklin D. Roosevelt sent warships to quell unrest, and ultimately helped install the government of Fulgencio Batista. A year later, the Platt Amendment was repealed. Batista would rule until 1959, when he was overthrown by Fidel Castro.

In the intervening years, the United States sought to keep Axis and Communist influence out of Latin America. Its opposition to outside invaders influenced support of military leaders, who tended to establish more stable, if less popular, regimes than did liberal democrats. The United States supported the creation of National Guard-style forces in Haiti and the Dominican Republic, and in

1946, established the U.S. Army School of the Americas in Panama. The school, which would provide military training to a generation of leaders, taught its students that the chief threat to a nation is internal subversion—i.e., leftist revolts.

U.S. Policy and Interventions, 1946–81

When the leftist regime of President Jacobo Arbenz Guzman seized control of United Fruit properties in Guatemala in 1954, the U.S. Central Intelligence Agency (CIA) began activities against him, training opposition forces in Honduras. Arbenz's purchase of arms from Czechoslovakia only heightened U.S. fears of Communist subversion. The CIA-backed paramilitary force overthrew his regime, replacing him with Carlos Castilla Armas, a leader more favorable to U.S. interests.

Such actions won the United States little support, but Washington's principal desires for the Americas were stability and protection of U.S. economic and strategic interests. If the United States could achieve this by supporting democratic movements and opposing dictatorships, it would, as it did when the administration of Ronald Reagan backed Jose Napoleon Duarte in El Salvador during the 1980s, or when that of George Bush deposed Manuel Noriega in Panama in 1989.

More often than not, however, military leaders—even those who seized power by coups—tended best to serve U.S. needs. President-elect John F. Kennedy articulated this fact in 1960, after right-wing forces seized power in El Salvador, when he noted that "Governments of the civil-military type of El Salvador are the most effective in containing communist penetration in Latin America."

Castro and Cuba. Castro's assumption of power in Cuba presented Washington with a nightmarish scenario. Not only was it presented with a pro-Moscow regime just 90 miles from Miami, but Castro—despite his unfailing support for Soviet policy—managed to position himself as a freedom-loving nationalist rather than a communist. Furthermore, he was a charismatic figure, who has continued to enjoy strong support among some U.S. intellectuals and entertainers.

In 1960, President Dwight D. Eisenhower authorized the CIA to undertake covert actions against Castro. Much of what followed, courtesy of a predecessor to the agency's Directorate of Science and Technology, ventured into the territory of the ridiculous: exploding cigars, poisoned milkshakes, powder that would cause the dictator's famous beard to fall off. In April, 1961, the United States sent in a force of 1,400 anti-Castro Cubans, who landed at Cuba's Bahía de los Cochinos, or Bay of Pigs. The venture turned into a rout, and gave Castro a huge public-relations victory.

A Soviet missile buildup in Cuba in October, 1962, prompted the Cuban Missile Crisis, bringing the United States close to nuclear war with the Soviet Union. The incident highlighted the degree to which Castro was a thorn in Washington's side, and throughout the 1960s, the United States conducted covert sabotage campaigns against Castro. It also maintained an economic embargo, and kept a close watch on Cuba from the naval base at Guantanamo Bay—a strategic piece of property retained by the United States when Cuba gained its independence decades earlier.

Dominican Republic, Chile, and the Panama Canal. From the 1960s to the 1980s, the United States opposed communist and pro-communist movements in several countries. President Lyndon B. Johnson, claiming threatened communist subversion, invaded the Dominican Republic in 1965. In Chile in 1973, the administration of President Richard M. Nixon, operating through the CIA, supported a coup led by the right-wing General Augusto Pinochet against the Marxist president, Salvador Allende. Allende died, either by suicide (according to Pinochet) or by murder (according to Allende's supporters).

Like Castro, Pinochet imprisoned and tortured opponents, suppressed free speech, and maintained a strong military presence throughout the country. Unlike Cuba, however, Chile—on the brink of economic collapse under Allende—prospered under Pinochet, who imposed free-market reforms. Pinochet, who later submitted to free elections and was voted out of office, is one of the most oft-cited examples, both by critics and supporters of U.S. policy, of a U.S.-supported dictator in Latin America.

The administration of President James E. Carter sought to shift from the U.S. tradition of support for right-wing regimes, and cut off aid to the dictatorships in Guatemala and Nicaragua. Carter undertook negotiations to return the Panama Canal to Panama, and did not attempt to intervene when the Sandinistas removed a later Somoza from power and established a pro-Moscow regime in Nicaragua in 1979.

U.S. Policy and Interventions, 1981-Present

President Ronald Reagan reversed this trend. In October, 1983, he launched Operation Urgent Fury, the first significant U.S. military action since Vietnam, on the Caribbean island of Grenada. Grenada had become a pro-Soviet dictatorship in 1979—President Maurice Bishop even called his cabinet a "politburo"—but neither the Carter nor the Reagan administration sought to disrupt its government.

Tensions rose, however, when Cuban military personnel began building an airport capable of accommodating large Soviet bombers. In 1983, Bishop's minister of

defense launched a coup, killing Bishop and half the politburo, including the minister of education, who was pregnant. After the new dictator placed the entire island under house arrest, Reagan sent in the military to protect some 600 U.S. students and other citizens there.

El Salvador. Meanwhile, the Reagan administration had become involved in another tiny country, El Salvador, which was caught in a battle between the Marxist FMLN, the right-wing ARENA Party under Roberto d'Aubisson, and the Christian Democrats under Duarte. The FMLN enjoyed considerable support from U.S. leftists, who claimed that Washington was backing d'Aubisson.

Ironically, throughout the period from 1982 to 1984, the CIA was funneling money into efforts in favor of Duarte and against d'Aubisson. For example, when European journalists visited the country in 1983, the CIA provided them with negative information on the right-wing leader. Despite the fact that Washington backed the liberal regime, El Salvador remained fraught with problems, as rightist and leftist death squads battled over the country. In 1989, Duarte was voted out in favor of an ARENA candidate.

Nicaragua. The Reagan administration provided considerably more support for efforts against a regime openly aligned with the Kremlin: the Sandinistas in Nicaragua. U.S. actions in Nicaragua were closely tied with undertakings in neighboring countries, and one of Reagan's aims was to keep the Sandinistas from exporting their revolution. In this, he would be strongly opposed by congressional Democrats, and by U.S. intellectuals and entertainers, many of whom visited Nicaragua and proclaimed their support for the regime.

Beginning in 1981, the CIA began training a number of anti-Sandinista groups, collectively known as *Contras,* and sponsored the production of two training manuals, *Freedom Fighters Manual* and *Psychological Operations in Guerrilla Warfare.* When these manuals later became public, their contents prompted an outcry against CIA tactics, leading to an internal investigation.

The agency also conducted its own efforts against the regime in Managua, despite the Boland Amendment to the War Powers Act of 1973, passed by Congress in December 1982. Boland prevented the CIA or Department of Defense from using funds to overthrow the Nicaraguan government. In 1984, Congress passed a second Boland Amendment in response to the CIA mining of harbors on Nicaragua's Atlantic and Pacific coasts. In 1986, however, Congress appropriated $70 million in aid for the Contras. (The Boland Amendment was later repealed.)

At the same time, the Reagan administration and the CIA became involved in an effort to sell weapons to Iran, secure the release of hostages in Lebanon, and divert funds to the Contras. A pro-Syrian newspaper in Lebanon broke the story of Iran-Contra in November 1986, and for many months thereafter, the administration would be caught up in the scandal. Thanks to support for the Contras, combined with reductions in Soviet aid to the Sandinistas, the two sides signed a ceasefire agreement in 1987. The Contras agreed to free elections in February 1990, and these resulted in the election of Violeta Chamorro, a member of the liberal democratic opposition.

Panama and Haiti. Although opponents of U.S. policy in Latin America cite early CIA alliances with Noriega, for most of his career as Panamanian dictator, Noriega was openly opposed to the United States and closely aligned with Castro. He was also involved in drug trafficking, for which he was indicted by a Florida grand jury in February, 1988.

In 1989, President H. W. Bush invested $10 million in clandestine radio broadcasts against Noriega, and in December launched Operation Just Cause. The operation, which involved 27,000 U.S. troops, was at the time the largest U.S. military undertaking since Vietnam. Its stated goals were the protection of the Panama Canal and the 35,000 U.S. citizens living in Panama, as well as the removal of Noriega himself, promoting democracy, and bringing an end to drug activities in the country. The operation resulted in Noriega's capture and trial.

Less clear were the results of a military operation in Haiti, undertaken by the administration of William J. Clinton in 1994. The purpose was to restore President Jean-Bertrand Aristide, who had been deposed by a military coup, and in that regard, the operation was successful. However, political, economic, and social conditions on the troubled island continued to erode, and in March, 1999, the remaining U.S. forces departed the island amid continuing instability.

The war on drugs. From Reagan's time onward, the United States has been involved in the war on drugs to stop the flow of cocaine, marijuana, and other narcotics from Colombia, Peru, Bolivia, and other countries. The U.S. Drug Enforcement Administration (DEA) has been, and continues to be, involved in this war, as is the CIA. The CIA has undertaken cooperative efforts with the governments of Colombia and Peru to interdict drug traffickers. Part of this program is an airborne initiative whereby CIA and national air force personnel shoot down aircraft whose pilots refuse to identify themselves. In many regards, these efforts have been successful, and helped to reduce the flow of drugs; however, in April 2001, miscommunications resulted in the Peruvian shootdown of a plane carrying a U.S. missionary family. The mother and her seven-month-old daughter were killed.

In the post-Cold War environment, drug gangs are a much greater threat to stability in Latin America than are

revolutionaries, although these are often linked. With the elimination of support from Moscow, leftist groups such as Colombia's FARC rebels have turned to kidnapping Americans, Europeans, and Japanese, and holding them for ransom. The same was the case with Peru's Tupac Amaru, which held prisoners at the Japanese embassy in Lima for several months before Peruvian forces stormed the building in early 1997.

Many of these groups make common cause with drug cartels, and some are directly involved with the drug trade. Such was the case with Peru's Sendero Luminoso, or "Shining Path," which, with its Maoist ideology, never accepted aid from Moscow. Instead, it supported itself largely through cocaine trafficking. Sendero was largely neutralized with the capture of its leader, Abimael Guzman, in 1992. The early 1990s also saw the death of Colombian cocaine lord Pablo Escobar and the capture of his associate Carlos Lehder, as well as international terrorist Carlos "the Jackal" Ramirez.

FURTHER READING:

BOOKS:

Bouvier, Virginia Marie. *Whose America? The War of 1898 and the Battles to Define the Nation.* Westport, CT: Praeger, 2001.

Gilderhus, Mark T. *The Second Century: U.S.-Latin American Relations Since 1889.* Wilmington, DE: Scholarly Resources, 2000.

Hillman, Richard S., John A. Peeler, and Elsa Cardozo da Silva. *Democracy and Human Rights in Latin America.* Westport, CT: Praeger, 2002.

Musicant, Ivan. *The Banana Wars: A History of United States Military Intervention in Latin America from the Spanish-American War to the Invasion of Panama.* New York: Macmillan, 1990.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

Sicker, Martin. *The Geopolitics of Security in the Americas: Hemispheric Denial from Monroe to Clinton.* Westport, CT: Praeger, 2002.

Szumski, Bonnie. *Latin America and U.S. Foreign Policy: Opposing Viewpoints.* St. Paul, MN: Greenhaven Press, 1988.

SEE ALSO

Argentina, Intelligence and Security
Bay of Pigs
Brazil, Intelligence and Security
Bush Administration (1989–1993), United States National Security Policy
Chile, Intelligence and Security
Colombia, Intelligence and Security
Cuba, Intelligence and Security
Cuban Missile Crisis
Customs Service, United States
DEA (Drug Enforcement Administration)
Drug Control Policy, United States Office of National Drug Intelligence Estimates
El Salvador, Intelligence and Security
FBI (United States Federal Bureau of Investigation)
Guatemala, Intelligence and Security
International Narcotics and Law Enforcement Affairs (INL), United States Bureau
Kennedy Administration (1961–1963), United States National Security Policy
Mexico, Intelligence and Security
National Drug Threat Assessment
NDIC (Department of Justice National Drug Intelligence Center)
Nicaragua, Intelligence and Security
Panama Canal
Peru, Intelligence and Security
Reagan Administration (1981–1989), United States National Security Policy
Spanish-American War

Ames (Aldrich H.) Espionage Case

ADRIENNE WILMOTH LERNER

A 31-year veteran of the Central Intelligence Agency, Aldrich "Rick" Hazen Ames became famous in 1994 as the highest paid "mole" (double agent) in United States history. Ames made millions of (US) dollars for information he provided to the Soviet KGB, and later Russian intelligence, while a mid-level employee of the CIA. The information he sold to the KGB included the names of Russian double agents and operatives working for the U.S. within the Soviet intelligence community, ultimately leading to their capture, imprisonment, or execution by Soviet authorities. Ames was thus, one of the most destructive double agents to compromise the security of the United States intelligence services.

A decade after Ames was born in 1941, his father, a college professor, gained employment as a CIA analyst. Ames attended college at George Washington University, majoring in history. He began working for the CIA in 1959 while still a student, largely because of his father's position there.

Ames's performance throughout his career at the CIA was marked by mediocrity. He continued to be promoted, but never attained routine access to the highest level of classified materials. Ames made his first deal with the Soviets in April, 1985, selling CIA secrets for an initial payment of $50,000. Later that year, Ames was sent to Mexico City to recruit new agents. One of his first recruits was a woman with whom he was having an affair, Colombian cultural attaché Maria Del Rosario Casas. Ames married Casas later that year. She aided Ames in his illegal activities.

The CIA and FBI significantly delayed the detection of CIA turncoat Aldrich Ames, shown handcuffed, by failing for five years to mount a serious, joint investigation into their loss of Russian agents from 1956 to 1986. AP/WIDE WORLD PHOTOS.

The CIA transferred Ames to Rome in 1986, where he stayed until 1988 working for the CIA's Soviet Counterintelligence Division, at the same time selling secrets to the KGB. Although Ames's job was allegedly to recruit Soviet agents (from the embassy in Rome) into the CIA, he failed to successfully recruit a single Soviet agent. His work, however, provided him with the names of Soviet informants and it was this information he sold to the KGB. By 1989, after his return to the United States, he had made enough money to pay cash for a $540,000 home in Arlington, Virginia, an exclusive suburb of Washington, D.C., and another $100,000 for improvements on the house. He told friends and acquaintances he and his wife had inherited money from her family in Colombia.

In 1991, Ames was transferred to the CIA's Counternarcotics Division. Although he no longer had authorized access to information his Russian handlers might want, he managed to stay on the payroll by stealing computer files and other sensitive material.

The CIA had suspected the presence of a mole in the agency since 1986, when the first two of the Soviet agents Ames betrayed were executed. Suspicions grew with every execution and disappearance of Soviet agents in the late 1980s. The CIA was aware of Ames's extravagant spending as early as 1990. Ames passed inquiry lie-detector tests in 1986 and 1991. However, In 1993, a joint investigation between the Federal Bureau of Investigation and the CIA narrowed a list of 200 suspects down to fewer than 40, and then down to Aldrich Ames. In May, 1993, they launched project "Nightmover," a criminal investigation under the FBI's jurisdiction charged with gathering evidence against Ames.

Compiling enough evidence to arrest Ames and his wife on conspiracy charges took nearly a year. Over one hundred FBI agents, some of them elite members of the Special Services Group, tapped Ames's phone wires, rooted through his garbage, planted a wire in his Jaguar, installed a video camera across from his house, shadowed him disguised as trash collectors and lawn maintenance workers, and kept his home under nearly constant surveillance.

The big break in the case occurred in early September, 1993. Ames was overheard talking on his cell phone with his wife. The conversation included details about a pending deal with Russian agents. A few days later, he was seen near what was assumed to be the signal or dead drop site used by Ames and his Russian contacts. On September 15, the FBI found a note in Ames's garbage can indicating he was arranging a meeting for October. The FBI then obtained a warrant to enter Ames's house. While Ames and his family were away for a weekend in early October, the FBI searched his home, finding in his personal computer detailed information about drop sites and meeting places along with files of classified CIA information Ames had no business taking home. They followed him to Bogota where he was to meet with his handler, Yuri Karetkin, but failed to catch him in the act. Ames returned home $125,000 richer.

Nothing happened for four months. Ames appeared to be laying low. Finally, after detecting an unusual number of Russian intelligence officers lurking around Ames's neighborhood, the FBI became worried that the Russians had guessed Ames was under investigation. Ames was scheduled to go to Moscow and the FBI feared he might defect. The FBI decided to act, even though they had not been able to catch Ames actually meeting with his Russian handler. Aldrich and Rosario Ames were arrested on February 21, 1994, and charged with espionage. To prevent them from fleeing the country, the couple were held without bail.

The Ames espionage case, called a "calamity" by the Senate Intelligence Committee, remains one of the most remarkable cases of double-dealing in the history of the United States. The case is remarkable not only because Ames made so much money selling CIA secrets and because of the huge amount of information he sold, allegedly compromising over a hundred covert operations, but also because Ames remained undetected for so long. The case prompted an investigation by the Senate into counterintelligence procedures at the CIA and calls from Congress and the public for sweeping reform of the agency.

Following the Senate Intelligence Committee's report, some minor reforms were instituted to guard against the possibility of another security breech.

Ames was sentenced to life in prison without the possibility of parole. To gain leniency for his wife, Ames plead guilty to all charges levied against him.

FURTHER READING:

BOOKS:

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today.* M.Evans, 1997.

SEE ALSO

CIA (United States Central Intelligence Agency)
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*
Russia, Intelligence and Security
Hanssen (Robert) Espionage Case

Anthrax

BRIAN HOYLE

In the 1990s, the use of biological weapons by terrorists became a serious threat to the security of countries around the globe, and the United States in particular. During the Gulf War of 1990 to 1991, and in subsequent United Nations inspection efforts, the government of Iraq's development of advanced anthrax based bioweapons was revealed.

Although the incidents have not been directly linked, following the September 11, 2001 terrorist attacks on the World Trade Center buildings in New York City and the Pentagon in Washington, D.C., anthrax was used as a bioterrorist weapon. Letters containing a powdered form of *Bacillus anthracis*, the bacteria that causes anthrax, were mailed to representatives of government and the media, among others. Multiple attacks eventually killed five people.

Anthrax refers to a disease that is caused by the bacterium *Bacillus anthracis*. The bacterium can enter the body via a wound in the skin (cutaneous anthrax), via contaminated food or liquid (gastrointestinal anthrax), or can be inhaled (inhalation anthrax). The latter in particular can cause a very serious, even lethal, infection.

The disease has been present throughout recorded history. Its use as a weapon stretches back centuries. Hundreds of years ago, bodies of anthrax victims were dumped into wells, or were catapulted into enemy encampments. Development of anthrax-based weapons was pursued by various governments in World Wars I and II, including those of the United States, Canada, and Britain.

Humans naturally acquire anthrax from exposure to livestock such as sheep or cattle or wild animals. The animals are reservoirs of the anthrax bacterium.

A microscopic view of the anthrax bacteria is seen in this photo from the U.S. Army Medical Research and Development Command at Ft. Detrick, Maryland. AP/WIDE WORLD PHOTOS.

While all three types of anthrax infections are potentially serious, prompt treatment usually cures the cutaneous form. Even with prompt treatment, the gastrointestinal form is lethal in 25%–75% of those who become infected. The inhaled version of anthrax is almost always lethal.

When *Bacillus anthracis* is actively growing and dividing, it exists as a large "vegetative" cell. But, when the environment is threatening, the bacterium can form a spore and becoming dormant. The spore form can be easily inhaled. Only 8,000 spores, hardly enough to cover a snowflake, are sufficient to cause the inhalation form of anthrax when the spores resuscitate and begin growth in the lungs.

The growing *Bacillus anthracis* cells have several characteristics that make them so infectious. First, the formation of a capsule around the bacterium can mask the surface from recognition by the body's immune system. The body can be less likely to mount an immune response to the invading bacteria. Also, the capsule helps fend off antibodies and immune cells that do respond. This protection can allow the organism to multiply to large numbers.

The capsule also contains a protein that protects the bacterium. This "protective antigen" dissolves other protein molecules that form part of the outer coating of host cells. This allows the bacterium to evade the host's immune response by burrowing inside host cells such as the epithelial cells that line the lung.

A toxic component called lethal factor actively destroys the host's immune cells. Finally, another toxic factor called the edema factor (edema is the build up of fluid at the site of infection) disables a host molecule called calmodulin. Calmodulin regulates many chemical reactions in the body.

With the various toxic factors, *Bacillus anthracis* is able to overcome the attempts of the host to deal with the infection. Bacterial toxins enter the bloodstream and circulate throughout the body. The destruction of blood cells and tissues can be lethal.

The early symptoms of anthrax infections are similar to other, less serious infections, such as the flu. By the time the diagnosis is made, the infection can be too advanced to treat. This can make the recognition of a deliberate anthrax attack difficult to recognize until large numbers of casualties have resulted. While the bacteria can be killed by antibiotics, in particular an antibiotic called ciprofloxacin (cipro), the antibiotic needs to be administered early in an infection.

The ease by which anthrax can be transported (i.e., via the mail) has made anthrax a weapon of frightening severity.

A vaccine for anthrax does exist, although the possibility of serious side effects has limited its use to only those at high risk for infection (i.e., soldiers, workers in meat processing plants, anthrax researchers). Vaccine researchers are exploring the possibility that the edema factor and the capsule could be exploited as targets of vaccines. The idea is that the vaccines would stop the bacteria from getting into host cells. This would make it easier for the immune response to kill the invading bacteria.

■ FURTHER READING:

BOOKS:

Heyman, D. A., J. Achterberg, and J. Laszlo. *Lessons from the Anthrax Attacks: Implications for U.S. Bioterrorism Preparedness: A Report on a National Forum on Biodefense.* Washington, DC: Center for Strategic and International Studies, 2002.

Koehler, T. M. *Anthrax.* Berlin: Springer Verlag, 2002.

PERIODICALS:

Jernigan, J. A., D. S. Stevens, D. A. Ashford, et al. "Bioterrorism-Related Inhalational Anthrax: The First 10 Cases Reported in the United States." *Emerging Infectious Diseases* no. 7 (2001).

ELECTRONIC:

Centers for Disease Control and Prevention. "Anthrax." Division of Bacterial and Mycotic Diseases. October 30, 2001. <http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax_t.htm>(9 December 2002).

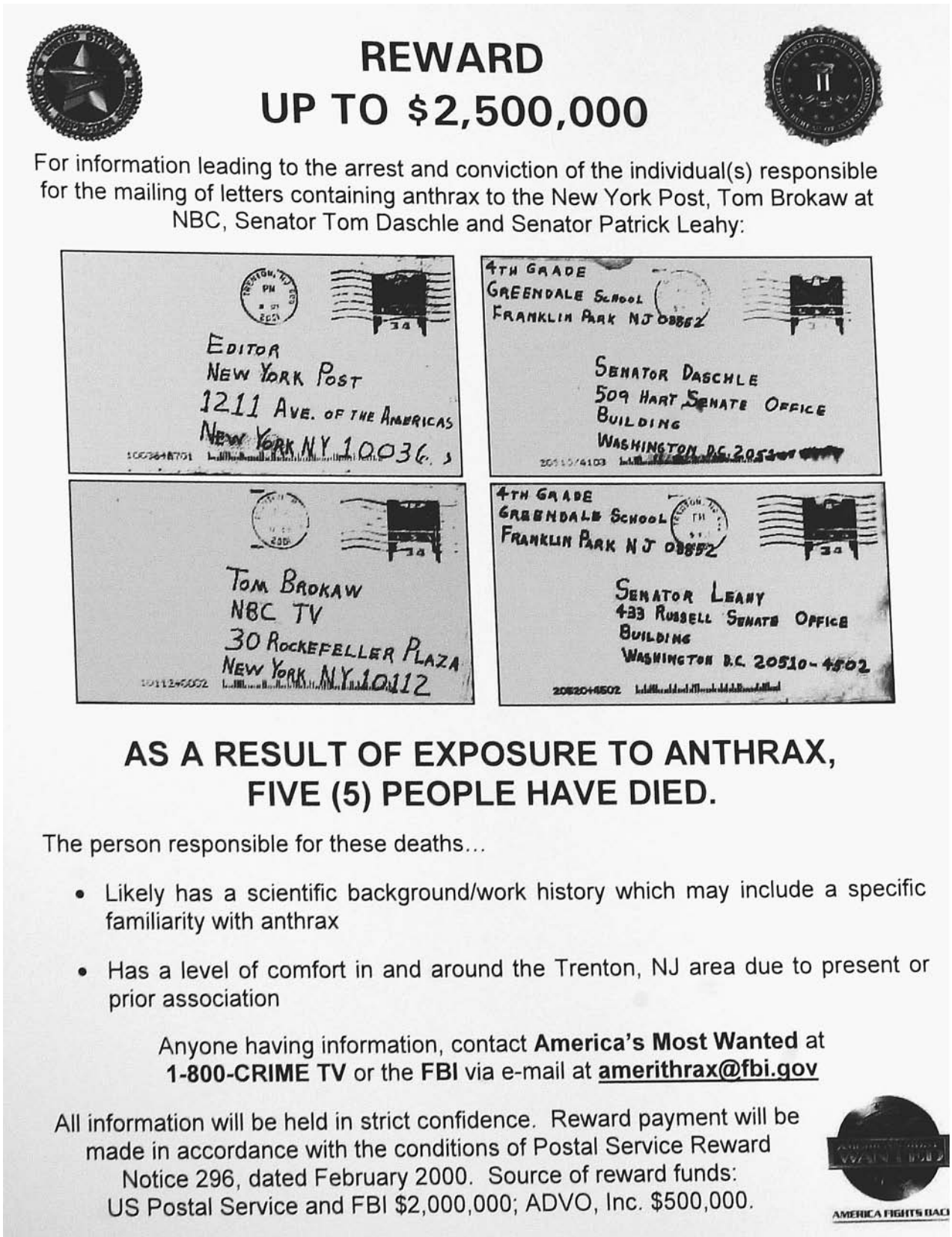
SEE ALSO

Anthrax, Terrorist Use as a Biological Weapon
Anthrax Vaccine
Anthrax Weaponization
Antibiotics
Biological Weapons, Genetic Identification
Infectious Disease, Threats to Security
USAMRIID (United States Army Medical Research Institute of Infectious Diseases

Anthrax, Terrorist Use as a Biological Weapon

■ BRIAN HOYLE

During the past two decades, the potential use of biological weapons by terrorist groups has received a great deal of attention, particularly in the United States. The existence of an anthrax bioweapon development campaign by the government of Iraq was revealed during the Persian Gulf War from 1990 to 1991. Then, in the aftermath of the September 11, 2001 terrorist attacks on the World Trade Center buildings in New York City and the Pentagon in Washington, DC, letters containing a powdered form of *Bacillus anthracis*, the bacteria that causes anthrax, were mailed to government representatives, members of the news media, and others in the United States. The anthrax-laced powder inside the letters was aerosolized (i.e., the



The FBI and the U.S. Postal Service released this reward flyer for information leading to the arrest and conviction of the individuals responsible for mailing anthrax-tainted letters in 2001 to members of Congress and the media. AP/WIDE WORLD PHOTOS.

spores became airborne) when the letters were opened, and in a few cases were inhaled. The death of a Florida man was the first case of an inhalational anthrax death in the United States since 1978 and as of June 2002, more than 20 cases and five deaths were attributed to the terrorist attacks.

Although anthrax is a relatively new weapon in the hands of modern potential bioterrorists, the threat of death from the inhalation of spores has been part of human history since antiquity. Some scholars argue that anthrax is the sooty "morain" in the Bible's Book of Exodus, and is likely the "burning wind of plague" that begins Homer's *Iliad*.

As well, the use of microorganisms such as the anthrax bacteria as weapons is not new. In ancient military campaigns, diseased bodies (including those who died of anthrax) were used to poison wells and were catapulted into cities under siege. Research into the military use of anthrax was carried out during World War I by combatants on all sides of the conflict, and by World War II, anthrax research was actively underway. For example, Allied efforts in Canada, the United States, and Britain to develop anthrax-based weapons included the production of five million anthrax "cakes," designed to be dropped on Germany to infect wells and contaminate the food chain. The weapons were never used.

Only within the past several decades, however, have biological weapons, including anthrax, been added to the arsenal of terrorists. For example, the Japanese cult Aum Shinrikyo (which released Sarin gas into the Tokyo subway system in 1995, killing 12 people and hospitalizing 5,000) was developing anthrax-based weapons. Indeed, the group had released crude anthrax preparations in Tokyo on at least eight separate occasions in 1993. These incidents constituted the first use of anthrax as a weapon against a civilian population. In addition, state-sanctioned terrorism by the government of Iraq has also involved the production of anthrax bioweapons, and Western intelligence sources openly insist that Iraq—and or terrorist groups operating with Iraq's assistance—continued to develop biological weapons, including anthrax based weapons. Finally, during the terrorist attacks of the United States in the latter part of 2001, the use of anthrax by a terrorist or terrorists (as of July, 2003, yet unidentified) pointed out how easily the lethal agent could be delivered.

This ease of delivery of anthrax is one feature that has made the bacterium an attractive weapon for terrorists. Scenarios developed by United States government agencies have shown that even a small crop dusting plane carrying only a hundred kilograms of anthrax spores flying over a city could deliver a potentially fatal dose to up to three million people in only a few hours. Although variations in weather patterns and concentration variables would substantially reduce the number of expected actual deaths, such an attack could still result in the deaths of thousands of victims and result in a devastating attack on the medical and economic infrastructure of the city attacked. In a less sophisticated effort, spores could simply be released into air intake vents or left in places like a subway tunnel, to be dispersed in the air over a much smaller area.

Another feature of anthrax that has led to its exploitation by terrorists is the physiology of the bacterium. *Bacillus anthracis* can live as a "vegetative cell," growing and dividing in a rapid and cyclical fashion. The bacterium can also form a metabolically near-dormant form known as a spore. An individual spore is much smaller and lighter than the growing bacterium. The spores can drift on air currents, to be inhaled into the lungs. Once in the lungs, the spores can resuscitate into an actively growing and dividing bacterium. The infections that are collectively termed anthrax can result. Although millions of spores can be released from a few grams (fractions of an ounce) of *Bacillus anthracis*, only about 5,000 to 8,000 spores are sufficient to cause the lung infection when they are inhaled. If left untreated or not promptly treated with the proper antibiotics (such as Cipro), the lung infection is almost always fatal. Non-inhalation contact with *Bacillus anthracis* can result in cutaneous anthrax—a condition more treatable with conventional antibiotic therapy.

An often-overlooked aspect of the use of anthrax as a terrorist weapon is the economic hardship that the dispersal of a small amount of the spores would exact. A report from the Centers for Disease Control and Prevention, entitled *The Economic Impact of a Bioterrorist Attack*, estimated the costs of dealing with an anthrax incident at a minimum of U.S. $26 billion per 100,000 people. In just a few months in 2001 alone, a flurry of anthrax incidents, most of which turned out to be hoaxes, cost the United States government millions of dollars.

Biotechnology and anthrax. The choice of anthrax as a weapon used by terrorists reflects the growing awareness of the power of biological research and biotechnology among the general community. The ability to grow and disperse infectious microorganisms was once restricted to specialists. However, the explosion of biotechnology in the 1980s and 1990s demonstrated that the many basic microbiological techniques are fairly simple and attainable. Experts in microbiology testifying before the U.S. Congress estimated that crude weapons could be developed with approximately $10,000 worth of equipment. A laboratory sufficient to grow and harvest the bacteria and to dry down the material to powdered form could fit into the average sized household basement. The more highly trained the terrorist, the more effective weapons could be expected to be produced.

Even though *Bacillus anthracis* could be grown in such a makeshift laboratory, the preparation of the spores and the drying of the spores into a powder is not a trivial task. For example, even after a decade of dedicated effort, United Nations inspectors who toured Iraq bioweapons facilities after the Gulf War found that Iraq had only managed to develop crude anthrax preparations. Still, the Iraqi

bioweapons program managed to produce 8,500 liters of concentrated anthrax.

Despite the technical challenges, the production of anthrax spores in quantities great enough to cause a huge loss of life is not beyond the capability of a small group of equipped and funded terrorists. The small size and nondescript nature of a bioweapons facility could make detection of such a lab very difficult. Accordingly, the terrorist potential of anthrax will remain a threat for the foreseeable future.

FURTHER READING:

BOOKS:

Heyman, D. A., J. Achterberg, and J. Laszlo. *Lessons from the Anthrax Attacks: Implications for U.S. Bioterrorism Preparedness: A Report on a National Forum on Biodefense*.Washington, DC: Center for Strategic and International Studies. 2002.

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague", in: *Emerging Infections 5* Washington, DC: American Society for Microbiology Press, 2001.

Koehler, T. M. *Anthrax.* Berlin: Springer Verlag, 2002.

ELECTRONIC:

University of California at Los Angeles. "Anthrax as a Weapon." College of Letters and Science. February, 2002. <http://www.college.ucla.edu/webproject/micro12/m12webnotes/anthraxweapon.html> (29 December 2002).

SEE ALSO

Anthrax Vaccine
Bacterial Biology
Biological Warfare
Bioterrorism, Protective Measures

Anthrax Vaccine

BRIAN HOYLE

Anthrax is an infection that is caused by the bacterium *Bacillus anthracis*.

Several different types of anthrax infection can be caused by the bacterium. Entry of bacteria through a skin wound can produce a skin infection known as cutaneous anthrax. Microorganisms can also contaminate food or water. Ingestion of the contaminated food or water produces gastrointestinal anthrax. The most serious type of anthrax results from the inhalation of the spore form of the bacterium. Inhalation anthrax has a high mortality rate.

In the 1990s, United States military personnel in the Persian Gulf region faced the possibility of retaliatory strikes using biological weapons, in particular anthrax. Domestically, the use of *Bacillus anthracis* spores by terrorists is a reality. Although not directly related by evidence to the September 11, 2001, terrorist attacks on the World Trade Center and Pentagon in the United States, letters containing powdered anthrax bacteria and spores were sent to a number of politicians, media personalities, and U.S. citizens. Even more ominously, the terrorists responsible for the September 11 attacks had attempted to procure a small crop dusting aircraft. Such an aircraft could potentially disperse several hundred kilograms of anthrax spores upwind of a major urban center in only a few hours. One scenario developed by scientists for Washington, D.C. indicated that up to three million people could be sickened or killed by such an attack.

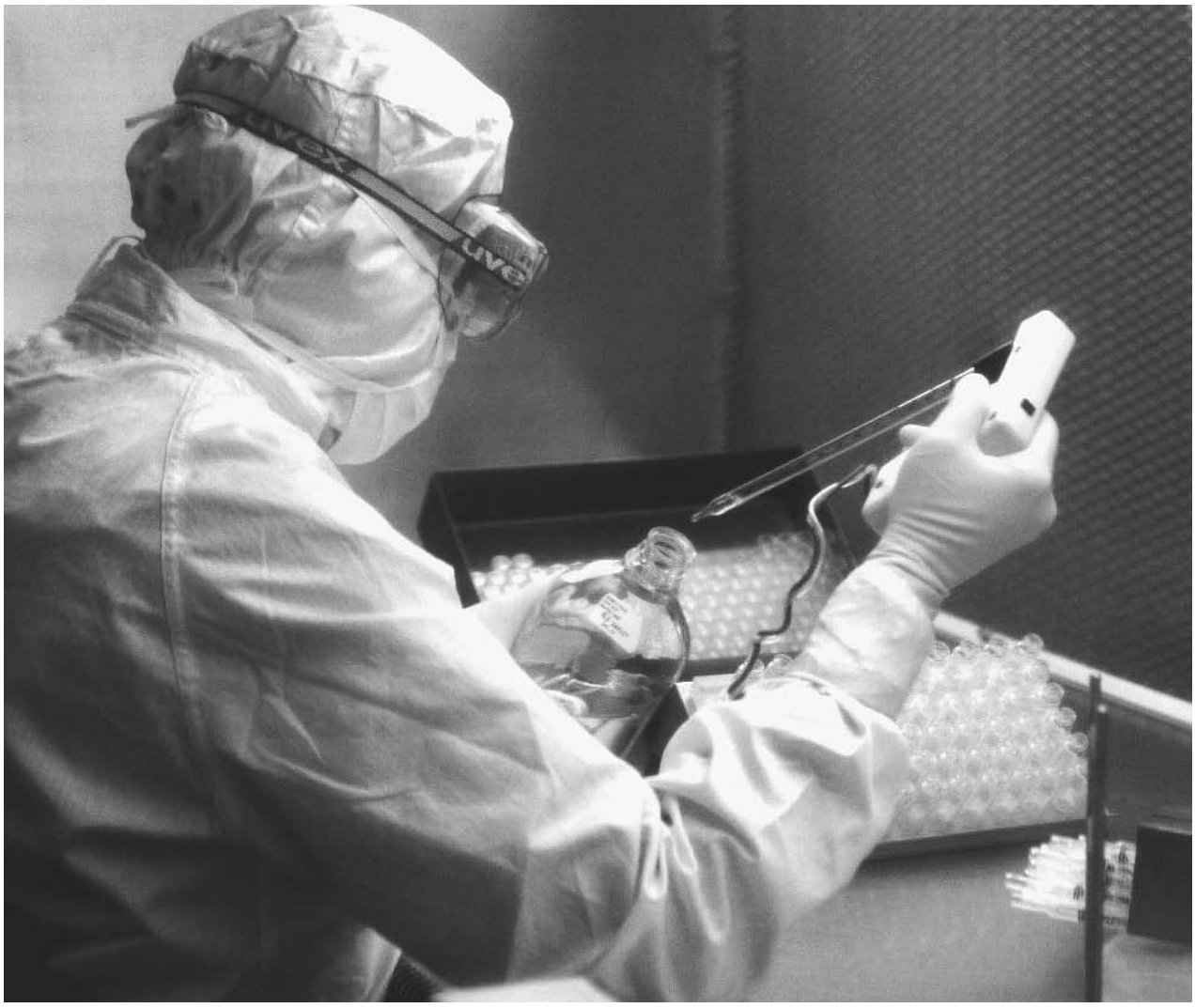
For some years, military personnel and others at risk for anthrax exposure (i.e., researchers and those handling animals) have received an anthrax vaccine. For example, U.S. military personnel were vaccinated in 1990, during the Gulf War, and again prior to another response in that region in 1998.

The increasing risk and incidence of anthrax exposure, however, have made the development of different and safer anthrax vaccines a priority. The use of anthrax against civilians, and the ominous scenarios of anthrax spores released in the ventilation systems of office buildings and over large urban centers, have created the possibility that millions of people would potentially require vaccination. As well, large stockpiles of anthrax vaccine (as well as antibiotics) would be required, in anticipation of future outbreaks.

Current anthrax vaccine. The anthrax vaccine now in use dates back to the time of Louis Pasteur, in the mid-nineteenth century. Pasteur noted that the injection of animals with an attenuated type of *Bacillus anthracis* protected the animals from contracting anthrax. An attenuated strain of bacteria is one that can be capable of growth, but which does not cause disease. The body's immune system will react to the bacteria, and produce antibodies that will protect the animal or person from future exposure to the disease-causing bacteria. A modification of this attenuated vaccine developed in the late 1930s still serves as the anthrax vaccine given to animals.

In the late nineteenth century, the use of live bacteria as vaccines was still too dangerous for humans. In the early years of the twentieth century, researchers began exploring the use of components of the anthrax bacterium as a protective measure. In 1954, a product was developed that consisted of soluble material called protective antigen, which is released by *Bacillus anthracis*, and which can be precipitated out of solution—along with two other cell components called the lethal factor and the edema factor—by the use of aluminum potassium sulfate (alum). Filtering the suspension captures the antigenic compounds.

By 1960, the selection of a strain of *Bacillus anthracis* that produced more of the protective antigen, the use of



A technician works in a clean room filling anthrax vaccine vials at a Spokane, Washington, laboratory in 2002. AP/WIDE WORLD PHOTOS.

growth media that was free of protein (that could also stimulate an immune reaction), and the use of aluminum hydroxide instead of alum had produced a superior vaccine. The improved product, anthrax vaccine adsorbed (AVA), was approved for use in the United States in 1965. AVA remains the only licensed vaccine in the United States as of early 2003.

Protective antigen, lethal factor, and edema factor. The protective antigen is a protein that can insert into the membrane of a host cell to create a hole, or pore, through the membrane. The pore then functions as a portal to allow the other two components to get inside of the host cell.

The lethal factor is a type of enzyme classified as a zinc protease. The enzyme attacks and breaks host proteins into smaller and nonfunctional pieces. Destroying host cell proteins is lethal to the host cell, hence the factor's name.

Edema factor is a toxin. The destruction of the host cells allows this toxin to enter the bloodstream, where it can kill cells of the immune system. Disabling the host's immune response allows the bacteria and the toxin to spread throughout the body.

Side effects of the anthrax vaccine. Like some other vaccines, AVA can cause side effects, which can, in rare instances, be life threatening or fatal. Data regarding adverse events are available from the Vaccine Event Reporting System (a U.S. vaccine safety surveillance program that is under the direction of the Food and Drug Administration and the Centers for Disease Control and Prevention). From January 1, 1990 through August 31, 2000, 1,859,000 doses of anthrax vaccine were administered in

the United States. The number of adverse events was 1,544 (e.g. sensitivity at injection site, headache, muscle ache) with 76 of these being serious (e.g., heart failure, blood infection). Other than reaction at the site of injection, it is still not clear whether the other maladies were directly due to the vaccine. Nonetheless, the number of adverse reactions were small.

Echoing this data, a report released in March 2002 by the U.S. National Academy of Sciences Institute of Medicine concluded that AVA is "acceptably safe." However, the report noted the lack of data on the long-term effects of the vaccine.

Studies conducted by the Department of Defense on vaccinated military personnel found that most adverse events were minor, were localized to the site of injection, and cleared up within a few days.

The involvement of anthrax vaccine to the development of a multi-symptom debilitating syndrome reported in military personnel deployed in the Persian Gulf conflicts ("Gulf War Syndrome") was investigated by the Centers for Disease Control and Prevention. No scientific evidence of an association was found. However, studies conducted on Canadian and British soldiers stationed in the Gulf and in Bosnia (where anthrax deployment was also a threat) were not as conclusive.

Limitations of the anthrax vaccine. While the risks posed by AVA may not be pronounced, the vaccine is problematic from the standpoints of supply and quality of the product.

In addition to aluminum, the vaccine contains benzethonium chloride as a preservative and formaldehyde to keep the vaccine mixture stable upon storage. Despite regulatory examinations that have confirmed the safety of the vaccine, there continues to be debate as to the possible long-term harm from the presence of these chemicals.

Another problem concerns the frequency of vaccination that is required to establish immunity. Primary vaccination requires three injections at 0, 2, and 4 weeks, followed by three booster injections at 6, 12, and 18 months. To maintain the immunity, annual injections are recommended.

Such a frequent regimen of injections is inconvenient and requires almost two years to establish peak protection. The vaccine is not designed to confer rapid immunity.

The nature of the vaccine's preparation—collection of material extruded by the bacteria—makes the vaccine crude in terms of its exact composition and proportion of the various components. This unpredictability, and the scarcity of the vaccine have limited the wide-spread availability of AVA.

The vaccine is currently manufactured at a single facility in the U.S., and only in sufficient quantity for use by those at risk of infection, such as combat personnel and researchers.

FURTHER READING:

PERIODICALS:

Advisory Committee on Immunization Practices. "Recommendations of the Advisory Committee on Immunization Practices: Use of Anthrax Vaccine in the United States." *Morbidity and Mortality Weekly Report* no. 49 (2000): 1–20.

Bradley, K. A., J. Mogridge, M. Mourey, et al. "Identification of the Cellular Receptor for Anthrax Toxin." *Nature* no. 414 (2001): 225–229.

Friedlander, A. M. "Tackling Anthrax." *Nature* no. 414 (2001): 160–161.

Joellenbeck, L. M., L. L. Zwanziger, J. S. Durch, et al. *The Anthrax Vaccine: Is It Safe? Does It Work?* Washington, DC: National Academies Press, 2002.

SEE ALSO

Biological Warfare
Microbiology: Applications to Espionage, Intelligence and Security
Toxins

Anthrax Weaponization

BRIAN HOYLE

The lethality of inhalation anthrax, combined with the ability of the lethal payload to be delivered in the spore form, has made anthrax an attractive candidate for weaponization. In addition, a vaccine to anthrax does exist, but is not yet widely available. Thus, troops can be vaccinated against the disease while the general population of the enemy remains unprotected. Many of these characteristics that make anthrax a desirable military weapon also make the disease a desirable weapon of the terrorist.

As of 2003, intelligence sources indicate that at least 17 nations around the globe have offensive biological weapons programs. How many of these nations are pursuing anthrax weaponization is unknown. The government of Iraq, however, admitted in 1995 to producing over 8,000 liters of concentrated anthrax as part of the nation's biological weapons program. Additionally, only a few generations ago, nations such as Britain and the United States actively engaged in anthrax weaponization programs.

Anthrax is a disease that is caused by the bacterium *Bacillus anthracis*. The bacterium lives naturally in grazing animals such as cattle and sheep. Depending on the route of entry of the bacterium into the human body, anthrax infection can occur in the intestinal tract, the skin, and, most seriously, in the lungs. The latter form, which is called pulmonary or inhalation anthrax, progresses swiftly and is lethal in over 50%. Early detection of the infection,

Members of an EPA and United States Coast Guard cleanup crew prepare to enter the American Media Inc. office building in Boca Raton, Florida, where at least two people contracted anthrax through a deliberately contaminated letter mailed to the facility in October, 2001. AP/WIDE WORLD PHOTOS.

combined with the use of antibiotic and supportive therapies offer the best chance of survival once an inhalation anthrax infection has been established.

A major factor that contributes to the spread of anthrax is the ability of the bacterium to form a spore. The spore is a tough shell that houses the genetic material of the microbe, and can preserve this material almost indefinitely through harsh environmental conditions that would kill the growing bacteria. When conditions become more hospitable—as when the spores are breathed into the warm and moist environment of the lungs—the spores "germinate" and bacterial growth resumes.

Most biological warfare experts concur that the manufacture of sufficient quantities of anthrax spores to permit an aerial assault or to form the payload of missiles requires manufacturing facilities and skilled personnel, and is a formidable challenge. Nonetheless, given time, funding and desire, an organization can muster the necessary resources. For example, the terrorist group Aum Shinrikyo, which was responsible for the release of Sarin gas in a Tokyo, Japan, subway station in 1995, also released spores

of *Bacillus anthracis* and *Clostridium botulinum* (the bacterium that causes botulism) throughout Tokyo on at least eight occasions.

The dispersal of anthrax via a crop dusting plane or a balloon is the most likely scenario for the mass exposure of a population. More traditional methods use missiles to deliver the payload of explosives. However, the heat that develops in a missile during its passage to the target, particularly as it re-enters the atmosphere, could kill even anthrax spores.

The most popular anthrax weapon to date has been the dried form of the bacterial spores. The powdery material becomes dispersed in the air very easily. For example, opening a letter can disperse the powder and cause spores to be inhaled.

In contrast, the process of manufacturing the spore powder is technically complex. When anthrax bacteria for spores and the spores are harvested, they form a sticky paste with the consistency of peanut butter. When this paste is dried, the result is a hard block of material. The block can be ground into a powder. But the spores will tend to have a surface charge and so will tend to clump together. The clumping can be overcome by coating the spores with chemicals such as silica or alumina clay. The Iraqi program utilized a clay preparation called bentonite.

For the spores to be inhaled deep into the lungs, each spore needs to be on the order of one to five micrometers in diameter. Anything smaller than this will behave as a gas, and so will be exhaled, while larger particles such as the clumps of spores will become stuck in the upper respiratory tract, where it is more difficult to establish the disease. Preparation of a spore powder where all the particles are the requisite size is not, in terms of difficulty, a trivial task. Nonetheless, the success of the anthrax terrorist attacks in the U.S. in 2001 shows that it is possible.

Studies on Gruinard Island—an island off the coast of Scotland where Britain conducted tests of anthrax spore delivery systems during World War II—has recovered spores that can germinate into disease causing bacteria even decades later. Thus, even an inefficient application of anthrax spores may leave a residual that will be capable of infecting people for long after the attack.

FURTHER READING:

BOOKS:

Heyman, D.A., J. Achterberg, and J. Laszlo. *Lessons from the Anthrax Attacks: Implications for U.S. Bioterrorism Preparedness: A Report on a National Forum on Biodefense.* Washington, DC: Center for Strategic and International Studies, 2002.

ELECTRONIC:

University of California at Los Angeles. "Anthrax as a Weapon." College of Letters and Science. February, 2002. <http://www.college.ucla.edu/webproject/micro12/m12webnotes/anthraxweapon.html> (29 December 2002).

SEE ALSO

Biological Warfare
Coordinator for Counterterrorism, United States Office
Infectious Disease, Threats to Security

Antiballistic Missile Treaty

LARRY GILMAN

The Antiballistic Missile (ABM) Treaty was signed by the United States and the Soviet Union (U.S.S.R.) in 1972. The treaty was one of two treaties produced by the first series of Strategic Arms Limitation Talks (SALT I) between the two countries; the other was an interim agreement limiting offensive nuclear weapons. The ABM treaty strictly limited the deployment—by both sides—of interceptor missiles, missile launchers, radars, and other devices designed to destroy ballistic missiles or their components in flight. In the original version, each nation was permitted to retain a limited number of ABM radars and no more than 100 ABM interceptor missiles at each of two circular sites 186 miles (300 km) in diameter, one centered on the nation's capital and the other on a cluster of ballistic-missile launch sites. A 1974 amendment reduced the number of permitted ABM sites to one per side and further bound both countries to not deploy ABM systems outside their own territory (e.g., at sea or on the territory of allies). In 1975, the U.S. dismantled its sole ABM system, SAFEGUARD; the U.S.S.R. (and, later, the Russian Federation) retained a single ABM system centered on Moscow. In 1997, further minor revisions were agreed upon, but never ratified by the U.S. The U.S. withdrew from the ABM treaty in July, 2002, and it is no longer binding on any country.

In the U.S., critics urged withdrawal from the ABM treaty soon after it was signed. They argued that it was ridiculous to prevent nuclear war by limiting defense against the primary means for delivering nuclear weapons to their targets. The Reagan administration, for example (1980–1988) sought to deploy an ambitious missile-defense system ("Star Wars") that would have required abrogation of the ABM treaty. However, supporters of the ABM treaty defended it successfully throughout the 1980s and 1990s based primarily upon the concepts of mutual deterrence, mutual destruction, and first-strike capability.

Since the 1950s, the U.S. and the Soviet Union (U.S.S.R.) possessed enough nuclear warheads mounted on ballistic missiles (and additional thousands on other delivery systems, such as bombers) to destroy each other many times over. Aggression by each side was, in theory, deterred by fear of the other side's weapons; if either side attacked, both attacker and attacked would be destroyed.

With his national security team assembled in the Rose Garden at the White House, President Bush, center, announces that the United States will withdrawl from the 1972 Anti-ballistic Missile Treaty in 2002, paving the way for the development of a defensive anti-ballistic missile technology program. AP/WIDE WORLD PHOTOS.

This policy—often termed Mutually Assured Destruction—was unstable to the extent that a "first strike" by one side was able (or was perceived as being able) to destroy the other side's missiles in their silos, eliminating most of that country's ability to retaliate. If such a strike were successful, the country to strike first might prevail. Building defenses against ballistic missiles, most arms-control experts assumed, would make this situation even more unstable for several reasons. First, it is impossible to build a system of antiballistic-missile weapons that can reliably protect most of the civilian population of any nation from a determined nuclear attack. (2) A partially effective shield, however, might serve to protect a nuclear aggressor from the effects of a weak counterattack. (3) Possession of such a partial defensive system would, therefore, make a first strike more attractive to the nation possessing it. (4) Finally, if one side built such a partial system, the other, knowing that a first strike had become more attractive to side possessing the partial ABM system, would have even more incentive to strike first itself (against the enemy's ABM system as well as its offensive nuclear weapons), and place itself on hair-trigger alert against attack, making accidental nuclear war more likely. The ABM treaty was designed, signed, and ratified by the U.S. and U.S.S.R. in order to prevent destabilization of this type.

The Reagan administration was prevented from developing a Star Wars system by domestic political resistance centered on the ABM treaty and on skepticism about the technical feasibility of the Stars Wars concept itself. However, the project has been funded by all succeeding administrations, and has now been fully revived under President George W. Bush. In December 2001, the United States gave six months' notice of its intent to withdraw from the ABM treaty, as provided for by the terms of the treaty itself. The U.S. officially withdrew from the treaty in July, 2002. A few days later, work began on a U.S. missile shield, with ground-breaking ceremonies at Fort Greeley, Alaska for a test-bed ABM system consisting of six interceptor missiles.

China, which at present has only about 20 intercontinental-range, land-based ballistic missiles, has stated that it is able to build offensive systems capable of overwhelming any ABM system deployed by the United States.

FURTHER READING:

BOOKS:

Alves, Péricles Gasparini. *Prevention of an Arms Race in Outer Space.* New York: United Nations Institute for Disarmament Research. 1991.

ELECTRONIC:

Stoullig, Jean-Michel. "ABM Treaty Ends, U.S. Open to Experiment on Missile Defense." Agence France-Presse (in SpaceDaily.com). June 13, 2002. <http://www.spacedaily.com/news/bmdo-02l.html> (December 9, 2002).

"Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, 944 U.N.T.S. 13." Nuclear Age Peace Foundation. 2002. <http://www.nuclearfiles.org/docs/1972/720526-abm.html> (December 9, 2002).

SEE ALSO

Ballistic Missile Defense Organization, United States
Ballistic Missiles

Antibiotics

BRIAN HOYLE

The security and stability of a country depends in part on the health of its citizens. One of the factors that influence the health of people is infectious disease (a disease that can be spread from person to person or from another living being to a human). A variety of infectious diseases are caused by bacteria.

Some bacterial infections can be treated using compounds that are collectively known as antibiotics. Antibiotics can be naturally produced. For example, the first antibiotic discovered (penicillin; discovered in 1928 by Sir Alexander Fleming) is produced by a species of a mold microorganism. There are a variety of different naturally produced antibiotics, while many other antibiotics have been chemically produced. Finally, antibiotics act only on bacteria and are not effective against viruses.

Prior to the discovery of penicillin there were few effective treatments to battle or prevent bacterial infections. Pneumonia, tuberculosis, and typhoid fever were virtually untreatable. And, in those persons whose immune system was not functioning properly, even normally minor bacterial infections could prove to be be life-threatening.

In nature, antibiotics help protect a bacteria or eukaryotic cell (i.e., plant cell) from invading bacteria. In the laboratory, this is evident as the inhibition of growth of bacteria in the presence of the antibiotic-producing species. This screening can be automated so that thousands of samples can be processed each day.

The chemical synthesis of antibiotics is now very sophisticated. The antibiotic can be tailored to affect a specific target on the bacterial cell. Three-dimensional modeling of the bacterial surface and protein molecules is an important aid to antibiotic design.

Penicillin is in a class of antibiotics called beta-lactam antibiotics. The name refers to the chemical ring that is part of the molecule. Other classes of antibiotics include the tetracyclines, aminoglycosides, rifamycins, quinolones, and sulphonamides. The action of these antibiotics is varied. The targets of the antibiotics are different. Some antibiotics disrupt and weaken the cell wall of bacteria (i.e., beta-lactam antibiotics), which causes the bacteria to rupture and die. Other antibiotics disrupt enzymes that are vital for bacterial survival (aminoglycoside antibiotics). Still other antibiotics target genetic material and stop the replication of deoxyribonucleic acid (DNA) (i.e., quinolone antibiotics).

Antibiotics can also vary in the bacteria they affect. Some antibiotics kill only a few related types of bacteria and are referred to as narrow-spectrum antibiotics. Other antibiotics such as penicillin kill a variety of different bacteria. These are the broad-spectrum antibiotics.

Following the discovery of penicillin, many different naturally occurring antibiotics were discovered and still many others were synthesized. They were extremely successful in reducing many infectious diseases. Indeed, in the 1970s the prevailing view was that infectious diseases were a thing of the past. However, beginning in the 1970s and continuing to the present day, resistance to antibiotics is developing.

As of 2002, the problem of antibiotic resistance is so severe that many physicians and security analysts think that the twenty-first century will initiate the "post antibiotic era." In other words, the use of antibiotics to control infectious bacterial disease will no longer be an effective strategy.

Resistance to a specific antibiotic or a class of antibiotics can develop when an antibiotic is overused or misused. If an antibiotic is used properly to treat an infection, then all the infectious bacteria should be killed directly, or weakened such that the host's immune response will kill them. However, if the antibiotic concentration is too low, the bacteria may be weakened but not killed. The same thing can happen if antibiotic therapy is stopped too soon. The surviving bacteria may have acquired resistance, which can be genetically transferred to subsequent generations of bacteria. For example, many strains of *Mycobacterium tuberculosis*, the bacterium that causes tuberculosis, are resistant to one or more of the antibiotics used to treat the lung infection. Some strains of *Staphylococcus aureus* that can cause boils, pneumonia, or bloodstream infections, are resistant to most (and with one strain, all) antibiotics.

The increasing antibiotic resistance of bacteria, and the resulting increase in infectious diseases, is a security risk. Disease can decimate the population. The misery and economic hardship that results can cause political instability. In underdeveloped countries, this instability can lead to anger directed at developed countries such as the United States. Even in developed countries, the increasing numbers of people needing hospitalization and medical care can strain the health care system.

The availability of antibiotics to combat bacterial epidemics has always been challenging. The appearance and rapid increase in an infection can tax the ability of a healthcare system to respond with medicines including the appropriate antibiotics.

The threat of biological warfare, such as the aerial distribution of *Bacillus anthracis*, the agent of anthrax, has made the provision of large quantities of antibiotics a priority for the United States and other nations. Plants that manufacture antibiotics are designed with sterility of manufacture in mind, not security. Disabling an antibiotic manufacturing facility would be a crippling blow to any potential biowarfare response.

Even if a large supply of a particular antibiotic were available, the emergency response would be challenging, as the antibiotic would need to be distributed to many

people (i.e., millions in the event of an aerial release of the anthrax bacterium) within hours.

FURTHER READING:

PERIODICALS:

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague." *Emerging Infections 5.* Washington, DC: American Society for Microbiology Press, 2001.

ELECTRONIC:

Central Intelligence Agency. "The Global Infectious Disease Threat and Its Implications for the United States." January 2000.<http://www.cia.gov/cia/publications/nie/report/nie99–17d.html> (22 November 2002).

World Health Organization. "Strengthening Global Preparedness for Defense against Infectious Disease Threats." Statement to the United States Senate Committee on Foreign Relations Hearing on The Threat of Bioterrorism and the Spread of Infectious Diseases. 5 September 2001. <http://www.who.int/emc/pdfs/Senate_hearing.pdf>(24 November 2002).

SEE ALSO

Biocontainment Laboratories
Biological Warfare
CDC (United States Centers for Disease Control and Prevention)
L-Gel Decontamination Reagent
Pathogens
Public Health Service (PHS), United States

Anti-Imperialist Territorial Nuclei (NTA)

The Anti-Imperialist Territorial Nuclei (NTA) is a small (approximately 20 members) clandestine leftist extremist group that appeared in the Friuli region in Italy in 1995. NTA adopted the class struggle ideology of the Red Brigade of the 1970s-80s and a similar logo—an encircled five-point star—for their declarations. The group opposes what it perceives as U.S. and NATO imperialism and condemns Italy's foreign and labor polices. NTA opposes both the U.S. and the NATO presence in Italy. NTA attacked property owned by U.S. Air Forces personnel at Aviano Air Base. The NTA also claimed responsibility for a bomb attack in September, 2000, against the Central European Initiative office in Trieste and a bomb attack in August, 2001, against the Venice Tribunal building. NTA members threw gasoline bombs at the Venice and Rome headquarters of the then-ruling party, Democrats of the Left, during the NATO intervention in Kosovo.

The NTA operates in northeastern Italy, including the Friuli, Veneto, and Emilia regions.

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

APIS (Advance Passenger Information System)

The Advance Passenger Information System (APIS) is an electronic database system that stores information about airline travelers. The system, operated by the United States Customs Service, the Immigration and Naturalization Service (INS), and the Federal Aviation Administration (FAA), provides searchable biographical and security information on air travelers entering the United States from a foreign location.

As of March 1, 2003, the newly created United States Department of Homeland Security (DHS) absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS.

BTS is scheduled to incorporate the United States Customs Service (previously part of the Department of Treasury), the enforcement division of the Immigration and Naturalization Service (previously part of the Department of Justice), the Animal and Plant Health Inspection Service (previously part of the Department of Agriculture), the Federal Law Enforcement Training Center (previously part of the Department of Treasury), Transportation Security Administration (previously part of the Department of Transportation) and the Federal Protective Service (previously part of the General Services Administration).

Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the reorganization the INS formally ceases to exist on the date the last of its functions are transferred.

Although the description of the technologies involved in the APIS entry security program remained stable, in an effort to facilitate border security BTS plans envision higher levels of coordination between formerly separate agencies and databases. As of April 2003, the specific coordination and future of the APIS dtaabase was uncertain with regard to name changes, database administration, and user policy changes.

Common APIS data includes information that that is routinely found on a passport or visa and airline boarding card, such as an individual's name, birth date, country of residence, country of origin and final destination. Records also note if the passenger has been issued a United States visa. In some locations, optical scanners are used to obtain digital records of passports, visas, and other documents.

Although initiated as a voluntary program for air carriers in 1988, anti-terrorism and security legislation passed in the wake of the September 11, 2001 terrorist attacks mandated participation in the APIS. Prior to departure of every international flight bound for the United States, APIS information is checked against the Interagency Border Inspection System (IBIS) database. IBIS is a combined Federal law enforcement database consisting of records from the Department of State, INS, Customs Service, and other agencies. IBIS, when used in conjunction with APIS, prevents entry into the United States by illegal aliens, and persons wanted on visa or customs violations. APIS information is also cross-checked with Federal Bureau of Investigation (FBI) and State Department wanted persons files.

A new voluntary programs encourages air carriers to submit APIS manifests for flights departing from the United States for international destinations. The INS is developing and testing various database systems to monitor more closely foreign nationals with U.S. visas. The outbound APIS program allows authorities to confirm when foreign nationals with visas leave the United States when their documents expire. Voluntary APIS is also being used on limited domestic flights.

Since its inception, over 200 million passengers have been processed through the APIS system.

FURTHER READING:

ELECTRONIC:

Bureau of Citizenship and Immigration Services. INSPASS. March 1, 2003. <http://www.immigration.gov/graphics/howdoi/inspassloc.htm> (April 14, 2003).

Department of Homeland Security. April 2, 2003. <http://www.dhs.gov/dhspublic/index.jsp> (April 11, 2003).

United States Department of Homeland Security. Immigration Information, INSPASS. March 4, 2003. <http://www.immigration.gov/graphics/shared/howdoi/inspass.htm> (April 9, 2003).

United States Department of Homeland Security. Bureau of Citizenship and Immigration Services, PORTPASS. March 11, 2003. <http://www.immigration.gov/graphics/howdoi/portpass.htm> (April 9, 2003).

SEE ALSO

IBIS (Interagency Border Inspection System)
IDENT (Automated Biometric Identification System)
INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)
NAILS (National Automated Immigration Lookout System)
PORTPASS (Port Passenger Accelerated Service System)
SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)

Archeology and Artifacts, Protection of during War

ADRIENNE WILMOTH LERNER

Plundering is a practice as ancient as warfare itself. With the development of the world's great civilizations, the proverbial "spoils of war" often included national and cultural treasures, including priceless art and antiquities. The looting of exotic, foreign treasure filled the national coffers and museums of the victorious, while depleting the vanquished of tangible remnants of their history. The evolution of warfare, both technical and philosophical, altered international perceptions on the seizure of cultural goods. However, today's international bans on the looting and trafficking of antiquities, as well as the expectation that cultural sites remain protected during wartime, took three centuries to come to fruition.

The Colonial Era: The Beginning of Modern Conflicts over Wartime Plunder

The discovery of the New World by European explorers sparked a fierce competition among European nations to obtain territories abroad. Colonialism was fueled by the desire to fill national coffers, through trade, agriculture, or plunder. In the sixteenth and seventeenth centuries, exaggerated rumors of indigenous wealth and stores of gold encouraged plunder of Indian villages. Almost immediately, the demand for exotic objects d'art from the Americas swelled, as wealthy aristocrats clamored for Incan jewelry and Mayan antiquities.

In the 1790s, the birth of the academic discipline of archaeology spurred further interest in antiquities. Archaeologists conducted expeditions, excavating sites and capturing the popular imagination with the artifacts they found. The development of archaeology occurred with a contemporary revival in colonialism. In the early 1800s, independence movements drove European colonial powers from much of the Americas. Seeking other venues for expanding colonial markets, obtaining natural resources, and extending political influence, several European nations, including Britain, France, and the Netherlands, turned to colonial endeavors in Africa and Asia. As imperial powers expanded, so too did public interest in exotic artifacts. During the mid-nineteenth century, Chinese porcelains, costumes, and figurines were popular goods in Holland, Britain, and France. At the turn of the twentieth century, British collectors favored artifacts and antique jewels from Egypt and India. Colonialism provided a means for such cultural resources to be trafficked to Europe for sale or display in museums.

Even in times of warfare, such as the Napoleonic Wars and wars of colonial expansion, cultural resources were a prime consideration. Many western armies freely destroyed indigenous or ancient sites of cultural significance in the heat of battle—a practice that later devastated the many Medieval and Renaissance treasures in Europe itself during World War I. Western archaeologists and antiquities collectors, in an era before the discipline became highly scientific, looted sites to locate artifacts. Antiquities of value were removed from their national contexts, and sent back to museums in Europe. Napoleon employed special spies to locate and gather the best art and antiquities in conquered nations to send back to Paris. In Britain, ancient Egyptian goods and mummies proved immensely popular with collectors and museum audiences. Later, French wars in Indochina created a popular vogue of Buddhist relics and ancient Chinese artifacts.

Even though many of the great finds of the last three hundred years were considered spoils of war or colonialism, the removal of artifacts from their national contexts in the eighteenth and nineteenth centuries was illustrative of the colonial worldview. Many archeologists, antiquities collectors, and museum collectors considered the removal of foreign treasures to European museums a chief means of preservation. They considered themselves better stewards of the world cultural resources, believing that European collections offered better access for scholars, and a safer environment for the storage of the artifacts themselves.

Changing practices in the discipline of archaeology, which is now highly specialized, scientific, and wholly dependent on the provenience (location and context) of cultural goods, and the fall of colonialism, facilitated the end of widespread plundering of African and Far Eastern antiquities to Western museums. The demise of nineteenth century values regarding antiquities, however, raised new questions about the ownership of goods plundered during past conflicts.

One of the most complicated cases in the international dispute over antiquities repatriation, the giving back of antiquities or works of art to their original owner, is that of the British-owned Elgin Marbles. The stone sculptures hail from the Greek Parthenon, but were purchased by Lord Elgin, a British collector, from Greek authorities, shortly before Greece erupted in a decades-long series of wars. The Parthenon was in dubious condition, and Elgin took the statues in an allegedly legal transaction. After the establishment of international laws governing the repatriation of both wartime and peacetime plundered goods, the Greek government appealed to the British History Museum for the return of the Elgin Marbles. The legal battle remains ongoing, intensified by Greece's desire to repossess the statues before the 2004 Olympics in Athens, but Britain has retained ownership of the prized antiquities.

Plunder and Warfare in the Twentieth Century

In the early twentieth century, the question of wartime plunder of cultural resources came to the fore in Europe. The outbreak of World War I challenged national art and antiquities holdings in a new manner. The advent of total war threatened archaeological sites, buildings, museums, and other national treasures. More intense and powerful weaponry leveled entire cities. Improvements in transportation permitted a more swift, and expansive, invasion force. Long before the fighting of World War I bogged down in the stalemate of the trenches, museum curators in France, Belgium, and Germany endeavored to protect national art and antiquities treasures. At the Louvre, France's premier art and antiquities museum, the staff evacuated the contents of the museum into secret tunnels and antechambers. Some works were sent to various homes throughout France for protection during the war. A special guard force was established to look after the hidden works, and catalog those sent to safe houses. After the Allied victory in 1918, most all of the works were returned to the Louvre, and only a few were captured by German forces or lost.

Plundering of national museums, on both sides of the conflict, was kept to a minimum in Western Europe. However, the fall of the Austro-Hungarian Empire prompted ethnic regional resistance groups to steal some works, many previously plundered from various small nations subsumed into the empire, from Austria. In Russia, the 1917 Revolution prompted wide-scale looting of treasures from deposed aristocrats and the czar's family. Some treasures ended up in Soviet museums, but more were sold to private collectors in the West willing to pay premium prices for the contraband goods. For decades, Soviet intelligence employed special forces to track and locate stolen Russian art treasures, reclaiming many that ended up in private homes and museums in Eastern Europe.

When World War II erupted in Europe in 1939, many governments embarked on well-orchestrated efforts to protect national treasures from wartime plunder. Most nations perceived an acute threat to cultural resources from Nazi Germany. As Nazi Germany grew in power throughout the 1930s, the nation made plunder of the world's antiquities and art treasures a strategic priority. The Nazi government employed archaeologists, art historians, antiquities specialists, and agents of espionage to locate and seize foreign treasures, especially in Egypt and the Middle East. When war broke out in Europe, Nazi invasion plans for neighboring nations included special provisions for the theft of national treasures, and their relocation to Germany. A methodical bureaucratic system was established to facilitate the cataloging of Nazi wartime plunder—ironically, after Germany's defeat, this careful inventory system aided international repatriation and reclamation efforts.

In France, museum staff once again emptied the Louvre in advance of German occupying forces. The most valuable works of the Louvre were sent into hiding in a variety of locations throughout the nation, trafficked by members of the French Resistance. When Nazi agents broke into the museum to plunder their spoils of war, the galleries were largely empty. After the first weeks of the London Blitz, the German bombing campaign against London, British officials moved the international treasures of the nation's famous museums to underground storage and to safe houses in Wales, Northern England, and Scotland. Many European nations sent valuables to the United States, Australia, or neutral Switzerland for protection. Despite the success of Britain and France in protecting national treasures, the Nazi government plundered antiquities throughout Europe, Africa, and the Middle East. Wartime campaigns of total warfare devastated cultural sites in Belgium, France, the Netherlands, Poland, Germany, and Italy.

The Holocaust: The Great Theft and the Establishment of International Cultural Resource Protections

The Nazis directed their effort to plunder the world's art and antiquities not only against rival nations, but also at Europe's Jews. During the Holocaust, the German government orchestrated not only the systematic execution of Europe's Jewish population, but also the plunder of all of their goods. In Germany, France, and Northern Europe, wealthy Jews possessed extensive collections of art and antiquities. Some were the major benefactors of national museums, and a few were among some of Europe's leading art and antiquities brokers. Holocaust plunder, known as the Great Theft, was less extensively catalogued by German authorities. The plundered goods, formerly located in private collections, were not catalogued by museums. Thus, the total loss of priceless cultural resources during the Holocaust is immeasurable.

Though the human tragedy of the Holocaust far outweighed devastation to art and antiquities, the Great Theft was addressed in the 1946 Nuremberg Trials of Nazi war criminals. Theft of personal and cultural property was added to the international standards for war crimes in the 1940s. Much of the stolen Holocaust art and antiquities remain in dispute. With few surviving original owners left to claim stolen goods, many items were subsequently repatriated to their nation of origin, returned to the nation of plunder, or were sold in private art markets. However, the theft of cultural resources during the Holocaust prompted the formation of strict international policy regarding the treatment of art and artifacts in times of both war and peace.

Protecting art, artifacts, and cultural sites today. A 1970 United Nations Educational, Scientific and Cultural Organization (UNESCO) convention outlined international policy on the protection of artifacts and cultural sites during both war and peacetime. The convention recommended the repatriation of all antiquities, even those acquired from former colonies. In the 1980s, several UN member nations signed a treaty limiting the destruction of cultural sites during military actions. Archaeologists, art scholars, and antiquities specialists successfully lobbied for a ban on the plunder and traffic of illegally obtained artifacts, or removing any antiquities from their context without express permission of national and local governments. INTERPOL now maintains a special force to investigate art and artifact crimes, including those perpetrated during wartime.

A change in war ethos in the West prompted swift reforms of how military campaigns dealt with cultural resources during war. Cultural sites are generally avoided in battle plans, and many governments maintain both civilian and military intelligence forces trained to protect cultural goods. In the recent conflict in Iraq, however, the national museum, containing a vast wealth of antiquities from ancient Mesopotamia, was looted before guard forces were established. The rampant looting raised questions about the enforcement of international anti-theft laws, the effectiveness of military protection, and the readiness of international intelligence forces to track down the stolen goods. Subsequently, many of the artifacts feared initially stolen or lost were recovered from hidden vaults.

The incident in Baghdad also brought to the attention of the international media one of the most basic concerns of preservationists. The growth of the modern antiquities market, and the continued international hunger for plundered goods, has elevated the price of antiquities to enticingly high levels. High prices encourage the looting

of cultural sites by local populations desperate for income. Despite international action, looting has become an increasing local phenomenon, but looters are better connected to dealers and antiquities markets. The Internet aided the proliferation of illegally obtained antiquities, but also helps law enforcement monitor the illegal cultural goods trade.

One of the greatest protections to archaeological sites and cultural resources during wartime is the continued development of "smart weapons," ammunition that is carefully guided to specific strategic targets and detonated to minimally impact surrounding areas. Smart weapons permit militaries to strike targets in close proximity to cultural sites. Use of smart weapons by Britain and the United States in the Iraq War minimized damaged to Baghdad's numerous museums, mosques, and cultural sites. However, these weapons are only developed, possessed, and used by a handful of the most developed nations. Less developed regions, many of which are prone to endemic conflict, rely on more conventional weapons and techniques of total warfare.

Today, the national governments of the United States, Canada, and the European Union maintain the most comprehensive intelligence forces devoted to the protection of the archaeological and art resources. In 1998, several European nations sent a special task force into the Balkans, in conjunction with UN operations in Bosnia, to track the trafficking and theft of cultural resources. Coalition nations from the Iraq War in 2003 have devoted intelligence resources to an international effort to recover goods stolen from the Iraqi museum. Thus far, the international intelligence community and INTERPOL have arrested persons suspected of trafficking Iraqi treasures in Europe, the United States, and Asia.

FURTHER READING:

BOOKS:

Brodie, Neil, and Kathryn Walker Tubb. *Illicit Antiquities: The Theft of Culture and the Extinction of Archaeology.* London: Routledge, 2002.

Feliciano, Hector. *The Lost Museum: The Nazi Conspiracy to Steal the World's Greatest Works of Art.* New York: Basic Books, 1987.

Simpson, Elizabeth. *The Spoils of War: World War II and Its Aftermath: The Loss, Reappearance, and Recovery of Cultural Property.* New York: Abrams, 1997.

SEE ALSO

Architecture and Structural Security
Document Forgery
Espionage and Intelligence, Early Historical Foundations
Forensic Geology in Military or Intelligence Operations
Interpol (International Criminal Police Organization)
Libraries and Information Science (NCLIS), United States National Commission
World War I
World War II

Architecture and Structural Security

JUDSON KNIGHT

Buildings have always stood under the threat of physical attack, but until the advent of organized terrorism in the latter twentieth century, most structural dangers were limited to fires, natural disasters, and acts of war. Since the early 1970s, however, it has become increasingly apparent to authorities in the West that their physical structures are potential targets for terrorist actions, especially bombings, even during peacetime. Such concerns have given rise to efforts by architects, engineers, and planners, sometimes working closely with government security experts, to create structures designed to meet two differing, almost contradictory, needs: security on the one hand, usability and aesthetics on the other.

Bombings of the 1990s

Among the most notable terrorist bombings of buildings prior to 2001 was the assault on the United States Marine barracks in Beirut, Lebanon, in October 1983, followed a decade later by a string of bombings throughout the 1990s: the first attack on the World Trade Center (WTC) in February 1993; the explosion of the Alfred P. Murrah Federal Building in Oklahoma City in April 1995; the bombing of Khobar Towers in Dharran, Saudi Arabia, in June 1996; and the attack on the U.S. embassies in Kenya and Tanzania in August 1998.

Death tolls differed, from fewer than ten in the case of the first WTC incident to several hundred in the Marine barracks bombing 10 years earlier. And although most of these were perpetrated by Middle Eastern terrorists—albeit from differing groups that collectively represented the breadth of the Islamic fringe—Oklahoma City was an exception, the work of American extremists. Yet, each bombing was alike in terms of basic method: the use of a truck, driven alongside the building or beneath it, to deliver explosives.

The conflict between comfort and safety. In order to create structures that could withstand such an attack, designers must confront a classic dilemma of architecture and structural security articulated by Cheryl Kent in the *New York*

Times. "At heart, the task involves what seems like a contradiction: designing a building that is secure from attack while affording the openness appropriate for a public building."

Prior to the 1970s, security was not the paramount consideration in architecture and therefore, comfort and the human touch remained preeminent considerations. Planners of the 1972 Olympic Village in Munich, Germany—wanting to avoid the appearance of an armed camp, with its potential evocations of Hitler and the 1936 Berlin Games—had created an open, friendly village that proved vulnerable to Palestinian terrorists. The subsequent assault by Black September left 11 Israeli athletes and one German policeman dead. Olympic officials learned from Munich and, thenceforth, greatly intensified the security measures surrounding the Games; likewise the planners of government buildings eventually learned from the terrorist attacks of the 1990s.

The Ronald Reagan building. The learning process was far from instantaneous, as illustrated by a look at the Ronald Reagan Building in Washington, D.C. It was completed in July 1997, a year after the Khobar Towers and a year before the Africa bombings. The first World Trade Center bombing and Oklahoma City were still fresh in memory as evidence that terrorism was no longer a phenomenon from which Americans on U.S. soil were exempt. Yet, a 1999 report by security experts at Sandia National Laboratories found that the building, which had run well over budget to finish at $818 million, was "highly vulnerable" to terrorist attack.

Several factors made the vulnerability of the Reagan Building particularly dismaying. There was its proximity to the White House and Capitol, combined with the large numbers of employees to be housed there. Additionally, it would serve as the headquarters of sensitive agencies such as the U.S. Customs Service, and the venue of high-security events such as the North Atlantic Treaty Organization 50th anniversary celebrations in April, 1999. Yet, the GSA, hoping to defray some of the costs by leasing space to the private sector for restaurants, shops, and convention facilities, had wanted to avoid creating a building that looked like an armed fortress.

The Oklahoma City Federal Campus. By contrast, a Chicago architectural firm managed to create a secure environmental—yet one that did not seem constricting to its inhabitants or visitors—in their design for Oklahoma City's Federal Campus. The new name was chosen to avoid any reference to "Federal Building," a term forever associated in local minds with the structure in Oklahoma City that had been destroyed, along with 168 people.

Design architects planned the site in such a way that, rather than lying hidden behind a protective plaza, the building fills the block on which it sits. This has the added benefit of addressing an aesthetic problem in the Oklahoma City downtown, which, like that of other sunbelt cities such as Atlanta or Houston, is pockmarked with empty lots. By building to the boundaries of the site, the Federal Campus conveys a sense of a populated environment that serves to invite traffic. Welcoming traffic was also apparently in the architects' considerations when they fought off security planners' attempts to close off streets around the building, a measure that might have kept away the public.

One of the few obvious signs of protective considerations in the design is the lack of glass in the outer perimeter of the Federal Campus. The building does have extensive glass areas, but these are inside the protected courtyard, and the glass itself is reinforced—rather like that of a car windshield—so that it would shatter rather than break in the face of concussive force. Walls on either side of the lobby are made to create a powerful aesthetic effect, while protecting office workers in the event of an explosion.

Designing and Protecting the Post-September 11, 2001, World

Ironically, in its September, 2001 issue, which went to press before the bombings, *Signal* reported that GSA was testing a risk assessment and property analysis software product called RAMPART as a means of determining buildings' vulnerabilities to terrorism. Designed at Sandia, RAMPART made it possible to study a number of threats, both natural and manmade, and allowed users to assess buildings with a point-and-click walk-through assessment tool that took less than two hours.

After the World Trade Center terrorist attack, the idea that such software could get into the wrong hands prompted a joint statement by the American Institute of Architects (AIA) and the GSA to immediately report any suspicious requests to the appropriate local FBI field office. Just as terrorists' strange requests at flight schools—e.g., their desire to learn how to fly a plane, but not how to land—should have, and in some cases did raise red flags, the AIA and GSA warned architects, engineers, and others concerning requests for intricately detailed plans of major buildings.

Months earlier, an AIA member firm had received several e-mail messages from an alleged student in Egypt who requested plans that would show extremely specific information about conduits, duct work, wiring, risers, and other aspects of a particular building. Acting with prescience (given that this was before September 11), the firm turned the requests over to the FBI. The wisdom of such measures became all the more apparent after the March, 2003, capture of Khalid Sheikh Mohammed, a high-ranking al Qaeda figure who revealed that plans were in the works for attacks on structures ranging from the White

House and Israeli embassy in Washington, D.C. to bridges in Manhattan and the Sears Tower in Chicago.

In December, 2001, the FBI revealed that the World Trade Center terrorists might have actually used commercially available software to plot the destruction of the towers. Several hundred such programs were on the market at that time, although fewer than half a dozen would have been capable or portraying the effects of a plane crash in any detail.

Studying how the towers fell. During late 2001 and 2002, government and private investigators undertook studies to understand how a jetliner could have caused the collapse of the towers. Quickly, the investigators, including representatives of the American Society of Civil Engineers and the Federal Emergency Management Agency (FEMA), concluded that it was not the impact, but the heat from the burning jet fuel that weakened the steel. The National Institute of Standards and Technology (NIST), which later did its own study, found that the temperatures were not high enough to actually melt the steel, as had been originally assumed. The temperatures were sufficient however, to weaken the steel beams, which crumbled at the impact levels of the towers and, in turn, resulted in weight loads sufficient to crush the floors remaining below, resulting in the total collapse of the structures.

Those involved in the World trade Center site investigation also attributed part of the buildings' vulnerability to what had also been their strength, the use of exterior walls as support. In older skyscrapers such as the Empire State Building, support was at the building's core. This thicket of massive steel girders not only took up rentable interior space, but they had their structural shortcomings, including the fact that they did not prevent a building from swaying in the wind. In the WTC, the exterior columns were linked to the core with steel trusses that had been inadequately fireproofed in the building process. Surrounded only by light foam fireproofing and walled off with sheetrock rather than concrete, the trusses at the impact site were easily exposed by the twin plane crashes, leaving them vulnerable to melting or loss of integrity.

Building for the future. The GSA approved a wide range of designs in December, 2001, that seemed to have already taken into account the World Trade Center tragedy three months before. In fact, these were the result of the same post-Oklahoma City studies that yielded the Federal Campus earlier.

Among the $6 billion worth of projects released in a flurry of GSA approvals was a district courthouse for Miami. Unlike the Federal Campus, this building did sit back from the street, with the intervening space hosting an arboretum. Yet, the arboretum served a security purpose, and not only because it separated the building from the street. "Even if a truck got through the trees," architect Bernardo Fort-Brescia of Arquitectonica, the design firm, told the *Wall Street Journal,* "they would hit this undulating lawn. We've created an invisible barrier in the sense that it doesn't look like a wall."

Another courthouse, in Springfield, Massachusetts, solved the conflict of security versus aesthetics in a different fashion. Planners wanted local citizens to visit the courthouse frequently for community events, and if attendees had to pass through magnetometers and checkpoints upon entering, this would create a decidedly unfriendly environment. Instead, they separated the entry pavilion from the interior portion, with its security checkpoints hidden from view.

At the new headquarters for the Bureau of Alcohol, Tobacco, and Firearms (ATF) in Washington, designers had dealt with the problem of bollards, the stubby concrete posts that prevent vehicles from driving into buildings at street level. Although useful for security, they are typically far from pleasing visually, yet the architects of the ATF building managed to create bollards that were an exception to the rule. "Instead of looking like dragon's teeth," GSA commissioner for public buildings F. Joseph Moravec told the *Journal,* "there will be some really cool metal bollards. They'll have an antique, almost Edwardian look."

In at least one spot in Washington, D.C., the GSA's "post-9/11" design criteria had been implemented before the World Trade Center attacks. This was the Pentagon, where architects of a remodeling project had used new techniques and materials intended to ensure that, in the event of a devastating attack, the building section would collapse progressively, rather than in a heap. Architects had also used shatterproof glass and other materials because, as Moravec noted, "One of the terrible lessons of Oklahoma City was that when a bomb goes off near a building, it's not so much the blast that kills people. It's that the explosion creates flying elements, pieces of walls and glass that kill." In the remodeled portion of the Pentagon, "When the blast hit the wall, the wall itself didn't become a weapon. There's no question that the glass panels there saved a lot of lives."

FURTHER READING:

PERIODICALS:

Aveni, Madonna. "Software Analyzes Potential Threats to Buildings." *Civil Engineering* 71, no. 10 (October 2001): 36.

Brouwer, Greg. "Oklahoma City Complex Will Usher in New Design Criteria." *Civil Engineering* 72, no. 3 (March 2002): 16.

Dunlap, David W. "Architects Put on the Alert over Requests That Are Rare." *New York Times.* (October 4, 2001): B8.

Grant, Peter. "Plots and Ploys." *Wall Street Journal.* (December 26, 2001): B4.

Kent, Cheryl. "A Safer Federal Building for Oklahoma City." *New York Times.* (August 22, 1999): 34.

Ottaway, David B. "Reagan Building Vulnerable to Attack." *Washington Post.* (March 8, 1999): A1.

"RAMPART Assesses Threats." *Signal* 56, no. 1 (September 2001): 7.

Salamon, Julie. "A Detective-Story Approach to the Twin Towers' Collapse." *New York Times.* (April 30, 2002): E1.

Smith, Ray A. "The Aesthetics of Security—Building Owners, Architects Seek to Make Properties Safer Without Look of a Fortress." *Wall Street Journal.* (February 19, 2003): B1.

Solis, Suzanne Espinosa. "Software May Have Mapped N.Y. Hit." *San Francisco Chronicle.* (December 12, 2001): A11.

Watts, John M., Jr. "Our Changing World." *Fire Technology* 38, no. 2 (April 2002): 99–100.

SEE ALSO

Computer Modeling
FEMA (United States Federal Emergency Management Agency)
General Services Administration, United States
Kenya, Bombing of United States Embassy
Khobar Towers Bombing Incident
NIST (United States National Institute of Standards and Technology)
Sandia National Laboratories
September 11 Terrorist Attacks on the United States
World Trade Center, 1993 Terrorist Attack

Area 51 (Groom Lake, Nevada)

Area 51 is the popular name of a secret military facility at Groom Lake, Nevada, approximately 90 miles north of Las Vegas. The 6-by-10 mile rectangular air base lies within the Switzerland-sized boundaries of Nellis Air Force Base, and has served as a testing ground for "black budget" (top-secret) military prototype aircraft since the mid-1950s. Area 51 is also a well-known folk symbol of an assumed government conspiracy to cover up information on UFOs and extraterrestrial life.

The United States government has never publicly discussed the existence or purpose of the Groom Lake base, but historical accounts chronicle the site's long history as a preliminary testing ground for the U.S. military's most secret aircraft. The U-2 Spy plane, A-12 and SR-71 Blackbird supersonic reconnaissance jets, and F-117A and B-2 Stealth fighters were all tested at the site before production, as was a reverse-engineered version of a Vietnam War-era Russian MIG-21. Development and testing of secret military aircraft and Unmanned Arial Vehicles (UAVs) likely continues at Area 51 today.

The secrecy surrounding Groom Lake has piqued public interest since 1955, when the Central Intelligence Agency and Lockheed Skunk Works chose the remote desert area as a testing ground for the U-2. President Eisenhower signed Executive Order 10633 to restrict a rectangle of airspace over the base that year, and the Department of the Interior withdrew a 60-square-mile rectangle of land beneath the airspace from public use in 1958. Today, the so-called "Groom box" includes a 22-by-20 nautical mile rectangle of restricted airspace, the original 60 square mile base, and a large area of surrounding land with enforced public entry and viewing restrictions.

The present popular fascination with Area 51 bloomed in 1989 when KLAS-TV in Las Vegas broadcast a series of interviews with Robert Lazar, a self-proclaimed aerospace engineer who maintained that he had been hired to help reverse-engineer an alien spacecraft at the Papoose Lake facility near Groom Lake. Lazar asserted that the United States government had recovered a downed extraterrestrial spacecraft and stored it in an underground bunker at Area 51. Lazar's bizarre story elicited support from the community of UFO and alien conspiracy theorists based in Roswell, New Mexico, and ignited public curiosity. The April 1994 issue of *Popular Science* magazine carried a satellite image of Groom Lake on its cover and featured an in-depth article on the military history of the facility. Since then, Area 51 has become a science-fiction staple. The site played a role in several episodes of the FOX television's popular series "The X-Files" and was featured in the 1996 movie "Independence Day." Though the United States military often collaborates with the entertainment industry, it has never sanctioned a project involving Area 51.

FURTHER READING:

BOOKS:

Rich, Ben and Leo Janos. *Skunk Works.* New York: Bantam, 1994.

ELECTRONIC:

Area 51 Research Center. "Area 51: Military Facility, Social Phenomenon and State of Mind." Glenn Campbell. January, 2000. <http://www.ufomind.com/area51/> (December 5, 2002).

Airmen, Magazine of the United States Air Force. "Flights, Camera, Action!" June, 1997. <http://www.af.mil/news/airman/0697/index.html> (December 5, 2002).

SEE ALSO

Aviation Intelligence, History
Stealth Technology
Unmanned Aerial Vehicles (UAVs)

Argentina, Intelligence and Security

Since gaining its independence from Spain in 1816, Argentina has struggled to maintain stable, democratic rule.

Conflict between the military and government factions is endemic. In 1946, the election of President Juan Domingo Peron began a period of authoritarian rule and heightened tensions between military and civilian forces. A military junta overthrew the government again in 1976. Both regimes employed civilian and military intelligence agencies in domestic espionage against Argentinean citizens and persecuted political dissidents. Democratic rule was restored in 1983. The new government overhauled government structure, separating civilian and military agencies into specialized, relatively autonomous units. In 1992, the government modernized and redesigned the nation's intelligence system.

Argentina's intelligence community is divided into civilian and military branches. The civilian intelligence system operates under the direction of the executive branch of the government. The keystone of this network is the National Intelligence Center (CNI). The CNI is responsible for gathering information from various intelligence agencies and coordinating daily operations. In recent years, however, the power of the CNI has greatly diminished. The Office of the State Intelligence Secretary (SIDE) assumed many CNI duties.

SIDE is the oldest Argentinean intelligence agency. Reporting directly to the President, SIDE is charged with culling domestic and foreign intelligence information with which to brief members of the executive branch. The agency also directs the nation's counterintelligence program.

Domestic security was the primary concern of Argentinean legislators who pushed for intelligence reform in the early 1990s. To this end, passage of the Internal Security Law of 1992 created the domestic security service, the National Direction of Internal Intelligence. The agency, a subsidiary of the Ministry of the Interior, created national security policy and coordinates the protection of national interests with the aid of intelligence services and law enforcement agencies, such as the National Gendarmerie and Federal Police.

Military intelligence is coordinated by the Joint Staff of the Armed Forces, and a subcommittee known as J-2 Intelligence. The committee reports to the executive, and like all military intelligence organizations is subject to congressional oversight review, but remains largely autonomous. Each branch of the Argentinean military, the Air Force, Army, and Navy, maintains its own intelligence services.

A car moves along the Extraterrestrial Highway, a roadway that runs along the eastern border of Area 51, a military base on the Nevada test site that the U.S. government has only recently admitted "officially" exists. AP/WIDE WORLD PHOTOS.

In 2002, Argentina again began a period of political instability, in large part due to an economic crisis gripping the country. Until government stability is restored, the future of Argentina's intelligence agencies is uncertain. As in past periods of unrest, military intelligence and security agencies have gained power and influence, eliciting the concern of Argentinean civilians and members of the international community.

Argonne National Laboratory

K. LEE LERNER

Argonne National Laboratory is operated by the University of Chicago for the U.S. Department of Energy (DOE). Located in Argonne, Illinois, the lab is divided operationally into five principle divisions: Physical, Biological & Computing Sciences; Advanced Photon Source; Energy & Environmental Science & Technology; Engineering Research; and Operations.

Argonne scientists collaborate on several projects related to nuclear safety. Argonne's International Nuclear Safety Center (INSC) is dedicated to improving safety related technology and safety protocols for nucler reactors—including reactors in the former Soviet Union. Funded by DOE's Office of Nonproliferation and National Security, INSC scientists maintain an extensive database related to a variety of nuclear facilities. The INSC database is organized so that researchers can quickly access site-specific information on reactors around the world.

Argonne scientists provide technical support to several agencies involved in stemming proliferation or use of weapons of mass destruction. As of 2003, Argonne's national security related programs supported research dedicated to developing technology—and providing expert guidance—related to arms control and nuclear, chemical, and biological counter-terrorism.

Argonne developed technologies include methods to track nuclear fuels and to support nuclear waste cleanup of spent fuels.

Argonne scientists have developed an electrometallurgical treatment process to handle spent nuclear fuels. The treatment process uses electrorefining techniques that separate uranium, radioactive wastes, and inert materials in sodium bonded metallic fuels. In preparing nuclear waste for disposal, the electrometallurgical treatment process allows the isolation and removal of uranium and also allows the remaining waste into a ceramic or a metal alloy by heating and compressing a composite of borosilicate glass and zeolite (a mineral that incorporates fission waste products). Components of the metal alloy are derived from the steel cladding used to encase the fuel in the reactor. By restricting plutonium access—binding it with waste products—the plutonium is placed in a form that reduces or eliminates its potential use in a nuclear weapon.

In support of several agencies, Argonne scientists are capable of providing field measurements of radiation exposure dangers and of guiding decontamination efforts associated with reactor decontamination and decommissioning. Part of the decommissioning effort is dedicated to ensuring safe disposal of nuclear fuels so that the fuels can not be used to manufacture nuclear weapons.

Argonne engineers collaborate on efforts to develop sensitive detectors capable of identifying concealed nuclear materials.

Argonne personnel provide technical expertise to Federal Bureau of Investigation counterterrorism operations and aid in domestic infrastructure assurance programs designed to improve security at critical U.S. infrastructure sites. For example, Argonne's PROTECT system, developed by the Decision and Information Sciences Division, features an integrated detection, communication and response program to secure subways against chemical attacks.

Argonne research also includes efforts to improve instruments and sensors capable of detecting chemical and biological agents. As a part of the Joint Chemical Aid Detector Program, Argonne researchers developed portable cyanide-gas microsensors. Engineers are especially interested in developing hypersensitive detectors capable of identifying trace evidence of dangerous chemical or biological agents and developed a series of portable biochip microarrays that are capable of detecting bioagents, including anthrax bacterium.

Argonne's Advanced Photon Source (APS) allows study of the 3-D structure of toxins—including Anthrax toxins. Micro Array of Gel-Immobilized Compounds or MAGIC chips were developed by Argonne researchers to identify biological pathogens and disease related genetic mutations.

FURTHER READING:

ELECTRONIC:

Environmental Measurements Laboratory. National Security. <http://www.eml.doe.gov/> (March 16, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <http://www.dhs.gov/dhspublic/display?theme=27&content=374> (March 23, 2003).

SEE ALSO

Brookhaven National Laboratory
DOE (United States Department of Energy)
Environmental Measurements Laboratory
Lawrence Berkeley National Laboratory
Lawrence Livermore National Laboratory (LLNL)
Los Alamos National Laboratory

President Bush, center, gets a look at new weapons in the war on terror during a visit to the Argonne National Laboratory in Argonne, Illinois. AP/WIDE WORLD PHOTOS.

NNSA (United States National Nuclear Security Administration)
Oak Ridge National Laboratory (ORNL)
Pacific Northwest National Laboratory
Plum Island Animal Disease Center
Sandia National Laboratories

Armed Islamic Group (GIA)

An Islamic extremist group, the Armed Islamic Group (GIA) aims to overthrow the secular Algerian regime and replace it with a fundamentalist Islamic state. The GIA began its violent activity in 1992 after Algiers voided the victory of the Islamic Salvation Front (FIS)—the largest Islamic opposition party—in the first round of legislative elections in December 1991.

Organization activities. GIA frequently attacks civilians and government workers in Algeria. Between 1992 and 1998, the GIA conducted a terrorist campaign of civilian massacres, sometimes wiping out entire villages in its area of operation. Since announcing its campaign against foreigners living in Algeria in 1993, the GIA has killed more than 100 expatriate men and women—mostly Europeans—in the country. The group uses assassinations and bombings, including car bombs, and it is known to favor kidnapping victims and slitting their throats. The GIA hijacked an Air France flight to Algiers in December 1994. In late 1999, a French court convicted several GIA members for conducting a series of bombings in France in 1995.

Precise numbers of the GIA members are unknown, but are estimated at about 200 members. Algerian expatriates, some of whom reside in Western Europe, provide some financial and logistic support to GIA. In addition, the Algerian government has accused Iran and Sudan of supporting Algerian extremists.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Arms Control, United States Bureau

The Bureau of Arms Control is an office of the United States Department of State devoted to policy on military arms of all types, from conventional to nuclear. It falls under the U.S. Arms Control and Disarmament Agency, which Congress placed under State Department control in 1999. Among its functions is the implementation of existing arms agreements. The bureau also serves the secretary of state in an advisory capacity, providing the secretary with information on a variety of national security issues related to arms control.

The Bureau of Arms Control was a product of the merger between the United States Arms Control and Disarmament Agency (created by Congress in 1961) and the State Department on April 1, 1999. Thenceforth, the newly created bureau, along with the bureaus of Nonproliferation, Verification and Compliance, and Political-Military Affairs, would be subordinate to the undersecretary of state for Arms Control and International Security. Answering to the undersecretary on behalf of the Bureau of Arms Control is an assistant secretary.

Areas of responsibility for the Bureau of Arms Control include developing policy with regard to use of conventional, chemical/biological, and nuclear forces and arms. The bureau is also charged with supporting negotiations for arms control agreements, and for implementing existing agreements. It further supports the secretary of state on relevant national security issues, such as those involving testing of nuclear weapons or the development of missile-defense systems.

The bureau's mission extends beyond these responsibilities, however, to the most creative area in the field of arms control: the negotiation of new agreements. For example, the bureau helped lead efforts toward the creation of the Moscow Treaty on strategic offensive reductions in May 2002.

■ FURTHER READING:

BOOKS:

Butler, Richard. *The Greatest Threat: Iraq, Weapons of Mass Destruction, and the Crisis of Global Security.* New York: Public Affairs, 2000.

Forsberg, Randall. *Nonproliferation Primer: Preventing the Spread of Nuclear, Chemical, and Biological Weapons.* Cambridge, MA: MIT Press,1995.

ELECTRONIC:

U.S. Department of State Bureau of Arms Control <http://www.state.gov/t/ac/> (December 30, 2002).

SEE ALSO

NNSA (United States National Nuclear Security Administration)

Army for the Liberation of Rwanda (ALIR)

The Army for the Liberation of Rwanda (ALIR) also operates as, or is known as, Interahamwe, Former Armed Forces (ex-FAR).

The FAR was the army of the Rwandan Hutu regime that carried out the genocide of 500,000 or more Tutsis and regime opponents in 1994. The Interahamwe was the civilian militia force that carried out much of the killing. The groups merged and recruited additional fighters after they were forced from Rwanda into the Democratic Republic of Congo (then Zaire) in 1994. They are now often known as the Army for the Liberation of Rwanda (ALIR), which is the armed branch of the PALIR or Party for the Liberation of Rwanda. The group seeks to topple Rwanda's Tutsi-dominated government, reinstitute Hutu-control, and, possibly, complete the genocide. In 1996, a message allegedly from the ALIR threatened to kill the United States ambassador to Rwanda and other U.S. citizens. In 1999, ALIR guerrillas, critical of alleged U.S.-U.K. support for the Rwandan regime, kidnapped and killed eight foreign tourists including two U.S. citizens in a game park on the Congo-Uganda border. In the current Congolese war, the ALIR is allied with Kinshasa against the Rwandan invaders. Several thousand ALIR regular forces operate alongside the Congolese army on the front lines of the Congo civil war, while a like number of ALIR guerrillas operates behind Rwandan lines in eastern Congo closer to the Rwandan border and sometimes within Rwanda.

FAR generally operates in the Democratic Republic of the Congo and Rwanda, but has operated in Burundi. The Democratic Republic of the Congo provides ALIR forces in Congo with training, arms, and supplies.

■ FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Army Medical Research Institute of Chemical Defense (USAMRICD).

SEE *USAMRICD (United States Army Medical Research Institute of Chemical Defense).*

Army Medical Research Institute of Infectious Diseases (USAMRIID).

SEE *USAMRIID (United States Army Medical Research Institute of Infectious Diseases).*

Army Security Agency

■ JUDSON KNIGHT

The Army Security Agency (ASA) provided the United States Army with signal intelligence and security information from 1945 to 1976. During the 1960s, ASA played a key role in the Vietnam conflict, a role symbolized by the fact that an ASA operative was the first soldier killed in the war.

For almost as long as there has been viable electronic communication, the U.S. military has been concerned with the field of signals intelligence (SIGINT): information gathered from the interception, processing, and analysis of electronic communications. The first SIGINT efforts in World War I were informal, and only in 1930 did the army organize the first permanent SIGINT organization, the Signal Intelligence Service (SIS).

In 1943, the army renamed SIS as the Signal Security Agency, or SSA. On September 15, 1945, less than two weeks after the end of World War II, SSA became the Army Security Agency. Commanded by the director of military intelligence for the army, the newly formed office possessed broad powers, a fact made evident by its wide geographic presence: in addition to untold fixed sites, or field stations, across the globe, it also maintained significant theatre headquarters in both Europe and east Asia.

Four years after its formation, in 1949, the ASA was placed—along with its navy and air force counterparts—under the new Armed Forces Security Agency (AFSA). Though AFSA was a forerunner of the National Security Agency (NSA; formed in 1951), unlike NSA, AFSA had little actual power. Therefore, the reorganization had little effect on ASA operations other than the reassignment of most ASA civilian personnel to AFSA. ASA, meanwhile, continued its duties in the field, and would play a key intelligence role in the conflicts of the 1950s and 1960s.

ASA in Korea and Vietnam

As a result of needs created by the Korean War, ASA expanded its operations, and deployed numerous tactical units to support the army on the ground. The Korean conflict saw the first use of groups and battalions in the ASA structure, a symbol of its growth during wartime. In 1955, ASA expanded its mission to include electronic intelligence and electronic warfare functions that had formerly been the responsibility of the signal corps. Because its role now encompassed more than intelligence and security, it was reassigned from G-2 (military intelligence) to the U.S. Army chief of staff.

The first ASA personnel arrived in Vietnam on May 13, 1961, to set up a post at Tan Son Nhut Air Base in South Vietnam. Assigned to the 3rd Radio Research Unit (RRU), ASA personnel were chiefly concerned with direction-finding (DF) operations to locate Viet Cong transmitters operating in South Vietnamese territory. On December 22, 1961, a Viet Cong ambush outside the capital city of Saigon claimed the life of Specialist Fourth Class James T. Davis, a DF operator who became the first of more than 50,000 American soldiers killed in Vietnam during the next 11 years.

Davis's death pointed up the dangers for the DF operator in Vietnam: because of the difficulties of wave propagation in the thick southeast Asian jungles, the DF operator had to be close to the transmitter to detect it. The solution was an airborne DF platform, the first of which ASA deployed in March 1962. In 1965, as the U.S. presence in Vietnam reached its height, the 509th Radio Research Group replaced the 3rd RRU, and ASA personnel in country numbered as many as 6,000. The agency itself had grown to include some 30,000 personnel, and in 1964 had become a major army field command.

As the Vietnam conflict drew to a close, however, ASA began to contract rapidly. By 1975, reorganization

had effectively ended its existence, and it was formally disbanded on the last day of 1976. On January 1, 1977, a new security and intelligence command known as Headquarters, U.S. Army Intelligence and Security Command, replaced ASA.

■ FURTHER READING:

BOOKS:

Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: From the Cold War through the Dawn of a New Century.* New York: Doubleday, 2001.

ELECTRONIC:

Army Security Agency Online. <http://www.asa.npoint.net> (December 30, 2002).

Origins of the Army Security Agency and INSCOM. <http://www.nsa.gov/display/c130/ru8_asa.html> (December 30, 2002).

SEE ALSO

Codes and Ciphers
Cryptology, History
SIGINT (Signals Intelligence)

'Asbat al-Ansar

'Asbat al-Ansar—the Partisans' League—is a Lebanon-based, Sunni extremist group, composed primarily of Palestinians, which is associated with Osama Bin Ladin. The group follows an extremist interpretation of Islam that justifies violence against civilian targets to achieve political ends. Some of those goals include overthrowing the Lebanese government and thwarting perceived anti-Islamic influences in the country.

Organization activities. 'Asbat al-Ansar has carried out several terrorist attacks in Lebanon since it first emerged in the early 1990s. The group carried out assassinations of Lebanese religious leaders and bombed several nightclubs, theaters, and liquor stores in the mid-1990s. The group raised its operational profile in 2000 with two dramatic attacks against Lebanese and international targets. The group was involved in clashes in northern Lebanon in late December, 1999, and carried out a rocket-propelled grenade attack on the Russian embassy in Beirut in January 2000.

'Asbat al-Ansar commands about 300 hundred fighters in Lebanon. The group's primary base of operations is the 'Ayn al-Hilwah Palestinian refugee camp near Sidon in southern Lebanon, and it is thought that they receive money through international Sunni extremist networks and Osama Bin Ladin's al-Qaida network.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Asilomar Conference

Soon after the discovery in 1970 of the first restriction enzyme by American microbiologist Hamilton Smith, it became possible to combine DNA from different sources into one molecule, producing recombinant DNA. Concern by scientists and lay people that some of this recombinant technology DNA might be harmful to humans—either by unintentional or deliberate release or recombinant DNA into the environment—prompted the research to stop until scientists could evaluate its risks.

In February 1975, over 100 internationally respected molecular biologists met at the Asilomar conference center in California. There, they decided upon a set of guidelines to be followed by all scientists doing recombinant DNA research. They considered each class of experiments, and assigned it a level of risk: minimal, low, moderate, or high. Each level of risk required a corresponding set of containment procedures designed to minimize the chance of vectors (carriers) containing recombinant DNA molecules from escaping into the environment where they could potentially harm humans or other parts of the ecosystem. Because these projected experiments had never been done, assignment to a risk category was, of course, somewhat speculative and subjective. Accordingly, the potential risks were arrived at by estimate.

At all risk levels, the guidelines called for the use of biological barriers. Bacterial host cells should be from strains unable to survive in natural environments (outside the test tube). Vectors carrying recombinant DNA, including plasmids, bacteriophages, and other viruses, were to be nontransmissible and also unable to survive in natural environments.

For experiments having minimal risk, the guidelines recommended that scientists follow general microbiology

safety procedures. These included not eating, drinking, or smoking in the lab; wearing laboratory coats in the work area; and promptly disinfecting contaminated materials.

Low risk procedures required a bit more caution. For example, procedures producing aerosols, such as using a blender, were to be performed under an enclosed ventilation hood to eliminate the risk of the recombinant DNA being liberated into the air.

Moderate risk experiments required the use of a laminar flow hood, the wearing of gloves, and the maintenance of negative air pressure in the laboratory. This would ensure that air currents did not carry recombinant DNA out of the laboratory.

Finally, in high risk experiments, maximum precautions were specified. These included isolation of the laboratory from other areas by air locks, having researchers shower and change their clothing upon leaving the work area, and the incineration of exhaust air from the hoods.

Certain types of experiments were not to be done at all. These most potentially dangerous experiments included the cloning of recombinant DNA from highly pathogenic organisms or DNA containing toxin genes. Also forbidden were experiments involved the production of more than 10 liters of culture using recombinant DNA molecules that might render the products potentially harmful to humans, animals, or plants.

The scientists at the Asilomar conference also resolved to meet annually to re-evaluate the guidelines. As new procedures were developed and safer vectors and bacterial cells became available, it became possible to re-evaluate and relax some of the initially stringent and restrictive safety standards.

■ FURTHER READING:

PERIODICALS:

Barinaga, Marcia, "Asilomar Revisted: Lessons for Today?" *Science* 287 (2000).

SEE ALSO

Biocontainment Laboratories
Biodetectors
Biological Weapons, Genetic Identification
DNA Fingerprinting
DNA Recognition Instruments
DNA Sequences, Unique

Assassination

■ JUDSON KNIGHT

Assassination is a sudden, usually unexpected act of murder committed for impersonal reasons, typically with a political or military leader as its target. Although assassination gained its name from that of a fanatical Near Eastern sect in the Middle Ages, the practice of assassination goes back to ancient times, and extends to the present day. At one time, the most widely used tool for assassination was a knife or dagger, whereas modern assassinations more often use guns or bombs, while poisons have long been a means of political killing.

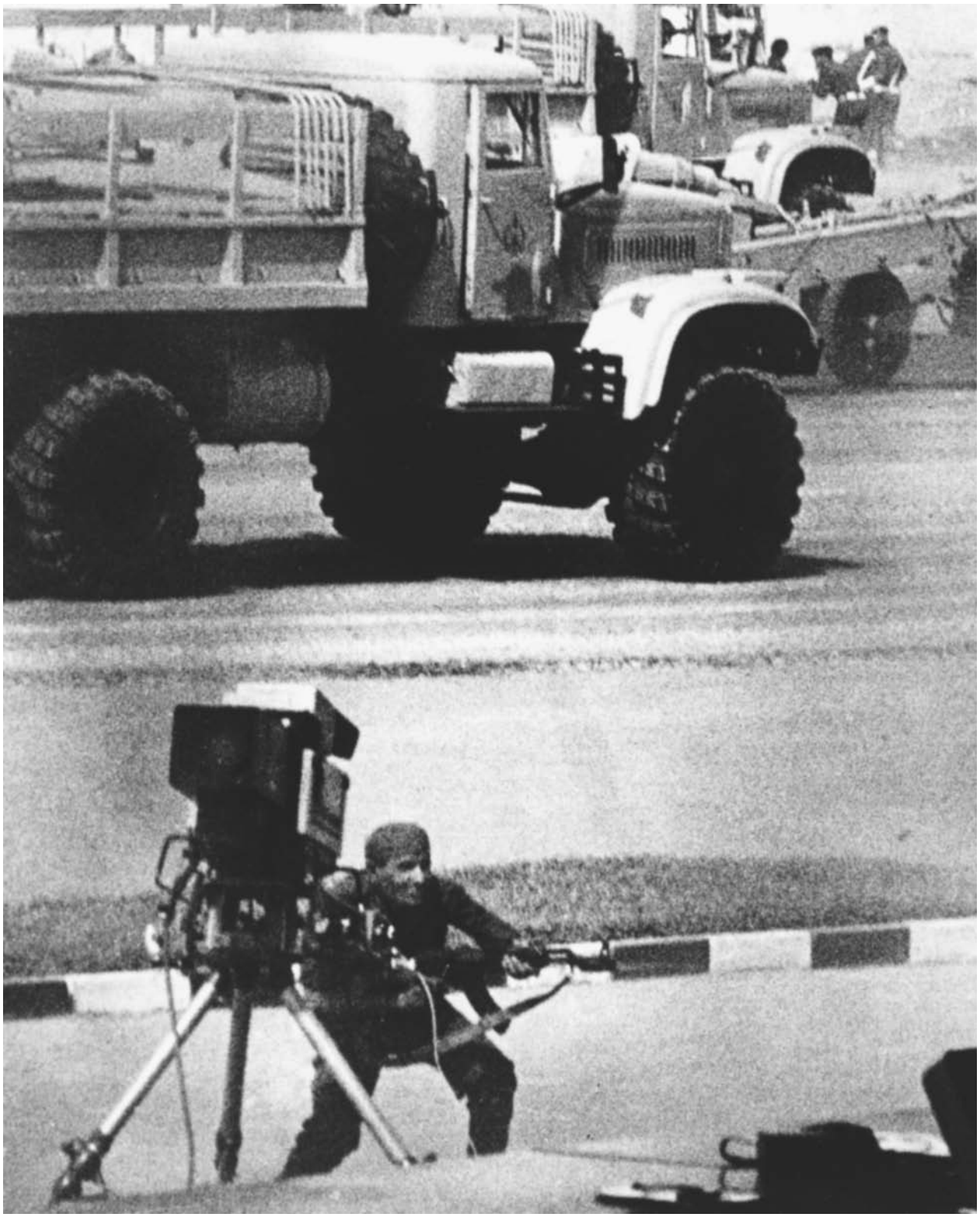
Assassination in History

The first significant assassination victim was probably the Egyptian pharaoh Amenemhet I, who established the Twelfth Egyptian Dynasty in 1986 B.C. Amenemhet gained his power by an act of usurpation, thus perhaps setting an example for a group of courtiers who conspired in his killing. Six centuries later, Horemhab, a general who competed with the grand vizier Aya for the hand of Tutankhamen's widow (and hence for the political legitimacy to be gained by marrying a queen), was likewise a victim of assassination—in this case, by his rival.

The list of assassination victims in ancient times is far too long to recount in detail. Roman history alone is studded with acts of murder. Long before and after the most famous assassination in Rome's history—that of Julius Caesar in 44 B.C.—the dagger proved a far more common instrument of political change than the ballot. The assassination of Domitian in A.D. 96, and that of Commodus in 192, serve as virtual bookends to the golden age of the empire, after which the western portion fell into a slow, but steady decline. During the half-century that began in 235, no fewer than 20 men held and lost the seat of Roman power, more often than not at the hands of assassins.

Assassination plots, or rumors of them, have sometimes had the effect of neutralizing a ruler indirectly. Some of the greatest and most despicable men of ancient times—Hannibal on the one hand, and Nero on the other—killed themselves rather than let assassins do the job. And Chandragupta, founder of the Mauryan empire of India in the third century, feared assassination so much that in 301 he left his throne, joined the Jain sect, and later died of starvation.

On the other hand, rulers secure in their power usually dealt severely with would-be assassins. Such is the case with the ruthless Prince Cheng of China's Ch'in state during the third century B.C. Many people wanted the tyrant Cheng dead, and the crown prince of the rival Yan kingdom set in motion assassination plans. It was a mark of the terror Cheng commanded that the king of Yan killed his own crown prince in the hope that it would please the Ch'in ruler. Although history does not record Cheng's response to this favor, the event marks one of those junctures in which assassination could or would have altered history: Cheng went on to unite China, which today



A gunman wearing an Egyptian uniform fires an automatic Kalashnikov submachine gun into a military parade reviewing stand during an attack that took the life of Egyptian President Anwar Sadat and five others at a Cairo suburb in 1981. AP/WIDE WORLD PHOTOS.

U.S. Special Forces assigned to guard Afghan President Hamid Karzai look for targets after an assassination attempt on Karzai as he was leaving the former governor's mansion in September, 2002. AP/WIDE WORLD PHOTOS.

still bears the name of his dynasty, commenced the building of the Great Wall, and established an empire that would continue for more than two thousand years.

The cult of the Assassins. Assassinations continued throughout the Middle Ages in western Europe and the Byzantine empire, as well as in the Muslim caliphates. It was in the Islamic world, in fact, that the first true assassins appeared on the stage. The Crusades created the political framework in which the cult of the Assassins, led by the Iranian Ismaili Hassan-i-Sabah, gained their infamous reputation, but Hassan founded the sect in 1090, a decade before the first crusaders arrived in the Holy Land, and throughout their existence, the Assassins were more apt to target Seljuk Turkish leaders than Christian invaders.

Two centuries later, Marco Polo, known for his tendency to weave fantastic tales, created a legend still believed by many today. According to Marco, Assassin leaders would ensure their men's loyalty by drugging them and taking them to a garden where they could enjoy all manner of earthly delights—pleasures which, they were told, would await them in the afterlife if they died on the field of battle. Contemporary Ismaili sources, however, contain no mention of the "Garden of Paradise." On the other hand, it is true that the word *assassin* comes from *hashshash,* or "one who chews hashish"—a reference to the Assassins' use of the drug.

Hassan was known as the "Old Man of the Mountain," a title that passed to each successive Assassin leader. Operating from a castle in a valley stronghold, the Assassins conducted acts of terrorism and political killing throughout the Muslim world, but particularly in Iran and Iraq. Because the Seljuks happened to be in power at that time, they were the primary target, and all attempts to uproot the Assassins proved fruitless. During the Crusades, Assassins in Syria terrorized both Turks and Christians, but combined attacks by the Mongols and Mamluks in the mid-1200s brought about the end of the sect.

Assassination in modern times. If the roster of ancient and medieval leaders killed by assassins was too lengthy to recount in any detail, such is true many times over where the modern world is concerned. Abraham Lincoln in 1865 became the first American president killed by an assassin's bullet, followed by three others: James A. Garfield in 1881, William McKinley in 1901, and John F. Kennedy in 1963. Franklin D. Roosevelt, Harry S Truman, Gerald Ford,

and Ronald Reagan were all targets of unsuccessful assassination attempts.

The roster of political murders in the twentieth century is lengthy. The assassination of Austrian Archduke Francis Ferdinand in 1914 precipitated World War I, and the attempted assassination of Adolf Hitler by his generals 30 years later very nearly ended World War II. Not only Mohandas K. Gandhi in 1948, but Indian Prime Minister Indira Gandhi (no relation) in 1984, and her son and successor, Rajiv Gandhi in 1991, fell victim to assassins' bullets. Leaders on both sides in the Middle East have been killed by assassins: King Abdullah of Jordan in 1951, President Anwar Sadat of Eygpt in 1981, and Israeli Prime Minister Yitzhak Rabin in 1995. Interestingly, each of these leaders was killed by extremists on their own political side. On the other hand, extremist leaders are as likely as any to become targets of assassins. Senator Huey Long of Louisiana in the 1930s, and Malcolm X 30 years later, both fell to assassins' bullets. So too did George Lincoln Rockwell, leader of the American Nazi Party, and Pim Fortuyn, founder of a radical anti-immigrant party that stunned the Dutch electorate by finishing second in the 2002 parliamentary elections.

Targets of assassination are not necessarily national leaders, formal office-holders, or even political leaders. When a Turkish assassin attempted to shoot Pope John Paul II in 1981, it was clearly a political act even though the pope is not a political leader per se. Martin Luther King and Robert Kennedy, both assassinated in 1968, were political leaders, but King held no formal office and Kennedy, although he was a senator and presidential candidate, symbolized a larger cultural atmosphere of optimism and activism. Furthermore, his status as John F. Kennedy's brother added greatly to the symbolic impact of the event.

Assassination by Stealth

Many of the assassinations mentioned in the preceding paragraphs were public acts, committed in crowded areas where the loud crack of a fired gun served as a signal of a murder in progress. Assassination committed by modern security organizations and other government-controlled response teams, however, is of a quite different nature. Indeed, assassination, whether undertaken by governments, nongovernmental organizations, or individuals acting alone, is most effective when performed in stealth.

Such was the case with an act of political murder that occurred at the outset of the modern era, during the French Revolution. As depicted in a famous painting by Jacques-Louis David, the radical leader Jean-Paul Marat was in one of the most vulnerable places—his bath—when young Charlotte Corday, a supporter of the opposition Girondists, caught up with him on the night of July 13, 1793. Corday entered Marat's private chambers under the pretense of being a journalist there to conduct an interview. More than two centuries later, the Muslim terrorist organization al-Qaeda used exactly the same pretext to gain an audience with Ahmad Shah Massoud. The leader of the rebels in the Northern Alliance, and widely regarded as the most popular opposition figure in Afghanistan, Massoud posed the principal threat to the ruling Taliban, who provided asylum to al-Qaeda and its leader, Osama bin Laden. Two Arab al-Qaeda operatives, posing as journalists with a camera, met with Massoud in private on September 9, 2001—just two days before al-Qaeda launched its infamous terrorist attacks on the United States. As the interview began, their "camera" exploded, killing both Massoud and the two assassins.

SMERSH and Trotsky. An excellent example of stealth assassination undertaken by operatives working for a modern government was the assassination of Leon Trotsky in Mexico City in 1940. Trotsky had long been a rival of Josef Stalin, who recognized that Trotsky's role in launching the Bolshevik takoever of Russia alongside V. I. Lenin gave him much greater revolutionary legitimacy. Stalin had Trotsky exiled, but still wanted him dead. For more than a decade, agents of SMERSH (*SMERrt SHpionam* or "Death to Spies"), the KGB assassination team, tracked him.

The individual who finally gained Trotsky's confidence was Ramón Mercader, whom Trotsky granted a private interview. Unbeknownst to Trotsky, however, Mercader had been recruited by SMERSH in Spain during its civil war. Using the cover identity of Jacques Mornard, a French journalist, Mercader had gradually worked his way into Trotsky's inner circle, in part by seducing an American named Sylvia Agelof, who had close connections to the radical leader.

Mercader worked patiently, meeting Trotsky on several occasions before mentioning that he had written a paper on Trotsky's political philosophies, and wished to have the master himself read it. Undoubtedly flattered, Trotsky agreed to meet with him on August 20, 1940. On the appointed day, Mercader arrived bearing the putative manuscript—which was actually gibberish—along with the concealed tool necessary for his mission: a 13-inch dagger, a pistol, and an Alpine mountain climber's ice ax. After Trotsky began to read the manuscript and realized that it was only a prop, he looked up at his guest, whereupon Mercader split his skull with the ice ax. Trotsky did not immediately die, and prevented his bodyguards from killing Mercador because "He has a tale to tell." Within 24 hours, Trotsky was dead in a hospital room, and Jacques Mercador was in the custody of police. Mercador maintained his false identity as Mornard throughout his trial, where he claimed that he had killed because he was jealous that Sylvia had an intimate relationship with Trotsky. Sentenced in 1943, Mercador served 17 years in a Mexican prison. After his release, he went first to Prague and then to Moscow, where the Kremlin awarded him the Order of the Soviet Union.

Wrath of God and "Black September." Another instructive example of a government undertaking a careful and calculated plan of assassination is that of Israel in response to

the murder of 11 Israeli athletes at the 1972 Summer Olympic Games in Munich. The killing had occurred at the hands of Black September, a terrorist group established by the Palestine Liberation Organization (PLO) as a "deniable" action team—in other words, a group that could not be conclusively tied to its sponsors. In seeking to mete out justice to Black September, Israel in turn set up its own deniable counterterrorist unit, known as the Wrath of God.

Between 1972 and 1974, Wrath of God (nicknamed "Israel's long arm") allegedly killed more than a dozen Black September operatives. Wael Zwaiter, for instance, had the misfortune to find himself in a Rome elevator with what turned out to be two Wrath of God agents carrying .22 caliber pistols. The group killed Mahmoud Hamshari with an explosive device on a telephone in Paris, and claimed Hussein Bashir in Nicosia, Cyprus, with a bomb under his mattress. An explosion also claimed Mohammed Boudia, who, after a night with his girlfriend in her Paris flat, started his automobile, only to discover too late that it had been rigged with a car bomb.

As efficient as the Wrath of God was, it made some mistakes. In Lillehammer, Norway, in 1974, Wrath of God operatives shot a man they believed to be Ali Hassan Salameh, operations chief of Black September. In truth, he was Ahmed Bouchiki, a Moroccan waiter carrying an Algerian passport. Five years later in Beirut, the Wrath of God finally eliminated Salameh with an explosive device. In the meantime, the Lillehammer incident provoked complaints from western European nations vexed at the Israelis for using their cities as hunting grounds, and Israel agreed to shut down the Wrath of God.

CIA. It is a truism of historically alleged assassinations carried out by the Central Intelligence Agency (CIA), and other such organizations in the United States that the only operations of which the citizenry ever learns would be the botched ones. Such is the situation of an agency dedicated to covert action under the aegis of a government with a degree of openness before its polity—a problem with which SMERSH, for instance, did not have to contend.

The CIA has been publicly embarrassed by revelations of attempts to kill Fidel Castro by a number of fanciful means, such as poisoning his cigar. There have also been allegations that the agency either undertook or supported the assassinations and attempted assassinations of numerous world leaders from Chou En-Lai of China in the 1950s to Saddam Hussein in the 1990s.

These and other revelations, many of which emerged during the 1975–76 hearings led by Senator Frank Church (D-ID), helped bolster an atmosphere of public suspicion toward the CIA and NSA. From the 1970s onward, popular conspiracy theories emerged among the public that linked the CIA to almost every political slaying around the world, including the assassination of President Kennedy. Conspiracy theories aside, some trained CIA operatives possess extraordinary skill in assassination techniques. Some of those techniques are discussed in a CIA assassination manual, apparently written in the 1950s and released to the public in 1997.

■ FURTHER READING:

BOOKS:

Lentz, Harris M. *Assassins and Executions: An Encyclopedia of Political Violence, 1865–1986.* Jefferson, NC: McFarland, 1988.

McKinley, James. *Assassination in America.* New York: Harper & Row, 1977.

Sifakis, Carl. *Encyclopedia of Assassinations.* New York: Facts on File, 1991.

Spignesi, Stephen J. *In the Crosshairs: Famous Assassinations and Attempts.* New York: New Page Books, 2003.

ELECTRONIC:

Doyle, Kate, and Peter Kornbluh. *CIA and Assassinations: The Guatemala 1954 Documents*. George Washington University. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB4/> (January 30, 2003).

SEE ALSO

Assassination Weapons, Mechanical
Biochemical Assassination Weapons
CIA (United States Central Intelligence Agency)
Mossad
Soviet Union (USSR), Intelligence and Security

Assassination Weapons, Mechanical

Throughout history, governments and groups have employed the tactic of assassination: a sudden, usually unexpected act of murder committed for impersonal reasons. The reasons for resorting to assassination have become perhaps a bit more complex as the balances of power have become more intricate, but not especially so. The purpose of assassination remains essentially the same as it was 4,000 years ago: to bring about political change quickly, or to remove someone considered a threat. The methods of assassination themselves, however, have changed greatly.

Mechanical weapons contrasted with biochemical techniques. In discussing assassination techniques, it is useful to divide these into mechanical and biochemical means. As their names imply, the first type of weapon gains its potency from its physical properties, whereas the second kills primarily through its effect on the individual's biochemistry. Into the first category would fall the basic types

The .22 caliber revolver used by John Hinkley, Jr. in his 1981 assassination attempt against U.S. President Ronald Reagan, displayed at Hinkley's trial in 1982. AP/WIDE WORLD PHOTOS.

of weapon to be discussed here: bludgeons, knives, guns, and other firing devices.

To varying degrees, all of these use the mechanical principles of force, pressure, and momentum, which are related through various ratios involving the fundamental physical interactions of mass, length, and time. Additionally, several are variations on the three classic "simple machines" of classical mechanics: the inclined plane (knife), the lever (the firing mechanism of a pistol), and the hydraulic press (some types of firing devices other than pistols).

Areas of overlap. There is often considerable overlap between mechanical and biochemical assassination weapons. At the simplest level, all ultimately kill by impacting some aspect of the victim's biochemistry, if only by causing his brain or heart to shut down, thus bringing an end to the functions of the body itself. Furthermore, firearms employ chemical properties. The gunpowder in a bullet undergoes a chemical, rather than a merely physical change. A physical change, such as the freezing of water, is reversible, but once gunpowder has chemically been altered by the addition of heat and the process of combustion brought about by interaction with oxygen, it turns into fire, smoke, and ash—and a fraction of it becomes energy—such that it can never become gunpowder again.

Another area of overlap is the use of firing devices to deploy the materials of biochemical assassination—that is, poisons. A classic example is the poison pen, most effectively employed by the Soviet KGB. Disguised as an ordinary writing pen, the device fired hydrocyanic acid in the form of gas. Another KGB pen-cum-assassination weapon fired pellets of ricin, a poison long favored by agents in the assassination squad known as SMERSH.

SMERSH, poison pistols, and ricin. SMERSH used variations on this technique to eliminate several Bulgarian dissidents living abroad in the 1970s. The most famous example of this occurred in London, where SMERSH caught up with journalist Georgi Markov in September 1978. As an unsuspecting Markov stood waiting in a crowd for a bus at Waterloo Bridge, a man walked past him and accidentally—or so it seemed—jabbed him in the thigh with the pointed end of his umbrella. The man apologized and walked on past. Within a few hours, Markov was dead. The man with the umbrella was a SMERSH assassin, and the pointed tip of his umbrella had fired a platinum pellet containing ricin.

So clever was this method of murder that it took some time before Western intelligence operatives realized what had happened, and arranged for Markov's body to be exhumed. Only then did they discover the pellet.

In this and other such cases, a biochemical agent actually caused death, yet the method of delivery was mechanical. In the same way, poison that passes through a syringe (a hydraulic pump) into the victim's body is a biochemical weapon delivered by mechanical means. By contrast, when the Aum Shinrikyo cult employed ricin to kill 12 commuters, and injure thousands more, in a Tokyo subway in 1995, they used it in the form of gas—an almost purely biochemical technique. Victims inhaled the gas, which went to work immediately on their systems.

Basic types of mechanical assassination weapon. The weapons under discussion here fall into a few broad categories: bludgeons; knives and other sharp objects; guns and other firing devices; and miscellaneous weapons. An encyclopedic treatment of such weapons would fill an entire book, especially where guns are concerned. Therefore, the focus here is confined to weapons, noted for their clever design or means of concealment that were developed by and for covert action organizations or similar groups. Even then, it is possible only to touch on a few notable examples.

Few of these weapons are known to be associated with a particular assassination, in part because most assassinations committed by covert-action organizations probably go undetected. Furthermore, the vast majority of assassinations are probably not directed against figures well known to the public at large, and therefore are likely to escape public attention. When Markov died, for instance, the people most likely to note the event were primarily in Bulgaria, where state-fed disinformation effectively covered all incriminating details regarding the cause of death.

Bludgeons and blunt instruments. A number of the potential assassination weapons that fall under the general heading of bludgeon are or were weapons for close combat also used in situations other than assassination missions. An example is the club-like instrument known as the cosh or blackjack, employed by the U.S. Central Intelligence Agency (CIA), the East German Stasi, and others. Though intended to stun the victim with a blow to the head, a cosh could certainly cause fatal injury if wielded with enough force. In a situation where a metal detector or other device would have revealed the presence of a gun, and where the operative was likely to be at close quarters with his victim, a cosh might well have been the weapon of choice.

In the 1950s, the CIA provided agents with an assassination manual that, due to the Freedom of Information Act, is now available to the public. In discussing blunt weapons, the author shows obvious respect for these simple tools of the trade, although he notes they "require some anatomical knowledge for effective use," The main advantage of a common blunt instrument such as a hammer is its universal availability.

Knives, edge weapons, and pointed instruments. The CIA author was equally explicit in discussing ways to use edge weapons, a term encompassing not only knives, but also other sharp weapons. British special forces in World War II, for example, used the push dagger and the thrust weapon, both sharp instruments that are more like stakes or spikes than knives per se. Other British forces, serving as commandos in North Africa, employed a combination of knife and brass knuckles, by which the user could first stun the victim, then put the knife itself to work.

As with most assassination weapons, concealment is a key issue. Hence, many units responsible for special operations in World War II used thumb knives, which were so small they could only be gripped with the thumb and forefinger. Their size made them easy to hide in the user's clothing, or even in a closed hand. Also during the war, the British Special Operations Executive (SOE) designed an ingenious knife kit for the U.S. Office of Strategic Services (OSS), forerunner of the CIA. The kit, made to fold up and fit neatly in a pocket, contained a plethora of knives and sharp instruments, ranging from a tiny knife painted black (so as to be nonreflective) to a fierce-looking open-handled dagger. OSS never officially adopted the kit, but many of its agents took a liking to it, and acquired their own while undergoing training in Britain.

Miscellaneous and hybrid devices. There are also miscellaneous assassination devices that either combine aspects of the bludgeon and edge weapon, or use strangulation as a means of killing. A notorious example of the latter is the garrote, typically used when the killer is able to approach the victim unsuspected from the back. Consisting of two handles joined by a thin, strong wire a little longer than a man's shoulders, the garrote is a highly effective low-tech weapon. Some are even designed with blade-like edges to the wire so that they can double as saws if the user needs to escape from a jail cell.

Similar to the garrote is the device known as the Gigli saw. Named for Leonardo Gigli, a nineteenth-century Italian physician who used it in performing surgery, the Gigli consists of long thin tempered steel blades arranged in an oval shape, with finger rings at either end. Made to cut through bone, it could certainly be used as a killing instrument, though mercifully it is more well known as an escape device employed by British intelligence operatives.

An all-purpose device, combining aspects of both the bludgeon and the sharp instrument, was the Peskett close-combat weapon. Used in Allied special operations during World War II, the Peskett was a veritable warehouse of low-tech killing equipment. Its wrist strap and attaching

ring were the only innocuous aspects of the Peskett, whose ring attached it to a combination of cosh, garrote, and dagger. The cosh was a heavy weighted ball at the far end. The garrote wire, which could be pulled from (and retracted to) a hole on the side, also had a smaller weighted ball, which the killer employed as a grip when garroting a victim. Close to the ring and strap was a button by which the user released a dagger.

Guns and other firing devices: clever concealment. The designs of various guns, firing mechanisms, and explosive devices are often so clever that many of them sound more like something from a James Bond movie than actual weapons used by CIA, KGB, and other real covert-operations organizations. In such an environment, something as exotic as the CIA "Dear Weapon," a 9-mm pistol used by the organization in Vietnam, seems perfectly ordinary. Also known as the "CIA zip gun," it was made to be dropped in a styrofoam box from a plane. The pistol could be assembled in a matter of seconds with the help of an extremely simple instruction sheet, printed on moisture-resistant paper using pictograms that required no knowledge of English. The weapon stored ammunition in its grip, and looked like a water pistol—but it fired real bullets.

The Stinger (not to be confused with the surface-to-air missile of the same nickname) was a .22-caliber pistol hidden in a toothpaste tube. Developed for CIA during the Cold War, it was one of several guns designed for concealment in innocuous-looking packages. The British SOE also designed .22 caliber pistols disguised as either cigarettes or cigars. Both had a string at the end the smoker would put in his mouth, at which point the agent pulled the string with his teeth, firing the pistol.

Although the Bulgarians used KGB help in Markov's case, they were also adept at designing assassination devices of their own. Bulgarian intelligence designed the keychain gun, which had two barrels and carried two .32 caliber bullets. The small size—about an inch wide and three inches long—was both an advantage and a disadvantage. On the negative side, the shortness of the barrel created a great deal of recoil, and the size of the weapon left little room for any muffling device that would reduce the loudness of the sound when fired. For this reason, the keychain gun was typically used only as a last resort. On the other hand, its size made it easy to conceal, and it was designed in such a way that the keychain gun could pass through airport metal detectors. Indeed, the keychain gun cannot be spoken of in the past tense: according to Interpol, Cold War versions or post-Cold War knockoffs continue to sell in eastern Europe for as little as $20. After the September 11, 2001, terrorist attacks, United States aviation authorities warned airport screeners to look for keychain pistols.

Guns have also been concealed as flashlights, pipes, pencils, and any number of other ordinary-looking devices. A celebrated example was the lipstick pistol, or "kiss of death." Created by KGB for its female agents (or for male agents operating as homosexuals, or "ravens"), this weapon contained a 4.5-mm single-shot pistol encased in rubber and disguised as a tube of lipstick. To fire it, the user twisted its knurled ring a quarter-turn.

Devices for firing poison gas. Innocent-looking everyday objects provide an effective cover for assassination equipment of all types—not just pistols, but devices for firing poison gas as well. The KGB, which developed (or arranged for the development of) the poison pens described earlier, was especially talented in this area. At different times, KGB agents used wallets concealing gas-firing cartridges, as well as variations on the umbrella that killed Markov. One tool was made to look like a blind person's cane. White tape concealed a triggering mechanism, but when the tape was removed, the user—who of course was a KGB operative with perfect vision—could fire poison gas from the cane's handle.

The KGB used a cigarette case to hide a poison-pellet gun. Once the pack was opened, it would fire hollow-point weapons containing poison gas. Another such weapon concealed a gas-firing device that had to be removed before using. In 1954, KGB sent Nikolai Khokhlov to assassinate dissident Georgi Okolovich in West Germany using a cigarette-pack poison weapon. Khokhlov, however, had secretly converted to Christianity, and renounced his profession. Therefore he warned Okolovich about the plot and defected to the West, subsequently revealing information about the cigarette-case weapons.

FURTHER READING:

BOOKS:

Irvin, Victor D. *Political Assassination: The Strategic Precision Weapon of Choice.* Carlisle Barracks, PA: U.S. Army War College, 2002.

Melton, H. Keith. *The Ultimate Spy Book.* New York: DK Publishing, 1996.

Minnery, John. *CIA Catalog of Clandestine Weapons, Tools, and Gadgets.* Boulder, CO: Paladin Press, 1990.

ELECTRONIC:

Doyle, Kate, and Peter Kornbluh. *CIA and Assassinations: The Guatemala 1954 Documents.* George Washington University. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB4/> (January 30, 2003).

International Spy Museum. <http://www.spymuseum.org> (January 31, 2003).

SEE ALSO

Assassination
Biochemical Assassination Weapons
Knives

Asymmetric Warfare

K. LEE LERNER

In contrast to traditional warfare or "linear warfare," asymmetric warfare refers to operations that do not rely on masses of troops or munitions to destroy and/or control an enemy. Asymmetric warfare most commonly refers to warfare between opponents not evenly matched where the smaller or weaker force must exploit geography, timing, surprise, or specific vulnerabilities of the larger and stronger enemy force to achieve victory.

At the tactical level, asymmetric warfare doctrine—first formally proposed by the ancient military strategist Sun Tzu—oftens attempts to specifically avoid a confrontation with the enemy's strengths, preferring instead to disrupt or impair command functions (intelligence gathering and communications) or logistics (supply and medical care) so as to prevent the larger enemy from effectively bringing their larger force to bear in an effective manner.

At a strategic level, asymmetric war is designed to discourage and demoralize enemy forces and political leaders of those forces from using their greater strength.

The high effectiveness and low cost of asymmetric warfare has led to the inclusion of smaller and more agile units within large power forces that can specifically disengage from the larger force so as to allow larger force commanders to use asymmetric techniques.

Terrorist organizations have embraced many of the concepts of asymmetric warfare—particularly when planning operations against Western power forces. After the American-led invasion of Afghanistan following the September 11, 2001 terrorist attacks on the United States, enemy Taliban forces utilized local tribal forces to attack civilian populations and destroy food supply infrastructure in an attempt to create a humanitarian aid crisis that would slow Western coalition forces.

Because of the superpower status of United States, enemy small state and terrorist groups must utilize asymmetric warfare techniques to bolster hopes of achieving limited victories. For example, terrorist organizations hope to exploit the vulnerabilities of a free and open society in the United States and Europe. By attacking infrastructure and civilian populations, terrorist groups hope to cause political turmoil, dissent, and ultimately to change United States and European foreign policy without exposing themselves to the might of Western military forces.

FURTHER READING:

BOOKS:

Bailey, Kathleen C. *Iraq's Asymmetric Threat to the United States and U.S. Allies.* Fairfax, VA: National Institute for Public Policy, 2001.

Rogers, Paul. *Political Violence and Asymmetric Warfare.* (U.S.-European Forum Paper) Washington, D.C.: Brookings Institution, 2001.

SEE ALSO

Biological Warfare
Chemical Warfare
Electronic Warfare
Guerilla Warfare
Information Warfare
Terrorism, Philosophical and Ideological Origins

ATF (United States Bureau of Alcohol, Tobacco, and Firearms)

JUDSON KNIGHT

In accordance with the Homeland Security Act of 2002, on January 24, 2003, the Bureau of Alcohol, Tobacco, and Firearms (ATF or BATF) was transferred from the Department of the Treasury to the Department of Justice. There it became the Bureau of Alcohol, Tobacco, Firearms, and Explosives, but retained the initials ATF.

ATF is responsible for enforcing federal law with regard to the sale and use of alcohol, tobacco, firearms, and explosives. Although the ATF itself was created in 1972, at that time making it the youngest tax-collecting office of the Treasury Department, its roots go back to the founding days of the Republic. The order of items in its name corresponds to the order in which Treasury began to assume control over the items themselves: alcohol in the post-Revolutionary War era, tobacco around the time of the Civil War, and firearms during the Great Depression.

Alexander Hamilton, the first secretary of the Treasury, suggested that Congress impose a tax on imported spirits to pay a portion of the debt incurred in the War of Independence. Congress passed a resolution calling for such a tax, and in 1789 gave Treasury responsibility for collecting it. An act passed in 1862 created the Office of Internal Revenue, whose responsibilities included the collection of taxes on spirits and tobacco products. Renamed the Bureau of Internal Revenue (BIR) in 1877, in 1886 it established a laboratory that in time would assume responsibility for analyzing a variety of alcohol and tobacco products, as well as firearms and explosives.

Following the passage of the Eighteenth Amendment, which banned the sale, distribution, and consumption of alcohol, Treasury in 1920 established the Prohibition Unit. The deeds of "revenuers" and "T-men" such as Eliot Ness in the years that followed would become legendary, as would the less admirable exploits of gangsters such as Al Capone. Nationwide concern over the violence

An Alcohol, Tobacco, and Firearms (ATF) agent searches for clues at a Manassas, Virginia, gas station in 2002 as part of the search for a sniper that terrorized the Washington, D.C. area. AP/WIDE WORLD PHOTOS.

associated with organized crime led to the passage of the National Firearms Act in 1934. Four years later, Congress passed the Federal Firearms Act, and BIR became responsible for collecting taxes on firearms.

After a number of changes in the section of BIR concerned with alcohol taxes, in 1940, this division became the ATU, or Alcohol Tax Unit. In 1942, Congress gave ATU responsibility for enforcing the Firearms Act.

ATF separates from the Revenue Office. Throughout much of the twentieth century, BIR had included a Miscellaneous Tax Unit (MTU), which had responsibility for tobacco taxes and, between 1934 and 1942, taxes on firearms. In 1952, MTU was dismantled, and its firearms and tobacco tax functions fell under ATU. At the same time, BIR received a new name, one familiar to millions of Americans today: Internal Revenue Service (IRS). ATU then came under IRS control as the Alcohol and Tobacco Tax Division, an arrangement that lasted for two decades.

In 1968, when Congress passed the Gun Control Act, the old BIR/IRS laboratory became responsible for analyzing firearms and explosives, and the Alcohol and Tobacco Tax Division became the Alcohol, Tobacco, and Firearms (ATF) Division. The 1970 passage of the Organized Crime Control Act made the role of the ATF Division more explicit, and signaled a shift away from IRS purview. On June 1, 1972, the Treasury Department issued Order No. 120–1, which separated the ATF from the IRS.

The order gave the new bureau authority not only over the three items listed in its name, but also over explosives. During the 1970s, ATF and its laboratory became involved in arson investigations, and in 1982, Congress amended Title XI of the Organized Crime Control Act to make arson a federal crime and formalize the ATF's role in investigating it.

During the 1990s and the beginning of the twenty-first century, ATF undertook a number of new efforts toward fighting and investigating crime. Among these was the Integrated Ballistic Identification System, a computerized program for matching weapons and ammunition fired from them. In the mid-1990s, after its abortive 1993 raid on a Waco, Texas, compound controlled by the Branch Davidian cult, the bureau became the focus of hostility on the part of fringe right-wing groups. By the turn of the century, ATF annually collected more than $13 billion in revenue for the federal government.

FURTHER READING:

BOOKS:

Moore, Jim. *Very Special Agents: The Inside Story of America's Most Controversial Law Enforcement Agency—The Bureau of Alcohol, Tobacco, and Firearms.* Urbana: University of Illinois, 2001.

A Report on the Bureau of Alcohol, Tobacco, and Firearms: Its History, Progress, and Programs. Washington, D.C.: U.S. Government,1995.

Vizzard, William J. *In the Cross Fire: A Political History of the Bureau of Alcohol, Tobacco, and Firearms.* Boulder, CO: Lynne Rienner, 1997.

ELECTRONIC:

Bureau of Alcohol, Tobacco, and Firearms. <http://www.atf.treas.gov> (December 30, 2002).

SEE ALSO

Treasury Department, United States

Atmospheric Release Advisory Capability (ARAC)

The Atmospheric Release Advisory Capability (ARAC) is an effort through which the United States Department of Energy (DOE) monitors and predicts the release of hazardous materials into the atmosphere. The bulk of its activities takes place at the National Atmospheric Release Advisory Center (NARAC), located at the University of California's Lawrence Livermore National Laboratory. ARAC and NARAC have provided assessment on more than 100 incidents of hazardous-material release, whether accidental or intentional, involving nuclear, chemical, biological, and natural materials.

In 1973, Rudy J. Engelmann of the DOE consulted scientists at Livermore to learn if it were possible to create an integrated system for providing data on potential and ongoing atmospheric hazards. The laboratory undertook a feasibility study, and the result was the creation of ARAC a year later. ARAC and its national center, NARAC, got their first major test on March 28, 1979, after a malfunction in the nuclear power plant at Three Mile Island near Harrisburg, Pennsylvania, threatened to release radioactive materials into the atmosphere. NARAC analysis helped provide DOE with an accurate picture of radioactivity in and around the plant, and helped prevent an environmental disaster.

Seven years later, a far worse nuclear incident occurred in what is now Ukraine, then a part of the Soviet Union. On April 26, 1986, an accident at the Chernobyl nuclear reactor killed 31 workers immediately, and ultimately led to the deaths of some 10,000 people. With the Soviet government withholding information, even from its own citizens in the threatened area, the U.S. government turned to ARAC. Over the weeks that followed, the team at NARAC assisted western European U.S. allies in assessing the threat, and accurately predicted the subsequent spread of radioactive material across the northern hemisphere.

Accidental nuclear hazards are only one type of event among many for which ARAC has provided data. Other examples include the oil fires set by a retreating Iraqi army

during the final days of the Persian Gulf War in February 1991; the volcanic eruption of Mount Pinatubo in the Philippines in June of that year; a sulfuric-acid spill in Richmond, California, in 1993; the reentry of a nuclear-powered Russian spacecraft over Chile in 1996; and the Hanford wildfire in Richland, Washington, in 2000.

Though ARAC and NARAC might seem to be virtually identical, the former is an agency of DOE, while the latter supports both DOE, the Department of Defense, and other governmental organizations. Nor are its DOE responsibilities confined to the consequence-management mission of ARAC, though this is certainly a primary activity for NARAC. NARAC also supports other federal, state, and even local agencies in accordance with the Federal Radiological Emergency Response Plan and the Federal Response Plan.

FURTHER READING:

BOOKS:

Cassaro, Edward, and Linda Lomonaco. *Operators Guide: Atmospheric Release Advisory Capability (ARAC) Site Facility.* Springfield, VA: Department of Energy, 1979.

Orphan, R. C. *A Study of Applying the Atmospheric Release Advisory Capability to Nuclear Power Plants.* Springfield, VA: Department of Energy, 1978.

ELECTRONIC:

National Atmospheric Release Advisory Center. <http://narac.llnl.gov/> (January 14, 2003).

SEE ALSO

Chernobyl Nuclear Power Plant Accident, Detection and Monitoring
DOE (United States Department of Energy)
Lawrence Livermore National Laboratory (LLNL)
Nuclear Detection Devices

Atmospheric Sampling Programs.

SEE *Environmental Measurements Laboratory.*

Atomic Bomb.

SEE *Nuclear Weapons.*

Audio Amplifiers

LARRY GILMAN

Any electronic device that increases the power of an electrical signal whose vibrations are confined to the audio frequency range—the range that can be perceived by the human ear—is an audio amplifier. All devices that transmit, record, or otherwise electronically process voice signals employ audio amplifiers. Voice-recognition or voice-synthesis systems, communications or eavesdropping devices, hearing aids, entertainment systems, talking toys, are examples of devices containing audio amplifiers.

The need for amplification. Acoustic or sound waves are longitudinal pressure waves (i.e., waves that cause molecules to oscillate along the wave's line of travel rather than across it) in air, water, or any other medium. A sound is said to be in the *audio* frequency range if it is not too high or low in frequency to be heard by the human ear. Audio sound waves may be converted by microphones into electrical signals for analysis, transmission, or recording. Electrical signals can also be converted by speakers into audible sound waves. Microphones and speakers are both transducers, that is, devices that convert energy from one form (e.g., electrical) into another (e.g., acoustic) or vice versa. Audio amplifiers are required with both microphones and speakers.

Input amplification. Amplification of the signal produced by a microphone—often termed preamplification—is necessary because the electrical signal that can be derived directly from sound waves impinging on a microphone is weak (i.e., on the order of .01 V or less; for eavesdropping applications, much less). Input signals of such low amplitude must be amplified before they can be processed in either analog or digital circuits.

In analog circuits—circuits that process smoothly-varying electrical quantities—there is a always a certain amount of random electrical activity or "noise." This noise is mixed with any information signal processed by the circuit, corrupting it. Amplifying a weak input, such as that from a microphone, before it mingles with circuit noise makes the noise problem manageable. Furthermore, all analog circuits that lack amplification (passive filters, transmission lines, etc.) experience signal loss; that is, they dissipate energy. A weak signal fed into a circuit that does not contain amplification will, therefore, quickly disappear, making amplification necessary in most analog circuits. Finally, amplification provides electronic isolation between the signal being amplified and the result of the amplification process; among other gains, this simplifies the circuit-design process.

If an audio signal is to be processed using digital circuitry (as is often the case today), a digital signal (i.e., on-off, high-low signal that can represent signal magnitudes symbolically) must be derived from the analog input. This conversion is performed by a device termed an analog-to-digital converter. For reasons ultimately deriving from the atomic properties of semiconductors, a typical analog-to-digital converter requires an analog input signal with an amplitude variation on the order of several

volts. A low voltage signal must therefore usually be amplified before being digitized.

Output amplification. Wherever human ears are the ultimate destination of a signal it is necessary to drive a physical sound-making device at the output. Here audio amplification is needed for a reason complementary to that which applies at the input: the signal power needed to drive an output device (e.g., speaker or headphones) is greater than that conveyed by the signals processed throughout the circuitry of a typical electronic device, whether analog or digital. An audio amplifier is thus found at the output as well as at the input of almost every system handling signals in the audio range.

Applications. The number of audio amplifier designs that have been produced over the last century is probably in the hundreds of thousands. Such devices are a ubiquitous feature of modern life, and are found in computers, telephones, radios, high-fidelity audio systems, all military voice-communication systems, many appliances, and even toys.

Audio amplifiers can be miniaturized for placement in headsets, mobile phones. In applications where small size is at a premium, as in hearing aides and espionage applications (bugs and "wires"), they may be ultraminiaturized. At the high-power end, audio amplification drives public-address systems, speaker systems, and (potentially) weapons. Research is being conducted by several countries, including Russia and the U.S. (through its Low Collateral Damage Munitions Program), into the use of highly amplified sound as a weapon; frequencies in the infrasonic, audio, and ultrasonic ranges are all being considered for use against human beings. Though acoustic weapons are sometimes assumed to always be in the nonlethal category, sound can be irritating, painful, or fatal, depending on its intensity and on the efficiency with which its energy is coupled to the body.

Loud music has repeatedly been used as a psychological weapon in siege situations (e.g., by the U.S. Army against former Panamanian dictator Manuel Noriega in 1989, by cult leader David Koresh against police in 1993, and by Peruvian police during the hostage crisis at the Japanese Embassy in 1997) and as an instrument of torture. Specially-designed acoustic weapons can induce, among other effects, vomiting, choking, spasms, incontinence, thermal burns, intolerable sensations in the chest, injury to internal organs, and hearing damage. The latter is considered a serious drawback in antipersonnel applications, as hearing loss caused by intense sound is often partly or wholly permanent. Like laser weapons designed to blind (which have been outlawed by recent international agreement), acoustic weapons designed to deafen would violate international humanitarian law. Further, they would be vulnerable to obvious countermeasures, such as earplugs. Indeed, some scientists are skeptical about the possibility of developing reliable, affordable weapons of any kind from sound. However, research and development are proceeding. Military and security applications of high-intensity sound currently under development in the U.S. or elsewhere include the following:

1. A device projecting "acoustic bullets," baseball-sized pulses of low-frequency (10-Hz) sound over distances of hundreds of yards, scalable in intensity from painful to lethal.
2. Multisensory grenades emitting disorienting light flashes, painfully loud sounds, and possibly disagreeable odors.
3. A ship-mounted system to disable crewmembers of nearby vessels (e.g., prior to boarding by Coast Guard personnel).
4. The "directed-stick radiator," an audio frequency, battery-powered weapon that could be clipped to a rifle. It fires acoustic bullets with a range in the tens of feet.
5. A helicopter-mounted nonlethal weapon emitting painfully loud sound in the audible range, with a reported (but unlikely) range of 1.2–6 miles (2–10 km).
6. Acoustic-beam weapons designed to cause discomfort: intended for embassy defense, denial of access to sensitive facilities, crowd control, and other miscellaneous antipersonnel uses.

It is unlikely that such devices will see widespread application or that, if they do, they will replace ordinary lethal weapons such as firearms. Due to the tendency of sound waves to diffuse with distance, the unpredictability of their effects on individual persons at sub-lethal levels, and the extremely high power requirements (megawatt range) for lethal levels, acoustic weapons are likely to remain a military curiosity. Audio amplification will thus remain ubiquitous in communications devices and rare in weaponry.

■ FURTHER READING:

BOOKS:

Jones, Dwight V., and Richard F. Shea. *Transistor Audio Amplifiers.* New York: John Wiley & Sons, 1968.

PERIODICALS:

Altmann, Jürgen. "Acoustic Weapons-A Prospective Assessment." *Science and Global Security* no. 9 (2001): 165–244.

ELECTRONIC:

Roxana, Tiron. "Acoustic-Energy Research Hits Sour Note." National Defense Magazine. August 21, 2001. <http://www.nationaldefensemagazine.org/article.cfm?Id=746> (December 13, 2002).

SEE ALSO

COMINT (Communications Intelligence)
Communications System, United States National

Aum Supreme Truth (Aum)

A cult (also know as Aum Shinrikyo and Aleph) established in 1987 by Shoko Asahara, the Aum aimed to take over Japan and then the world. Approved as a religious entity in 1989 under Japanese law, the group ran candidates in a Japanese parliamentary election in 1990. Over time, the cult began to emphasize the imminence of the end of the world, and stated that the United States would initiate Armageddon by starting World War III with Japan. The Japanese government revoked its recognition of the Aum as a religious organization in October 1995, but in 1997, a government panel decided not to invoke the Anti-Subversive Law against the group, which would have outlawed the cult. A 1999 law gave the Japanese government authorization to continue police surveillance of the group due to concerns that Aum might launch future terrorist attacks. Under the leadership of Fumihiro Joyu the Aum changed its name to Aleph in January, 2000, and claimed to have rejected the violent and apocalyptic teachings of its founder. (Joyu took formal control of the organization early in 2002 and remains its leader.)

Organization activities. On 20 March, 1995, Aum members simultaneously released the chemical nerve agent sarin on several Tokyo subway trains, killing 12 persons and injuring up to 6,000. The group was responsible for other mysterious chemical accidents in Japan in 1994. Its efforts to conduct attacks using biological agents have been unsuccessful. Japanese police arrested Asahara in May 1995, and he remained on trial facing charges in 13 crimes, including 7 counts of murder at the end of 2001. Legal analysts say it will take several more years to conclude the trial. Since 1997, the cult continued to recruit new members, engage in commercial enterprise, and acquire property, although it scaled back these activities significantly in 2001 in response to public outcry. The cult maintains an Internet home page. In July, 2001, Russian authorities arrested a group of Russian Aum followers who had planned to set off bombs near the Imperial Palace in Tokyo as part of an operation to free Asahara from jail and then smuggle him to Russia.

The Aum's current membership is estimated at 1,500 to 2,000. At the time of the Tokyo subway attack, the group claimed to have 9,000 members in Japan and up to 40,000 worldwide. The Aum's principal membership is located in Japan, but a residual branch comprising an unknown number of followers has surfaced in Russia.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Australia, Intelligence and Security

ADRIENNE WILMOTH LERNER

Australia gained its status as a British Commonwealth nation in 1901. The nation is largely autonomous, but technically under the British monarch. A 1999 national referendum sought to establish Australia as an independent republic, but Australians voted in favor of remaining part of Commonwealth.

Despite its location, Australia maintains close ties with the United States and Great Britain, joining the Allied efforts in World Wars I and II. Following the Second World War, Britain and the United States aided Australia in reconstructing and modernizing its intelligence community. Australian intelligence services flourished in the early 1950s, rapidly becoming one of the most advanced in the world. The nation's strategic location aided Cold War intelligence and security efforts by providing a regional location from which to monitor the expansion of Communism and Soviet influence in Asia. Today, Australia's strong intelligence community participates in international nonproliferation and anti-terrorism operations.

Australia's intelligence community is divided along traditional distinctions between civilian and military, domestic and foreign intelligence services. The Office of the Attorney General administers Australia's main civilian, domestic, intelligence agency, the Australian Security Intelligence Organization (ASIO). Founded in 1942 as the Allied Intelligence Bureau, the agency was key to allied intelligence and espionage efforts against Japan during World War II. Many of Australia's civilian intelligence services were disbanded after the war, but escalating Cold War tensions prompted their reinstatement in 1949.Today, the ASIO is charged with the protection of national security and focuses its operations on gathering and processing domestic intelligence. Participating in ongoing counter-intelligence operations, the ASIO and the Australian

Protective Service (APS) work to secure government computer, information, and communication systems from outside surveillance.

Though ASIO operations concentrate on broad-scale threats to national interests, duties such as the surveillance of extremist groups and crime syndicates are conducted with aid of accessory intelligence and security organizations. The ASIO works with the Australian Federal Police, the National Crime Authority (NCA), and the Australian Bureau of Criminal Intelligence (ABCI), providing information related to federal criminal investigations.

Australia's other large intelligence agency is the Australian Secret Intelligence Service (ASIS). The ASIS was formed in 1952, after United States and British intelligence proved to the Australian government that Soviet operatives had infiltrated high-levels of the national government. ASIS focuses on foreign intelligence, often joining international intelligence services in global peacekeeping, security, and intelligence operations. The agency relies on a variety of means, including human intelligence, to collect data, but is expressly barred from domestic political espionage or the use of weapons.

Within the ASIS are two important divisions, the Strategic Policy and Intelligence Branch (SPI) and the Intelligence and Counter-Terrorism Policy Section (ITC). The SPI coordinates intelligence and security policy among the nation's civilian intelligence community, sometimes working in close cooperation with military intelligence services. The ICT manages ASIS and inter-agency counter-terrorism efforts, sometimes working with foreign intelligence forces to combat global terrorist networks. Both divisions act as liaisons between the intelligence community and government officials, via the Office of National Assessments in the Office of the Prime Minister or Parliamentary oversight committees.

Australia's civilian intelligence community has undergone increasing scrutiny in the past two decades. In the 1990s, the Australian Parliament conducted a full review of the ASIS to determine its utility to the post-Cold War intelligence community. Parliament decided to keep the agency, but only after a detailed reorganization. In 1996, an Office of Inspector General was established to evaluate and report on the efficiency, ethicacy, and success of Australian intelligence operations. The Intelligence Services Act of 2001 placed ASIS under the stewardship of the Minister of Foreign Affairs and Trade. Parliament further implemented a formal oversight process to promote accountability in both the ASIS and the ASIO.

The Department of Defense oversees military and strategic intelligence forces. The Strategy and Intelligence Program (S&I) is the coordinated intelligence policy for Australia, managing the operations of a variety of agencies. The Defense Intelligence Organization (DIO) and the Defense Security Branch (DSB) are the major intelligence and security departments within the Department of Defense.

Australia maintains one of the world's strongest militaries. The Australian military community has three branches, the Royal Australian Navy, Air Force, and Army, each with its own intelligence units. The Royal Australian Navy conducts both on and offshore communications intelligence and remote surveillance operations. The main concern of Naval intelligence is monitoring foreign intelligence in the South Pacific—Indian Ocean region, and protecting Australia's territorial waters.

Army intelligence conducts a variety of intelligence operations and maintains several intelligence forces. The central Army intelligence agencies are the Defense Intelligence Wing and the Army Intelligence Corps. The routine operations of these forces are predominately classified, and a majority of Army strategic intelligence forces is imbedded in combat units. The Army also operates Australia's primary military intelligence training school.

Australia's Air Force participates in international military operations, but is also charged with aiding the Royal Australian Navy in guarding Australia's territorial waters and expansive coastlines. A special division, the Maritime Patrol Group, assumes part of this responsibility, routinely patrolling the nation's coastal waterways and ports. The Air Force conducts aerial surveillance and remote intelligence operations both within Australia and abroad, in accordance with national and international law.

Law enforcement in Australia is predominantly exercised by the nation's seven territorial police agencies, as well as individual municipal police forces. The Australian Federal Police work with these agencies to infiltrate suspected crime syndicates and prevent drug trafficking, money laundering, counterfeiting, paramilitary activities, and other federal crimes.

In 2001, Australia's intelligence and security agencies joined the international fight against global terrorism. Australia's strategic position in the South Pacific and Indian Ocean regions facilitates work of intelligence community surveillance of extremist groups and terrorist networks in southern Asia and Indonesia. Australian intelligence closely monitors the proliferation of weapons and nuclear technology in Asia and the Indian Ocean region, sharing information it garners with its allies and the United Nations Security Council. Remaining committed to international non-proliferation efforts, Australia joined the Coalition forces in the 2003 war in Iraq, providing military, intelligence, and humanitarian support.

FURTHER READING:

BOOKS:

Polmar, Norman and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1997.

ELECTRONIC:

Australian Security Intelligence Organization. <http://www.asio.gov.au/> (1 April 2003).

Australian Secret Intelligence Service. <http://www.asis.gov.au/> (1 April 2003).

Austria, Intelligence and Security

Following World War II, Austria faced the monumental task of restructuring its national government and intelligence forces. The Nazi government before and during the war substantially increased the nation's intelligence service, but post-war Austria sought to distance itself from the Nazi legacy. The intelligence system was reformed wholly, along with the nation's extensive police and security forces. Because of its central geographic location, post-war Austrian military intelligence agencies played a crucial role in signals intelligence during the Cold War.

Intelligence and security forces in Austria follow the traditional division between military and civilian, domestic and foreign intelligence agencies. The individual military services and the Ministry of Defense supervise military agencies; the Ministry of Interior regulates civilian intelligence agencies and police forces. The main units of the military intelligence force are the *Nachrichtendienstliche Aufklärung*, or Army Intelligence Service, and the *Nachrichtendienstliche Abwehr* , Army Counterintelligence Service. Both agencies primarily focus on external intelligence, often working with Austrian civilian and international intelligence agencies.

Austria's premier civilian intelligence agency is the *Generaldirektion für dieÖffentliche Sicherheitt*, or General Directorate for Public Safety. The agency coordinates domestic intelligence operations and assesses internal national security risks. The *Staatspolizei*, State Police, is the main national police force. The State Police is charged with ensuring public welfare and aiding in the protection of national interests within Austria's borders.

Proving that Austria is a pioneering nation in the widespread use of scientific forensic evidence, its civilian and military intelligence agencies created a nationwide DNA database. Austria's DNA database, the result of cooperation between the Ministry of the Interior and the Institute of Legal Medicine at the University of Innsbruck, was created in 1997. While the police and security agencies actively seek to expand the database, the Austrian government has enacted several measures to insure privacy and fairness in the use of the DNA database. The Ministry of the Interior maintains a database with personal information on each sample, while personal information is withheld from the lab that processes samples for criminal and intelligence investigations. The DNA database is controversial, but Austrian authorities claim the system aids police forces, protects citizens, and greatly improves counterintelligence operations.

Austria's domestic intelligence and security forces declared a new effort to combat money laundering and banking fraud in 2002. The country passed legislation in 2000 and 2001 permitting the continued use of limited anonymous bank accounts. With the creation of a financial market intelligence unit, Austrian intelligence hope to closely monitor the use of such accounts to ensure that their funds were not used to support fraudulent enterprise, illegal trafficking, or terrorism.

Following the September 11, 2001 terrorist attacks on the United States, Austria joined the international coalition to fight terrorism. A member of the European Union, Austria pledged to contribute signals intelligence technology to pan-European counterterrorism measures. Austria's advanced and extensive financial intelligence network aids the discovery and seizure of funds used by terrorist cells. Along with Switzerland, Austria ferreted out nearly forty percent of all such illegal funds seized in Europe in 2001. The Austrian government created an inter-ministerial committee to oversee counterintelligence against the financing of terrorism. The committee, comprised of representatives from the Ministries of Finance, Justice, and the Interior, coordinates the combined efforts of Austria's various counterintelligence units and their cooperation with foreign intelligence agencies.

SEE ALSO

Counter-Intelligence
European Union

Automated Biometric Identification System.

SEE *IDENT (Automated Biometric Identification System).*

Automatic Target Recognition (ATR).

SEE *Brain-Machine Interfaces.*

Aviation Intelligence, History

JUDSON KNIGHT

As lengthy and complicated as any aspect of modern espionage, the history of aviation intelligence has involved the use of aircraft both as intelligence-gathering platforms and as objects of study. These two aspects of aviation intelligence are known as aerial reconnaissance and air technical intelligence, respectively. Over the decades, the United States has emerged as a leader in both regards, from the earliest studies of the British DeHaviland fighter in World War I, to investigations of Soviet MiG fighters during the Cold War. From prop planes to missiles, from rickety biplanes to modern satellites high above

From the Cuban missile crisis overflights to missions in support of United Nations weapons inspection teams in Iraq, the U-2 spy plane performs a diverse array of intelligence gathering operations. ©CORBIS SYGMA.

Earth's surface, aviation intelligence has involved a variety of tools since the time of its inception, just a few years after the birth of flight.

History

The use of aircraft as instruments of both combat and reconnaissance began with the Italo-Turkish War of 1911–12. On October 23, 1911, the Italians first used an aircraft to conduct reconnaissance, against Turkish troops near Tripoli in what is now Libya. On November 1, the Italians again made aviation history when they conducted the first aerial bombing raid against an enemy. In 1912, during the same war, an Italian officer took the first aerial photographs of enemy forces from an airplane.

Aircraft also figured in the U.S. military action against Pancho Villa's Mexican rebels in 1911, and in the 1912–13 Balkan Wars. Yet at the beginning of World War I, the U.S. Army aeronautical division was woefully unprepared to gather intelligence in or on aircraft. To redress this shortcoming, the Army Signal Corps established an air technical intelligence (ATI) facility at McCook Field near Dayton, Ohio. There, in July 1917, they studied their first foreign aircraft, a British DeHaviland-4.

Meanwhile, in Europe, both sides in the world war conducted extensive aerial surveillance, with the Germans alone taking some 4,000 photographs a day. Despite Russian shortcomings in many aspects of military technology and tactics, Russia produced the most notable spy plane of the First World War: the Il'ya Mourometz bomber. Regarded as the world's first strategic reconnaissance aircraft, the Il'ya Mourometz was also the first operational four-engine plane, and could fly deep behind German lines at an altitude beyond the reach of what passed for antiaircraft artillery at the time.

By 1920, the Army ATI facility in Dayton had become the Technical Data Section (TDS), which relocated in 1927 to Wright Field (today known as Wright-Patterson Air Force Base) near Riverside, Ohio. TDS studied more than 300 captured German aircraft, as well as hundreds of British, French, and Italian planes. Weapons, parachutes, and various airplane parts were also among the materials examined by TDS.

During the interwar years, the Germans perfected the airship, which offered considerable promise as a reconnaissance platform at a time when the use of aircraft for this purpose in its infancy. In fact, the *Graf Zeppelin,* most famous of the airships, would barely see service in a reconnaissance capacity during World War II, and then

only in the early months of the conflict. On the other hand, as the Allies would discover after hostilities began, the Germans had studied reconnaissance aircraft, which yielded results in the high-altitude Ju (Junker) 86P and 86R, as well as the extremely durable Ju 88.

Other totalitarian powers also used the interwar years to build up their aerial capabilities. The Fascist Italians set the altitude record, and the Communist Russians the distance record, for aircraft during the 1930s, while the Nazi Germans established speed records. In 1939, more than a decade before jet aircraft came into use, the Germans even demonstrated a turbojet. Also during the 1930s, the Italians in Ethiopia, the Italians and Germans in Spain, and the Japanese in Manchuria, each gained considerable experience at aerial combat.

The most significant effort in aviation intelligence conducted by the British and French during the interwar years was a series of overflights in western Europe. French pilots conducted reconnaissance over western Germany beginning in 1936, and throughout 1939, British and French intelligence agencies sent Australian aviator Sidney Cotton on several flights over German and Italian facilities in Europe and North Africa. Using a specially modified Lockheed 12-A Super Electra, Cotton took a great number of photographs, and continued his reconnaissance missions throughout the war.

World War II. During World War II, the U.S. Army Air Force (established in 1941) modified a number of aircraft, including the B-17 Flying Fortress, B-24 Liberator, and P-51 Mustang, for reconnaissance missions. The United States also developed a few special photo-reconnaissance planes, primarily the F-11 and F-12. By the end of the war, the U.S. Ninth Air Force alone was flying some 600 photo reconnaissance missions a month from bases in the United Kingdom and western Europe.

Beginning with a U.S. Navy B-17 mission over the Solomon Islands in 1942, Allied forces also used aircraft to collect electronic intelligence (ELINT). These efforts continued and escalated throughout the remainder of the war.

At the same time, captured German and Japanese aircraft provided valuable material for study at Wright Field's ATI facility. Officers there learned to glean intelligence from the most seemingly innocuous details; for example, studies of ball bearings on German planes led to a number of successful bombing runs against German ball-bearing plants in 1943. Similarly, the nameplates of Japanese aircraft provided a wealth of target data on defense manufacturing plants in Japan.

Both sides used aircraft as a means of penetrating enemy territory and inserting intelligence operatives. This was an area in which the Germans particularly excelled, using captured Allied aircraft so as to appear less conspicuous as they dropped troops behind enemy lines. The Germans even developed a special three-man container for parachuting operatives and their equipment into hostile territory.

The Cold War

During World War II, the Army Air Force had organized the Air Documents Research Center (ARDC) in London to study literally tons of captured German technical documents. This effort, along with a similar one in the Pacific, greatly informed ATI during the early Cold War, an era in which aviation intelligence in all regards reached maturity.

Among the best-known aspects of the Cold War are the spy flights conducted by the United States against the Soviet Union and its allies using the U-2 and other craft. But this was only one aspect of aviation intelligence in the period after 1945, when the U.S. military turned its attention from the Axis powers to the Communist world.

So great was the number of aircraft populating the skies in the late 1940s that the Air Force—established by the National Security Act of 1947—established Project Sign (later named Project Grudge) to study unidentified flying objects (UFOs). These studies continued through 1969, and as documents released years later would show, there was never any credible evidence to authenticate the popular association of UFOs with extraterrestrial visitors. However, the widespread hysteria over UFOs in the early Cold War era serves to exemplify the palpable sense of external threat that characterized those years.

In September 1946, the United States conducted the first of many intelligence-gathering missions against the Soviets, in this case using a B-17 to collect ELINT from a Soviet station in the Arctic. In May 1951, the Air Force established the Air Technical Intelligence Center (ATIC), the principal military agency for ATI during the 1950s.

During the Korean War, the first major conflict using jet aircraft, ATIC personnel studied captured Soviet-built MiG-15 jets, as well as Il-10s and Yak-9s. At the same time, Allied forces flew reconnaissance using the RB-45C Tornado jet and other craft, collecting hundreds of thousands of images with an average of nearly 2,000 missions a month throughout most of the war.

Even as the jet made its debut, the U.S. military in Europe conducted reconnaissance against the Soviets using much older aerial technology, the balloon. Projects Moby Dick and Grand Union in the early 1950s, and Genetrix in the mid-1950s, proved less than successful, however. These failures helped influence the first overflights of Soviet territory, initially with the British Tornado, and later with the American U-2.

For their part, the Soviets proved highly adept at deceiving U.S. intelligence regarding their capabilities. They invited the American air attaché to the rehearsal for Soviet Armed Forces Day in 1954, at which their guest was shown what appeared to be 28 "Bison" bombers. This led to American estimates of a "bomber gap," though it would later turn out that the second wave of 14 bombers witnessed by the attaché was actually the first wave, flying back over. With the advent of the U-2, U.S. intelligence developed better estimates of Soviet bomber production, and instead of fearing a "bomber gap," U.S. leadership

projected a "missile gap." This, too, would turn out to be a fallacy, thanks to intelligence collection efforts, as well as studies by ATIC in the 1950s.

The capture of U-2 pilot Francis Gary Powers in 1960 did not bring an end to U.S. intelligence-gathering missions. American intelligence continued to use the U-2, as well as other craft, including the SR-71 Blackbird and the A-12 Oxcart. All of these flew extensive missions over North Vietnam, North Korea, China, and the Middle East in the 1960s. Overflights of Cuba using U-2s provided intelligence critical to the resolution of the Cuban Missile Crisis in October 1962. Other important aerial reconnaissance craft used during the 1960s and beyond included the A3D Skywarrior and A3J Vigilante, both flown from aircraft carriers, the RF-4 (a reconnaissance version of the F-4 Phantom), the P-3 Orion, the C-47 and C-130, and others.

In the realm of ATI, ATIC became the Foreign Technology Division (FTD) in July 1961. FTD pioneered a number of technologies for the analysis and production of intelligence. As with ATIC, which brought its first Readix computer on line in 1955, FTD personnel made extensive use of computers such as the Photo Online System (PHOTOLS), an imagery database introduced in 1961. FTD also introduced the Central Information Reference and Control (CIRC) system, a computerized technical database, in 1963. Additionally, FTD pioneered machine translation of foreign languages in the Department of Defense. From an IBM Mark I Translating Device acquired by ATIC in 1959, FTD graduated to a Mark II, which provided word-for-word Russian translations at the rate of 5,000 words per hour, in October 1963.

From the Late Cold War to the Present

During the late 1960s and early 1970s, FTD provided extensive support to U.S. efforts in Vietnam, including the December 1972 "Christmas bombings" of Hanoi and Haiphong. Beginning in 1969, FTD turned its attention from war to the prospect for peace, providing intelligence that greatly assisted U.S. diplomats taking part in the Strategic Arms Limitation Talks (SALT) and later the Strategic Arms Reduction Treaty (START) discussions. Throughout the era of detente that opened with these arms limitation talks, the United States continued to conduct surveillance against the Soviet Union. So, too, did the Soviets, whose acquisition of numerous allies during the 1970s gave them a number of friendly bases from which to conduct aerial reconnaissance missions.

U.S. efforts gained a massive boost with the launch of the KH-11, the first photographic satellite capable of directly transmitting images to a control base, in December 1976. The late Cold War also saw the introduction of unmanned reconnaissance vehicles, first flown by the Air Force in the 1960s. During their 1982 invasion of Lebanon, the Israelis debuted their Scout drones, and in the Persian Gulf War of 1991, the U.S. military made heavy use of the Pioneer, modeled on the Scout. Operation Desert Storm also saw the extensive use of American aerial capabilities, including the E-2C Hawkeye, J-STARS, Skywarrior, Orion, and other craft. Behind the scenes, FTD provided the Pentagon with a veritable encyclopedia of Iraqi equipment, most of which had been produced by the soon-to-be defunct Soviet Union.

In October 1991, the Air Force established the Air Force Intelligence Command (AFIC), of which FTD became a part as the Foreign Aerospace Science and Technology Center (FASTC). Beginning in 1992, FASTC participated in the Open Skies treaty, whereby friendly nations flew observation aircraft freely over one another's territory to collect information on military activities. FASTC operated the Open Skies Media Processing center from 1993. It also served as project manager for Red Tigress, a component of the Ballistic Missile Defense program, formerly known as the Strategic Defense Initiative. In October 1993, AFIC became the National Air Intelligence Center, which in turn merged with Air Combat Command in February 2001.

FURTHER READING:

BOOKS:

Burrows, William E. *By Any Means Necessary: America's Secret Air War in the Cold War.* New York: Farrar, Straus and Giroux, 2001.

Kreis, John F. *Piercing the Fog: Intelligence and Army Air Forces Operations in World War II.* Washington, D.C.: Air Force History and Museums Program, 1996.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

Stanley, Roy M. *World War II Photo Intelligence.* New York: Scribner, 1981.

Taubman, Philip. *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America's Space Espionage.* New York: Simon & Schuster, 2003.

ELECTRONIC:

U.S. Air Combat Command. <http://www2.acc.af.mil/> (April 13, 2003).

SEE ALSO

Aircraft Carrier
Air Force Intelligence, United States
Ballistic Missile Defense Organization, United States
Balloon Reconnaissance, History
Hypersonic Aircraft
J-Stars
Korean War
P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft
Persian Gulf War
Photographic Interpretation Center (NPIC), United States National
Photography, High-Altitude
Reconnaissance
SIGINT (Signals Intelligence)

SR-71 Blackbird
U-2 Spy Plane
Unmanned Aerial Vehicles (UAVs)

Aviation Security Screeners, United States

Prior to the terrorist attacks of September 11, 2001, security screening at the more than 400 major commercial airports around the United States was the work of personnel employed by private firms that contracted with airlines. One outcome of the attacks was the Aviation and Transportation Security Act (ATSA), signed into law by President George W. Bush on November 19, 2001, which placed security screeners under the control of the newly created Transportation Security Administration (TSA). Early assessments of the new program were uneven, and TSA has encountered a number of challenges in what has proven to be one of the largest mobilizations of a civilian agency in U.S. history.

The fact that ATSA was written and passed just two months after the terrorist attacks serves to indicate the intensity of concern over air safety that prevailed in early fall, 2001. In fact, the bill would have passed even more quickly if it had not been for the thorny question of whether the government or private enterprise should control security screeners—and, assuming government control, whether Transportation or Justice was the department better suited for this task.

Also symptomatic of the post-September 11 atmosphere was the spirit of bipartisanship that pervaded the debate over ATSA. Arguments were as heated as ever, but instead of the usual division between Republicans and Democrats, this time the disagreement was between the House of Representatives and the Senate. All agreed that the old system of airlines hiring security screeners and baggage handlers had to be changed and that a new ticket tax would pay for the new federal service. Legislators in the House, however, maintained that the Department of Transportation should hire security contractors, whereas their counterparts in the Senate favored a situation in which the Department of Justice would oversee a program made up of government employees.

In the end, the two houses agreed on a compromise. Over the year that followed passage of the bill, screeners under the employment of the federal government would be phased in at 419 commercial hub airports nationwide. At the same time, up to five airports would participate in a trial program whereby they could use private contractors. After two years, all airports would be permitted to use private contractors under federal supervision, assuming they received approval to do so from the Department of Transportation.

As the debate took place on Capitol Hill, many supporters of free-market economics maintained that private enterprise could inevitably do a better job than government. Yet, the World Trade Center attacks had occurred when private firms were utilized at airports, and as legislators debated ATSA, two companies had already come under scrutiny for alleged violations of federal law. In one case, for instance, the Transportation Department found that a security company had failed to conduct background checks, and had hired screeners with criminal records.

As of January 2002, TSA had just 13 employees, but by November 2002, a year after the passage of ATSA, there were 47,000 newly trained federal security screeners at airports nationwide. TSA spokesman Robert Johnson compared the mobilization to the rush of enlistees that followed U.S. entry into World War II in December, 1941. Others were not as sanguine in their appraisal. Representative Harold Rogers (R-KY) maintained that the average screener at his home facility, Kentucky Bluegrass Airport in Lexington, processed just four people per hour.

There were other concerns as well. According to Transportation Department assistant inspector general for auditing Alexis Stefani, security companies had begun increasing their fees once the government, rather than airlines, was paying the bill. Some of this money went toward increasing the notoriously low pay of airport screeners, which had been about $10,000 a year, to somewhere between $23,600 and $35,400. But, as one company had nearly doubled the rate it charged the government, it had increased employee pay by less than half that much.

Adding to TSA's challenges with the screener program were several legal battles. ATSA had contained a clause barring non-U.S. citizens from employment as airport security screeners, but in November, 2002—just as the newly mobilized screeners went to work—a federal judge in California found the ban on non-citizens unconstitutional. Meanwhile, the American Federation of Government Employees (AFGE), a union of government workers, had attempted to unionize security screeners, a move TSA officials blocked on grounds that a grant of collective bargaining rights to screeners could jeopardize national security. AFGE leaders vowed to continue the effort to unionize the screeners.

Beginning December 31, 2002, all checked bags were supposed to be screened for bombs, but as the deadline approached, it was clear that TSA would have difficulty meeting it. Screeners had already begun a practice of matching bags to passengers—that is, ensuring that for each name listed as the owner of the bag, there was a passenger with that name. Bag matching had been a practice on international flights since the 1980s, but many critics maintained that it would do nothing to stop suicide bombers such as those who perpetrated the September 11, 2001, attacks.

Meanwhile, confiscated items—some of them as unusual as deer antlers and rolling pins—piled up at airports. Some facilities had become so overwhelmed with surplus

A security screener uses a magnetic wand to check a passenger at Chicago's O'Hare International Airport in February, 2002. AP/WIDE WORLD PHOTOS.

items that they contracted with scrap-metal companies to haul away all the knives, scissors, and other sharp items confiscated. Passengers did not have to give up these items permanently, assuming the item was not illegal in the first place, and some airports had facilities for travelers to mail home items that they could not take on planes.

In contrast to these challenges and the dim prognoses offered by some critics, there was much about the federal screener program that pointed to success. The rockiness of its early months was considered inevitable in light of the monumental task administrators faced after September 11. Clearly, a mobilization such as the one required to federalize the screener program can only be properly evaluated after several months or years, not just a few weeks.

FURTHER READING:

PERIODICALS:

Croft, John. "Air Security Bill Clears Lawmakers' Logjam." *Aviation Week & Space Technology* 155, no. 21 (November 19, 2001): 46.

Goo, Sara Kehaulani. "Security Law Called Unconstitutional." *Washington Post.* (November 16, 2002): A12.

———. "Security's Growing Leftovers: Confiscated or Forgotten Objects Piling Up at Country's Airports." *Washington Post.* (February 4, 2003): E1.

Lee, Christopher, and Sara Kehaulani Goo. "TSA Blocks Attempts to Unionize Screeners." *Washington Post.* (January 10, 2003): A19.

Miller, Leslie. "Some Airport Screeners Raise Rates." *San Diego Union-Tribune.* (August 27, 2002): A7.

———. "Deadline Met for Airport Security Screeners." *San Diego Union-Tribune.* (November 17, 2002): A2.

Wald, Matthew L. "Some Busy Airports to Miss Deadline for Scanning Bags." *New York Times.* (November 19, 2002): A23.

ELECTRONIC:

Transportation Security Administration. <http://www.tsa.gov/public/> (March 5, 2003).

SEE ALSO

Air Marshals, United States
Civil Aviation Security, United States
FAA (United States Federal Aviation Administration)
September 11 Terrorist Attacks on the United States
Transportation Department, United States

B

B-2 Bomber

K. LEE LERNER

The United States Air Force B-2 stealth technology low-observable, strategic, long-range bomber is designed to penetrate air defense systems and destroy command, control, and air defense infrastructure during the opening days of a conflict when enemy forces and air defenses are fully operational.

A specially contoured radar absorbing skin and exhaust baffling system makes the flying wing configuration B-2 almost impossible to detect by radar and difficult to target with conventional thermal based system. The leading edges of the B-2 wings angle aft at approximately 33 degrees and trailing edge has a characteristic double "W" form. Although the B-2 does leave a weak RADAR return signature, the delay and low signal return confuse or obscure the B-2 track until it is too close to target—or has long passed the drop point.

The B-2 carries a crew of two and is equipped with a electronic flight instrumentation system (EFIS), that provides variable heads-up display of flight, engine, navigation, and weapons status.

Built by Northrop Grumman and costing more than $2 billion per bomber, the B-2 is the world's most expensive combat airplane.

The stealth technology requires special care, especially to preserve optimal "invisibility" to RADAR. To ensure this care, each B-2 is housed in a special climate-controlled hanger. The skin requires special treating occuring between missions to remove dirt and moisture. These special maintenance requirements meant that prior to Operation Iraqi Freedom the B-2 fleet operated exclusively out of Whiteman Air Force Base in Missouri. As a result, with mid-air refueling, B-2 crews flew 44-hour long round-trip bombing missions over Afghanistan in 2001. To increase the tempo of B-2 missions for Operation Iraqi Freedom, the air force transported (forward deployed) special climate-controlled shelters at bases in England and at the Diego Garcia base in the Indian Ocean.

As of April 2003, the U.S. Air force had 21 operational B-2s. It made its first secret operational flight in 1989. Stealth technology made its debut during the Persian Gulf War (1990–1991) and the B-2 saw action in Kosovo and Afghanistan (Operation Enduring Freedom).

The B-2 is designed to carry satellite-guided bombs, including earth penetrating "bunker busters" that can penetrate 20 or 30 feet of dirt or concrete before detonating. During Operation Iraqi Freedom a B-2 led strike opened the war with an attempt on an Iraqi leadership bunker in Baghdad that western intelligence sources thought might contain Iraqi leader Saddam Hussein. Nearly three weeks later another B-2 dropped four GBU-37 "bunker buster" bombs on a Baghdad target that U.S. intelligence sources source identified as a possible meeting location for Hussein and/or other enemy leaders.The missions were notable because the B-2s, already flying above Baghdad air defenses, were fully integrated with ground based intelligence operations that allowed no more than 35 minutes to elapse from the generation of on-site intelligence to weapons delivery on target.

To maintain its stealth configuration, the B-2 carries all its weapons internally in two separate weapons bays. The B-2 can carry up to 40,000 lbs (18,000 kg) of weapons load, including both conventional and nuclear precision-guided bombs and missiles. Operating at altitudes near 50,000 ft, B-2's can carry a number of conventional and nuclear weapons including, but not limited to, eight GBU-37s or 16 Joint Air to Surface Standoff Missiles (JASSM) and an undisclosed number of Joint Standoff Weapons (JSOW) and AGM-129 Advanced Cruise Missiles (with an estimated strike range of 1,500 miles).

FURTHER READING:

BOOKS:

Jones, Joseph. *Stealth Technology.* Blue Ridge Summit, PA: TAB Books, 1994.

ELECTRONIC:

Air Force Technology, B-2. <http://www.airforce-technology.com/projects/b2/> (April 8, 2003).

SEE ALSO

F-117A Stealth Fighter
Skunk Works
SR-71 Blackbird

B-52

The Boeing B-52 Stratofortress is a bomber made for missions of extraordinarily long range. During the Persian Gulf War in 1991, it flew the longest strike mission in history, taking off from Barksdale Air Force Base in Louisiana, flying to Iraq and launching its cruise missiles, then returning to Barksdale 35 hours after it left—all without stopping. B-52s flew numerous sorties against a variety of targets during Operation Iraqi Freedom in 2003. First deployed in February 1955, the B-52 has proven its endurance over the years, and is expected to remain in service to the middle of the twenty-first century.

Over a period of eight years that ended in October 1962, a total of 744 B-52s were built and delivered. The only models remaining in service are B-52Hs, which are assigned to Air Force Air Combat Command and the Air Force Reserves. The H model, of which 102 were built, is made to carry as many as 20 air-launched cruise missiles.

Over the years, the B-52 has been modified to incorporate ever more advanced weaponry, as well as global positioning and electro-optical viewing systems. Heavy stores adapter make it possible to carry munitions of enormous weight. The aircraft weights 185,000 pounds (83,250 kg) empty, and can take off with a weight of 488,000 pounds (219,600 kg). It can travel 8,800 miles (14,080 km) without refueling, and aerial refueling gives it a range limited only by the needs of the mission and the crew. Its ceiling is 50,000 feet (15,151.5 m).

The same plane that bombed North Vietnam remained in service to bomb Iraq over a quarter-century later. It was also used in Operation Allied Force, the North Atlantic Treaty Organization (NATO) campaign against Serbia in 1999. Engineering analysis conducted at the end of the twentieth century indicated that the B-52 could remain in service past 2045—a full 90 years after its initial deployment.

FURTHER READING:

BOOKS:

Boyne, Walter J. *Boeing B-52: A Documentary History.* New York: Jane's, 1982.

Holder, William G. *Boeing B-52 Stratofortress.* Blue Ridge Summit, PA: AERO, 1988.

Keaney, Thomas A. *Strategic Bombers and Conventional Weapons: Airpower Options.* Washington, D.C.: National Defense University Press, 1984.

Mandeles, Mark David. *The Development of the B-52 and Jet Propulsion: A Case Study in Organizational Innovation.* Maxwell Air Force Base, AL: Air University Press, 1998.

ELECTRONIC:

B-52 Stratofortress. Federation of American Scientists. <http://www.fas.org/nuke/guide/usa/bomber/b-52.htm> (March 8, 2003).

B-52 Stratofortress. U.S. Department of the Air Force. <http://www.af.mil/news/factsheets/B_52_Stratofortress.html> (March 8, 2003).

SEE ALSO

Electro-Optical Intelligence
GPS
Night Vision Scopes
Persian Gulf War

Bacillus Anthracis.

SEE *Anthrax.*

Background Investigations, Non-Governmental.

SEE *Security Clearance Investigations.*

Bacterial Biology

BRIAN D. HOYLE

An understanding of the fundamentals of bacterial biology is critical to bacteriologists and other forensic investigators attempting to identify potential biogenic pathogens that may be exploited as agents in biological warfare or by bioterrorists.

Fundamentals of Bacterial Biology

Bacteria are one-celled prokaryotic organisms that lack a true nucleus (i.e., a nucleus defined by a membrane). Bacteria maintain their genetic material, deoxyribonucleic acid (DNA), in a single, circular chain. Bacteria also contain DNA in small circular molecules termed plasmids.

The Dutch merchant and amateur scientist Anton van Leeuwenhoek was the first to observe bacteria and other

microorganisms. Using single-lens microscopes of his own design, he described bacteria and other microorganisms as "animacules."

In addition to not being contained in a membrane bound nucleus, the DNA of prokaryotes is not associated with the special chromosome proteins called histones, which are found in higher organisms. In addition, prokaryotic cells lack other membrane-bounded organelles, such as mitochondria.

Although all bacteria share certain structural, genetic, and metabolic characteristics, important biochemical differences exist among the many species of bacteria. The cytoplasm of all bacteria is enclosed within a cell membrane surrounded by a rigid cell wall whose polymers, with few exceptions, include peptidoglycans—large, structural molecules made of protein carbohydrate. Bacteria also secrete a viscous, gelatinous polymer (called the glycocalyx) on their cell surfaces. This polymer, composed either of polysaccharide, polypeptide, or both, is called a capsule when it occurs as an organized layer firmly attached to the cell wall. Capsules increase the disease-causing ability (virulence) of bacteria by inhibiting immune system cells called phagocytes from engulfing them.

The shape of bacterial cells are classified as spherical (coccus), rodlike (bacillus), spiral (spirochete), helical (spirilla) and comma-shaped (vibrio). Many bacilli and vibrio bacteria have whiplike appendages (called flagella) protruding from the cell surface. Flagella are composed of tight, helical rotors made of chains of globular protein called flagellin, and act as tiny propellers, making the bacteria very mobile. On the surface of some bacteria are short, hairlike, proteinaceous projections that may arise at the ends of the cell or over the entire surface. These projections, called fimbriae, facilitate bacteria adherence to surfaces.

Other proteinaceous projections, called pili, occur singly or in pairs, and join pairs of bacteria together, facilitating transfer of DNA between them.

During periods of harsh environmental conditions some bacteria can produce within themselves a dehydrated, thick-walled endospore. These endospores can survive extreme temperatures, dryness, and exposure to many toxic chemicals and to radiation. Endospores can remain dormant for long periods (hundreds of years in some cases) before being reactivated by the return of favorable conditions.

Identifying and Classifying Bacteria

The identification schemes of *Bergey's Manual* are based on morphology (e.g., coccus, bacillus), staining (gram-positive or negative), cell wall composition (e.g., presence or absence of peptidoglycan), oxygen requirements (e.g., aerobic, facultatively anaerobic) and biochemical tests (e.g., in which sugars are aerobically metabolized or fermented).

Another important identification technique is based on the principles of antigenicity—the ability to stimulate the formation of antibodies by the immune system. Commercially available solutions of antibodies against specific bacteria (antisera) are used to identify unknown organisms in a procedure called a slide agglutination test. A sample of unknown bacteria in a drop of saline is mixed with antisera that has been raised against a known species of bacteria. If the antisera causes the unknown bacteria to clump (agglutinate), then the test positively identifies the bacteria as being identical to that against which the antisera was raised. The test can also be used to distinguish between strains, slightly different bacteria belonging to the same species.

Pathogens are disease-causing bacteria that release toxins or poisons that interfere with some function of the host's body.

Aerobic and anaerobic bacteria. Oxygen may or may not be a requirement for a particular species of bacteria, depending on the type of metabolism used to extract energy from food (aerobic or anaerobic). Obligate aerobes must have oxygen in order to live. Facultative aerobes can exist in the absence of oxygen by using fermentation or anaerobic respiration. Anaerobic respiration and fermentation occur in the absence of oxygen, and produce substantially less ATP than aerobic respiration.

During the 1860s, the French microbiologist Louis Pasteur studied fermenting bacteria. He demonstrated that fermenting bacteria could contaminate wine and beer during manufacturing, turning the alcohol produced by yeast into acetic acid (vinegar). Pasteur also showed that heating the beer and wine to kill the bacteria preserved the flavor of these beverages. The process of heating, now called pasteurization in his honor, is still used to kill bacteria in some alcoholic beverages, as well as milk.

Pasteur described the spoilage by bacteria of alcohol during fermentation as being a "disease" of wine and beer. His work was thus vital to the later idea that human diseases could also be caused by microorganisms and that heating can destroy them.

Bacterial Growth and Division

A population of bacteria in a liquid medium is referred to as a culture. In the laboratory, where growth conditions of temperature, light intensity, and nutrients can be made ideal for the bacteria, measurements of the number of living bacteria typically reveals four stages, or phases, of growth, with respect to time. Initially, the number of bacteria in the population is low. Often the bacteria are also adapting to the environment. This represents the lag phase of growth. Depending on the health of the bacteria, the lag phase may be short or long. The latter occurs if the

bacteria are damaged or have just been recovered from deep-freeze storage.

After the lag phase, the numbers of living bacteria rapidly increases. Typically, the increase is exponential. That is, the population keeps doubling in number at the same rate. This is called the log or logarithmic phase of culture growth, and is the time when the bacteria are growing and dividing at their maximum speed.

The explosive growth of bacteria cannot continue forever in the closed conditions of a flask of growth medium. Nutrients begin to become depleted, the amount of oxygen becomes reduced, and the pH changes, and toxic waste products of metabolic activity begin to accumulate. The bacteria respond to these changes in a variety of ways to do with their structure and activity of genes. With respect to bacteria numbers, the increase in the population stops and the number of living bacteria plateaus. This plateau period is called the stationary phase. Here, the number of bacteria growing and dividing is equaled by the number of bacteria that are dying.

Finally, as conditions in the culture continue to deteriorate, the proportion of the population that is dying becomes dominant. The number of living bacteria declines sharply over time in what is called the death or decline phase.

Bacteria growing as colonies on a solid growth medium also exhibit these growth phases in different regions of a colony. For example, the bacteria buried in the oldest part of the colony are often in the stationary or death phase, while the bacteria at the periphery of the colony are in the actively-dividing lo phase of growth.

Culturing of bacteria is possible such that fresh growth medium can be added at a rate equal to the rate at which culture is removed. The rate at which the bacteria grow is dependent on the rate of addition of the fresh medium. Bacteria can be tailored to grow relatively slow or fast and, if the set-up is carefully maintained, can be maintained for a long time.

Bacterial growth requires the presence of environmental factors. For example, if a bacterium uses organic carbon for energy and structure (chemoheterotrophic bacteria) then sources of carbon are needed. Such sources include simple sugars (glucose and fructose are two examples). Nitrogen is needed to make amino acids, proteins, lipids and other components. Sulphur and phosphorus are also needed for the manufacture of bacterial components. Other elements, such as potassium, calcium, magnesium, iron, manganese, cobalt and zinc are necessary for the functioning of enzymes and other processes.

Bacterial growth is also often sensitive to temperature. Depending on the species, bacteria exhibit a usually limited range in temperatures in which they can growth and reproduce. For example, bacteria known as mesophiles prefer temperatures from 20° – 50° C (68° – 122° F). Outside this range, growth and even survival is limited. Other factors, which vary depending on species, required for growth include oxygen level, pH, osmotic pressure, light and moisture.

The events of growth and division that are apparent from measurement of the numbers of living bacteria are the manifestation of a number of molecular events. At the level of the individual bacterium, the process of growth and replication is known as binary division. Binary division occurs in stages. First, the parent bacterium grows and becomes larger. Next, the genetic material inside the bacterium uncoils from the normal helical configuration and replicates. The two copies of the genetic material migrate to either end of the bacterium. Then a cross-wall known as a septum is initiated almost precisely at the middle of the bacterium. The septum grows inward as a ring from the inner surface of the membrane. When the septum is complete, an inner wall has been formed, which divides the parent bacterium into two so-called daughter bacteria. This whole process represents the generation time.

Bacterial Genetics

Bacteria can exchange genetic material via conjugation. Genetic recombination between bacteria (or protists) occurs via a cytoplasmic bridge between the organisms. A primitive form of exchange of genetic material between bacteria involving plasmids also can occur. Plasmids are small, circular, extrachromosomal DNA molecules that are capable of replication and are known to be capable of transferring genes among bacteria. For example, resistance plasmids carry genes for resistance to antibiotics from one bacterium to another, while other plasmids carry genes that confer pathogenicity. In addition, the transfer of genes via bacteriophages—viruses that specifically parasitize bacteria—also serves as a means of genetic recombination.

Bioengineering uses sophisticated techniques to purposely transfer DNA from one organism to another in order to give the second organism new characteristics. For example, in a process called transformation, antibiotic susceptible bacteria that are induced to absorb manipulated plasmids placed in their environment can acquire resistance to that antibiotic substance due to the new genes they have incorporated. Similarly, in a process called transfection, specially constructed viruses are used to artificially inject bioengineered DNA into bacteria, giving infected cells some new characteristic.

Bacterial adaptation and resistance. Evolution has driven both bacterial diversity and bacterial adaptation. Some alterations are reversible, disappearing when the particular pressure is lifted. Other alterations are maintained and can even be passed on to succeeding generations of bacteria.

The first antibiotic was discovered in 1929. Since then, a myriad of naturally occurring and chemically synthesized antibiotics have been used to control bacteria.

Introduction of an antibiotic is frequently followed by the development of resistance to the agent. Resistance is an example of the adaptation of the bacteria to the antibacterial agent.

Antibiotic resistance can develop swiftly. For example, resistance to penicillin (the first antibiotic discovered) was recognized almost immediately after introduction of the drug. As of the mid 1990s, almost 80% of all strains of *Staphylococcus aureus* were resistant to penicillin. Meanwhile, other bacteria remain susceptible to penicillin. An example is provided by Group A *Streptococcus pyogenes*, another Gram-positive bacteria.

The adaptation of bacteria to an antibacterial agent such as an antibiotic can occur in two ways. The first method is known as inherent (or natural) resistance. Gram-negative bacteria are often naturally resistant to penicillin, for example. This is because these bacteria have another outer membrane, which makes the penetration of penicillin to its target more difficult. Sometimes when bacteria acquire resistance to an antibacterial agent, the cause is a membrane alteration that has made the passage of the molecule into the cell more difficult. This is adaptation.

The second category of adaptive resistance is called acquired resistance. This resistance is almost always due to a change in the genetic make-up of the bacterial genome. Acquired resistance can occur because of mutation or as a response by the bacteria to the selective pressure imposed by the antibacterial agent. Once the genetic alteration that confers resistance is present, it can be passed on to subsequent generations. Acquired adaptation and resistance of bacteria to some clinically important antibiotics became a great problem in the last decade of the twentieth century.

Bacteria adapt to other environmental conditions as well. These include adaptations to changes in temperature, pH, concentrations of ions such as sodium, and the nature of the surrounding support. This adaptation is under tight genetic control, involving the expression of multiple genes.

Bacteria react to a sudden change in their environment by expressing or repressing the expression of a whole lost of genes. This response changes the properties of both the interior of the organism and its surface chemistry.

Another adaptation exhibited by a great many bacteria is the formation of adherent populations on solid surfaces. This mode of growth is called a biofilm; bacteria within a biofilm and bacteria found in other niches, such as in a wound where oxygen is limited, grow and divide at a far slower speed than the bacteria found in the test tube in the laboratory. Such bacteria are able to adapt to the slower growth rate, once again by changing their chemistry and gene expression pattern. When presented with more nutrients, the bacteria can often very quickly resume the rapid growth and division rate of their test tube counterparts.

A further example of adaptation is the phenomenon of chemotaxis, whereby a bacterium can sense the chemical composition of the environment and either moves toward an attractive compound or shifts direction and moves away from a compound sensed as being detrimental. Chemotaxis is controlled by more than 40 genes that code for the production of components of the flagella that propel the bacterium along, for sensory receptor proteins in the membrane, and for components that are involved in signaling a bacterium to move toward or away from a compound.

Bacteriocidal and bacteriostatic treatment of bacteria.

Bacteriocidal is a term that refers to the treatment of a bacterium such that the organism is killed. Bacteriostatic refers to a treatment that restricts the ability of the bacterium to grow.

Bacteriocidal methods include heat, filtration, radiation, and the exposure to chemicals. The use of heat is a very popular method of sterilization in a microbiology laboratory. The dry heat of an open flame incinerates microorganisms like bacteria, fungi and yeast. The moist heat of a device like an autoclave can cause deformation of the protein constituents of the microbe, as well as causing the microbial membranes to liquefy. The effect of heat depends on the time of exposure in addition to form of heat that is supplied. For example, in an autoclave that supplies a temperature of 121° F (49.4° C), an exposure time of 15 minutes is sufficient to kill the so-called vegetative form of bacteria. However, a bacterial spore can survive this heat treatment. More prolonged exposure to the heat is necessary to ensure that the spore will not germinate into a living bacteria after autoclaving. The relationship between the temperature and the time of exposure can be computed mathematically.

A specialized form of bacteriocidal heat treatment is called pasteurization after Louis Pasteur, the inventor of the process. Pasteurization achieves total killing of the bacterial population in fluids such as milk and fruit juices without changing the taste or visual appearance of the product.

Another bacteriocidal process, albeit an indirect one, is filtration. Filtration is the physical removal of bacteria from a fluid by the passage of the fluid through the filter. The filter contains holes of a certain diameter. If the diameter is less than the smallest dimension of a bacterium, the bacterium will be retained on the surface of the filter it contacts. The filtered fluid is sterile with respect to bacteria. Filtration is indirectly bactericidal since the bacteria that are retained on the filter will, for a time, be alive. However, because they are also removed from their source of nutrients, the bacteria will eventually die.

Exposure to electromagnetic radiation such as ultraviolet radiation is a direct means of killing bacteria. The energy of the radiation severs the strands of deoxyribonucleic acid in many locations throughout the bacterial

genome. With only one exception, the damage is so severe that repair is impossible. The exception is the radiation resistant bacterial genus called *Deinococcus*. This genus has the ability to piece together the fragments of DNA in their original order and enzymatic stitch the pieces into a functional whole.

Exposure to chemicals can be bacteriocidal. For example, the gas ethylene oxide can sterilize objects. Solutions containing alcohol can also kill bacteria by dissolving the membrane(s) that surround the contents of the cell. Laboratory benches are routinely "swabbed" with an ethanol solution to kill bacteria that might be adhering to the bench top. Care must be taken to ensure that the alcohol is left in contact with the bacteria for a suitable time (e.g., minutes). Otherwise, bacteria might survive and can even develop resistance to the bactericidal agent. Other chemical means of achieving bacterial death involve the alteration of the pH, salt or sugar concentrations, and oxygen level.

Antibiotics are designed to be bacteriocidal. Penicillin and its derivatives are bactericidal because they act on the peptidoglycan layer of Gram-positive and Gram-negative bacteria. By preventing the assembly of the peptidoglycan, penicillin antibiotics destroy the ability of the peptidoglycan to bear the stress of osmotic pressure that acts on a bacterium. The bacterium ultimately explodes. Other antibiotics are lethal because they prevent the manufacture of DNA or protein. Unlike bacteriocidal methods such as the use of heat, bacteria are able to acquire resistance to antibiotics. Indeed, such resistance by clinically-important bacteria is a major problem in hospitals.

Bacteriostatic agents prevent the growth of bacteria. Refrigeration can be bacteriostatic for those bacteria that cannot reproduce at such low temperatures. Sometimes a bacteriostatic state is advantageous as it allows for the long-term storage of bacteria. Ultra-low temperature freezing and lyophilization (the controlled removal of water from a sample) are means of preserving bacteria. Another bacteriocidal technique is the storage of bacteria in a solution that lacks nutrients, but which can keep the bacteria alive. Various buffers kept at refrigeration temperatures can keep bacteria alive for weeks.

Bacteria and Disease

Bacteria can multiply and cause an infection in the bloodstream. The invasion of the bloodstream by the particular type of bacteria is referred to as a bacteremia. If the invading bacteria also release toxins into the bloodstream, the malady can also be called blood poisoning or septicemia. *Staphylococcus* and *Streptococcus* are typically associated with septicemia.

The bloodstream is susceptible to invasion by bacteria that gain entry via a wound or abrasion in the protective skin overlay of the body, or as a result of another infection elsewhere in the body, or following the introduction of bacteria during a surgical procedure or via a needle during injection of a drug.

Depending on the identity of the infecting bacterium and on the physical state of the human host (primarily with respect to the efficiency of the immune system), bacteremic infections may not produce any symptoms. However, some infections do produce symptoms, ranging from an elevated temperature, as the immune system copes with the infection, to a spread of the infection to the heart (endocarditis or pericarditis) or the covering of nerve cells (meningitis). In more rare instances, a bacteremic infection can produce a condition known as septic shock. The latter occurs when the infection overwhelms the ability of the body's defense mechanisms to cope. Septic shock can be lethal.

Septicemic infections usually result from the spread of an established infection. Bacteremic (and septicemic) infections often arise from bacteria that are normal resident on the surface of the skin or internal surfaces, such as the intestinal tract epithelial cells. In their normal environments the bacteria are harmless and even can be beneficial. However, if they gain entry to other parts of the body, these so-called commensal bacteria can pose a health threat. The entry of these commensal bacteria into the bloodstream is a normal occurrence for most people. In the majority of people, however, the immune system is more than able to deal with the invaders. If the immune system is not functioning efficiently then the invading bacteria may be able to multiply and establish an infection. Examples of conditions that compromise the immune system are another illness (such as acquired immunodeficiency syndrome and certain types of cancer), certain medical treatments such as irradiation, and the abuse of drugs or alcohol.

Examples of bacteria that are most commonly associated with bacteremic infections are *Staphylococcus*, *Streptococcus*, *Pseudomonas*, *Haemophilus*, and *Escherichia coli*.

The generalized location of bacteremia produces generalized symptoms. These symptoms can include a fever, chills, pain in the abdomen, nausea with vomiting, and a general feeling of ill health. Not all these symptoms are present at the same time. The nonspecific nature of the symptoms may prevent a physician from suspecting bacteremia until the infection is more firmly established. Septic shock produces more drastic symptoms, including elevated rates of breathing and heartbeat, loss of consciousness and failure of organs throughout the body. The onset of septic shock can be rapid, so prompt medical attention is critical.

As with many other infections, bacteremic infections can be prevented by observance of proper hygienic procedures including hand washing, cleaning of wounds, and cleaning sites of injections to temporarily free the surface of living bacteria. The rate of bacteremic infections due to surgery is much less now than in the past, due to the

advent of sterile surgical procedures, but is still a serious concern.

Bacterial infection does not always result in disease—even if a pathogen is virulent (able to cause disease). The steps of pathogenesis (the process of causing actual disease) can depend on a number of genetic and environmental factors. In some cases, pathogenic bacteria produce toxins released extracellularly (exotoxins) that migrate from the actual site of infection to cause damage to cells in other parts of the body.

FURTHER READING:

BOOKS:

Alberts, et. al. *Molecular Biology of the Cell,* 4th ed. New York: Garland Science, 2002.

Cullimore, Roy D. *Practical Atlas for Bacterial Determination.* Boca Raton, FL: CRC Press, 2000.

Dyer, Betsey Dexter. *A Field Guide to Bacteria.* Ithaca, NY: Cornell University Press, 2003.

Groisman, Eduardo A. *Principles of Bacterial Pathogenesis.* Burlington, MA: Academic Press, 2000.

Koehler, T. M. *Anthrax.* New York: Springer Verlag, 2002.

Walsh, Christopher. *Antibiotics: Actions, Origins, Resistance.* Washington, D.C.: American Society for Microbiology Press, 2003.

ELECTRONIC:

The Foundation for Bacteriology, New York University. "Virtual Museum of Bacteria" <http://www.bacteria-museum.org/main1.shtml> (February 5, 2003).

SEE ALSO

Biological and Toxin Weapons Convention
Biological Warfare
Biological Weapons, Genetic Identification
Bioshield Project
Bioterrorism
Bioterrorism, Protective Measures
Viral Biology

Baghdad Pact.

SEE *Cold War (1950–1972).*

Ballistic Fingerprints

A ballistic fingerprint is the unique pattern of markings left by a specific firearm on ammunition it has discharged. Ballistic fingerprinting efficacy as a tool of forensics is a matter of some controversy. On the one hand, many law-enforcement officials insist that ballistic fingerprints are as useful as ordinary fingerprints in linking a round of ammunition to a specific gun. On the other hand, many advocates of gun-owners' rights maintain that these fingerprints change so much over time that they are largely useless as a means of matching a spent round to a firearm.

In 1997, the National Integrated Ballistics Identification Network, established by the Federal Bureau of Investigation and the Bureau of Alcohol, Tobacco, and Firearms, made 8,800 ballistic fingerprint matches, which resulted in the linking of 17,600 crimes. As of 2000, two states—Maryland and New York—had passed laws requiring the ballistic fingerprinting of weapons. Upon selling a firearm, a dealer was required to provide the state with a spent round from the gun, so as to establish a permanent record of the gun's ballistic fingerprint. By 2002, four other states—California, Connecticut, Massachusetts, and New Jersey—were considering ballistic fingerprinting laws of their own.

Police used ballistic fingerprints, in part, to link the shootings of numerous people in the Washington, D.C., area during the fall of 2002 to the accused "Beltway snipers," John Muhammad and John Lee Malvo. The case brought ballistic fingerprinting to national attention, but not all of that attention was positive. Gun ownership advocacy groups such as Gun Owners of America and the National Rifle Association hold that ballistic fingerprints are ineffective in solving crimes, not only because the fingerprint changes over time, but also because criminals usually steal, rather than buy, their weapons. Ballistic fingerprinting, these groups claim, is actually a subtle means of further tightening gun control.

On the other hand, criminologist Daniel W. Webster, director of the Center for Gun Policy and Research at Johns Hopkins University in Baltimore, is an advocate of ballistic fingerprints as a tool of forensics, or the application of scientific techniques to crime-solving. In *Comprehensive Ballistic Fingerprinting of New Guns,* Webster cited research showing that the majority of criminals actually obtain their firearms legally. He also noted studies suggesting that though ballistic fingerprints change over time, these changes do not prevent authorities from establishing a match between a firearm and a spent round.

FURTHER READING:

BOOKS:

Lowry, Edward D. *Interior Ballistics: How a Gun Converts Chemical Energy into Projectile Motion.* Garden City, NY: Doubleday, 1968.

Nickell, Joe, and John F. Fischer. *Crime Science: Methods of Forensic Detection.* Lexington: University Press of Kentucky, 1999.

Webster, Daniel W. *Comprehensive Ballistic Fingerprinting of New Guns: A Tool for Solving and Preventing Violent Crime.* Baltimore, MD: Johns Hopkins Bloomberg School of Public Health, 2002.

ELECTRONIC:

Gun Owners of America. "Why Ballistic Fingerprinting Is Not an Effective Crime Tool." October 2002. <http://www.gunowners.org/fs0203.htm> (January 14, 2003).

SEE ALSO

Forensic Science

Ballistic Missile Defense Organization, United States

CARYN E. NEUMANN

The Ballistic Missile Defense Organization (BMDO), the successor to the Strategic Defense Initiative Organization in the United States Department of Defense, develops systems to detect, track, and destroy ballistic missiles. Working in collaboration with all of the U.S. military departments, all federal agencies, the private sector, and major research institutions, BMDOs use the most current advanced technologies to develop layered defenses that employ complementary sensors and weapons to eliminate threatening missiles in the boost, midcourse, and terminal phases of flight.

BMDO began on May 13, 1993 in the wake of a congressional ban on the deployment of space-based weapons. The collapse of the former Soviet Union had made a global attack upon the U.S. appear much less likely and Congress sought to push the Department of Defense to update missile defense programs to address the dangers of the post-Cold War world. In this changed political climate, Secretary of Defense Les Aspin announced that former President Ronald Reagan's ten-year old Strategic Defense Initiative (popularly known as "Star Wars") would be terminated with missile defense responsibilities transferred to the newly formed BMDO. At this time Aspin also changed the missile defense priorities of the United States, ordering the BMDO to focus on theater missile defense, the protection of U.S. forces deployed overseas, as well as the guarding of allies and friends. National missile defense, the protection of the U.S. from deliberate, accidental, or unauthorized limited ballistic missile attacks, would officially become a secondary priority. At the end of the decade, priorities again shifted in response to the growing threat posed by the spread of ballistic missile technology to perceived non-deterrable countries like Iraq and North Korea. Theater missile defense and national missile defense would subsequently receive equal attention as part of an integrated system of research, development, and testing programs.

To provide defense, BMDO developed a two-tier architecture system designed to intercept missiles as far away as possible from protected areas. The system is based on a hit-to-kill technology that sends a U.S. missile to destroy an enemy missile by crashing directly into it. The upper tier, named Theater High Altitude Area Defense (THAAD), provides a wide area defense including coverage of dispersed assets and population centers. After receiving target identification and guidance information from radar, THAAD intercepts missiles either outside the atmosphere or high in the atmosphere. If the radar and operations center determines that the target has not been destroyed, then the Theater Missile Defense-Ground Based Radar (TMD-GBR) cues a lower tier system, named Patriot PAC-3, to engage the missiles that have evaded THAAD. Patriot PAC-3, an Army-run lower-tier system established in 1999 as an upgrade of the PATRIOT system, includes radar, a communications capability, and a command and control system. Navy Area Defends (NAD), a sea-based, lower-tier system upgrade of the Aegis air defense system that is the Navy's equivalent of PAC-3, will intercept missiles aimed at naval targets.

Research and testing consume the bulk of the BMDO's operating budget. It has focused on the development of kinetic and directed energy weapons such as high-energy lasers and particle-beam systems for potential sea-, ground-, air-, and space-based operations. It also bears responsibility for the creation of sensors to detect a launch, track the thruster booster of a missile through space and the atmosphere, distinguish actual warheads from decoys, and deliver this information to the battle management. It is this latter research that has been shared with the commercial scientific and technological communities. As mandated by law, the BMDO attempts to transfer its technical knowledge to U.S. companies to benefit the national economy. The BMDO Technology Applications program distributes antimissile defense technologies, such as sensors, lasers, and materials, to commercial markets in the non-defense public and private sectors.

The technology transfer program has been among the BMDO's greatest successes. The intercept of missiles with THAAD has proved enormously difficult as well as costly, but blame for the high failure rate has been placed by the Department of Defense military contractors instead of the BMDO system designers. The growing threat from foreign missiles means that the organization will likely continue to receive strong governmental support because the development of a defense system to engage all classes and ranges of ballistic missile remains an urgent need.

FURTHER READING:

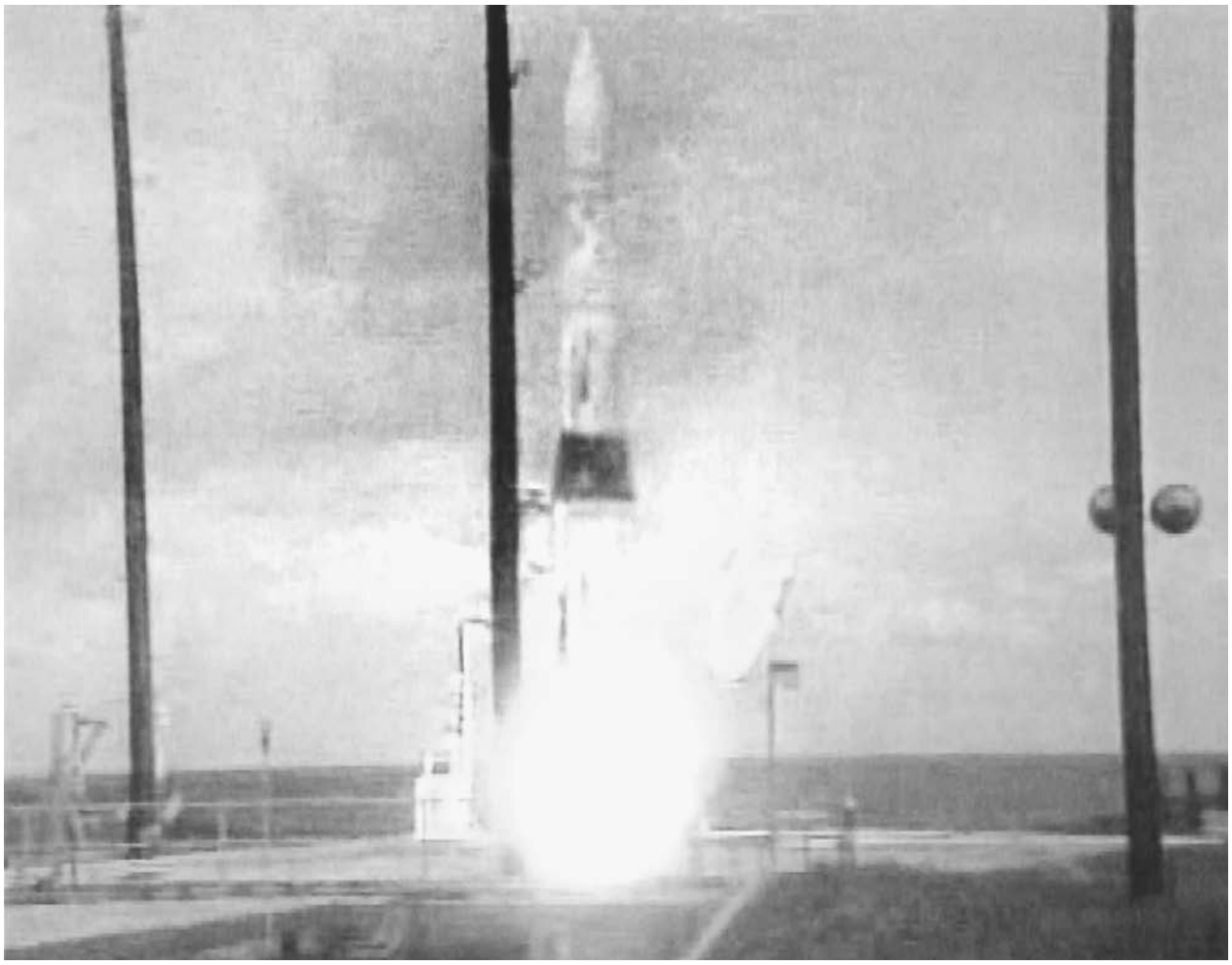
BOOKS:

Handberg, Roger. *Ballistic Missile Defense and the Future of American Security: Agendas, Perceptions, Technology and Policy.* Westport, CT: Praeger, 2002 .

Naveh, Ben-Zin and Azrid Lorber, eds. *Theater Ballistic Missile Defense.* Reston, VA: American Institute of Aeronautics and Astronautics, 2001.

United States General Accounting Office National Security and International Affairs Division. *Ballistic Missile Defense: Evolution and Current Issues.* Washington, D.C.: United States General Accounting Office, 1993.

Werrell, Kenneth P. *Hitting a Bullet with a Bullet: A History of Ballistic Missile Defense.* Maxwell AFB, AL: Air University Press, 2000.



This modified Minuteman intercontinental ballistic missile (ICBM) launched from Vandenberg Air Force Base in the U.S., was intercepted by a prototype interceptor over the Pacific Ocean in 2001. ©REUTERS NEWMEDIA INC./CORBIS.

SEE ALSO

Aviation Intelligence, History
DOD (United States Department of Defense)
RADAR
Strategic Defense Initiative and National Missile Defense

Ballistic Missiles

LARRY GILMAN

Any missile that lofts an explosive payload which descends to its target as a ballistic projectile—that is, solely under the influence of gravity and air resistance—is a ballistic missile. Missiles that do not deliver a free-falling payload, such as engine powered cruise missiles (which fly to their targets as robotic airplanes), are not "ballistic."

A ballistic missile has two basic components: a package contains guidance systems and explosives (the payload) and the rocket that lofts the payload into the upper atmosphere or into space (the booster). Ballistic missiles traverse distance rapidly; a long-range ballistic missile can travel to the other side of the world in 30 minutes. Because they give so little advance warning and deliver small, fast-moving payloads that may contain nuclear weapons capable of destroying entire cities, ballistic weapons are highly destructive and difficult to defend against.

History

The world's first ballistic missile was the V-2, developed by Nazi Germany during World War II. The V-2 , which was first test-launched on October 3, 1942, could deliver a 1,650-lb (750-kg) warhead to a target 225 miles away. Germany launched approximately 3,000 V-2s during the war, but with little military effect; the V-2, lacking the

In 1999, Pakistan test fired this Ghauri II ballistic missile, which is capable of carrying a nuclear warhead deep inside the territory of its neighbor and rival, India.
AP/WIDE WORLD PHOTOS.

sophisticated guidance computers of later ballistic missiles, was inaccurate. Only 50% of V-2s aimed at a given point would, on average, land within 11 mi (17 km) of that point. The V-2 was therefore not aimed at military installations but, like its predecessor the V-1 (the first cruise missile, also developed by Nazi Germany), at the city of London. Some 518 V-2s struck London during the final years of World War II, killing over 20,000 people and making the V-2 the deadliest ballistic missile in history—so far. (The "V" in V-1 and V-2 stands for *Vergeltungswaffe*, German for "retaliation weapon," reflecting the fact that the V-2's primary purpose was not victory but vengeance.)

The United States and Soviet Union were far behind Germany in the design of large rockets during World War II, but both captured V-2 technicians and information at the end of the war and used them to accelerate their own missile programs. The U.S. began by experimenting with captured V-2s, and during the late 1940s built several new rockets of its own based on the V-2. During the 1950s both the Soviet Union and the United States turned their attention to the development of ballistic-missile boosters that could reach the other country's heartland from anywhere in the world. The Soviet Union flight-tested the world's first ICBM, the R-7, in August, 1957. Two months later the R-7 was used to launch the world's first artificial satellite, Sputnik I, and four years later launched the world's first orbital manned space flight. The U.S. was not far behind, and by 1959 had deployed its own ICBMs, the liquid-fueled Atlas and Titan missiles. The Americans also used their ICBMs for early space-flight efforts; the first manned U.S. space flights (Mercury and Gemini programs) used the Redstone, Atlas, and Titan II missile boosters.

Throughout the Cold War, the U.S. and Soviet Union competed in the development of numerous types of ballistic missiles and built thousands of missiles in all range categories. At the peak of their buildup, which occurred in the late 1980s, the two superpowers together possessed approximately 70,000 nuclear weapons, many mounted on ballistic missiles. After the Cold War ended with the dissolution of the Soviet Union in 1991, arms-control agreements were made between Russia and the U.S. that reduced their combined nuclear arsenal to approximately 30,500 warheads. The number of ballistic missiles in all range categories was also drastically reduced.

Nevertheless, the U.S. and Russia still maintain hundreds of nuclear-armed long-range ballistic missiles (i.e., ICBMs and SLBMs) in a state of launch readiness, mostly in submarines and in concrete-lined holes in the ground (silos). Specifically, the U.S. as of 2003 has approximately 550 ICBMs carrying 2,325 warheads and 432 SLBMs carrying 3,616 warheads, while Russia (the nuclear inheritor-state of the now-dissolved Soviet Union) has approximately 756 ICBMs carrying 3800 warheads and 348 SLBMs carrying 2272 warheads. (The warhead numbers are greater than the missile numbers because of MIRVing.) The U.S. and Russia also maintain hundreds of nuclear warheads mounted on various BSRMBs, SRBMs, MRBMs, and IRBMs, and hundreds of nuclear weapons configured for delivery by aircraft rather than by ballistic missile.

Categories of Ballistic Missiles

With the exception of submarine-launched ballistic missiles (SLBMs), ballistic missiles are categorized according to range. Five commonly accepted categories of ballistic missile, with their associated ranges, are as follows: (1) battlefield short range ballistic missiles (BSRMBs: <93 mi [150 km]); (2) short range ballistic missiles (SRBMs: 93–497 mi [150–800 km]), (3) medium range ballistic missiles (MRBMs: 497–1490 mi [800–2400 km]), (4) intermediate range ballistic missiles (IRBMs: 1490–3416 mi [2400–5500 km]), and (5) intercontinental range ballistic missiles (ICBMs:>3416 mi [> 5500 km]).

Alternatively, the U.S. Department of Defense defines ballistic missiles with ranges less than 683 mi (1100 km) as SRBMs, those with ranges between 683 and 1708 mi (1100–2750 km) as MRBMs, those with ranges between 1708 and 3416 mi (1100–5500 km) as IRBMs.

Ballistic missiles can be launched from submarines, silos (i.e., vertical underground tubes), ships, or trailers. All ballistic missiles launched from submarines, regardless of range, are categorized as SLBMs; modern SLBMs have ranges comparable to those of ICBMs. The purpose of mounting ballistic missiles on submarines is to make them secure from attack. Modern missile submarines, such as those in the U.S. Trident class, are difficult to locate and can launch their missiles without surfacing.

Ballistic Missile Function

The flight of a ballistic missile can be divided into three phases: boost phase, cruise phase, and descent (terminal) phase. Boost phase begins with the ignition of the missile's booster rocket. The booster lofts the missile at a steep angle, imparting a high speed to the payload before burning out. The payload and booster then separate, beginning the cruise phase. The spent booster falls back to Earth while the payload, starting to lose speed, continues to gain altitude. If the missile is sufficiently long-range, its payload rises above the Earth's atmosphere during cruise phase, where it jettisons its aerodynamic protective shroud and arcs under the influence of gravity. The payload may be a single cone-shaped warhead or a flat "bus" with several warheads attached to it like upside-down ice-cream cones arranged circularly on a plate.

Individual warheads are not propelled downward toward their targets on the ground, but follow ballistic paths determined by gravity and aerodynamics, gaining speed as they lose altitude. Modern reentry vehicles usually feature small external fins or other steering devices that enable them to control their course, within limits, as they fall through the atmosphere; though such maneuverable

reentry vehicles (MARVs) are not, strictly speaking, ballistic objects, missiles delivering them are still termed "ballistic" missiles for convenience. Maneuverability increases accuracy; a modern MARV delivered by ICBM or SLBM can land within a few hundred feet of its target after a journey of thousands of miles. Warheads may explode in the air high above their targets, on the surface, or under the surface after striking into the ground.

Boosters. The booster rockets of early ballistic missiles were powered by liquid fuels. A liquid-fuel rocket carries fuel (hydrazine, liquid hydrogen, or other) and liquid oxygen in tanks. Pressurized streams of fuel and oxygen are mixed and ignited at the top of a bell-shaped chamber: hot, expanding gases rush out of the open end of the bell, imparting momentum to the rocket in the opposite direction. Liquid fuels are unwieldy, as they must be maintained at low temperatures and may leak fuel or oxygen from tanks, pipes, valves, or pumps. Early U.S. ICBMs such as the Atlas and Titan I required several hours of above-ground preparation, including fueling, before they could be launched.

Since the late 1950s, ballistic-missile design has concentrated on solid-fuel boosters, which require less maintenance and launch preparation time and are more reliable because they contain fewer moving parts. Solid-fuel rockets contain long, hollow-core casts of a fuel mixture that, once ignited, burn from the inside out in an orderly way, forcing gases out the rear of the rocket. Starting in the early 1960s, liquid-fuel ballistic missiles were gradually phased out of the U.S. and Russian arsenals in favor of solid-fuel missiles. The first U.S. solid-fuel ICBM was the Minuteman I missile (so-called because of its near-instant response time), which was deployed to underground silos in the Midwest starting in 1962. Today, the ballistic-missile fleet of the United States consists almost entirely of solid-fuel rocket boosters. The Minuteman III, for example, like the Minuteman I and II it replaces, has a three-stage solid-fuel booster and a range of over 7000 miles. (*Stages* are independent rockets that are stacked to form a single, combined rocket. The stages are burned from the bottom up; each is dropped as it is used up, and the stage above it is ignited. The advantage of staging is that the booster lightens more rapidly as it gains speed and altitude. There are single-stage, two-stage, and three-stage ballistic missiles; the greater the number of stages, the longer the range of the missile.)

Payloads, warheads, and MIRVs. As mentioned above, the payload of a ballistic missile may be either a single warhead or a bus bearing several warheads which can each be sent to a different target in the same general area (e.g., the eastern United States). Such a payload is termed a *multiple independently targetable reentry vehicle* (MIRV) system, and missiles bearing multiple independently targetable warheads are said to be MIRVed. The first MIRVed missiles were deployed the U.S. in 1970; only long-range ballistic missiles (ICBMs and SLBMs) are MIRVed. After a MIRV bus detaches from the burnt-out upper stage of its booster, it arcs through space in its cruise phase. It may possess a low-power propulsion system that enables it to impart slightly different velocities to each of its warheads, which it releases at different times. (Slight differences between individual warhead trajectories in space can translate to relatively large differences between trajectories later on, when the individual warheads are approaching their targets.) The U.S. Minuteman III ICBM is a modern MIRVed missile carrying up to three warheads; other MIRVed missiles, such as the MX, have been capable of carrying up to 10 warheads.

Regional or approximate targeting for each MIRVed warhead is achieved by bus maneuvering and release timing during cruise phase. During descent phase, the warhead may steer itself to its precise target by means of inertial guidance, radar, or a combination of the two. Inertial guidance is based on the principle that every change in an object's velocity can be sensed by that object as an acceleration. By knowing its exact prelaunch location and state of motion (e.g., by consulting the Global Positioning System) and by precisely measuring all accelerations during and after launch, an inertial guidance system can calculate its location at all times without needing to make further observations of the outside world. Ballistic-missile payloads rely primarily on inertial guidance to strike their targets; MARVs may refine their final course by consulting the Global Positioning System (as is done, for example, by the Chinese CSS-6 SRBM) or by using radar to guide themselves during final approach (as was done, for example, by the Pershing II IRBM deployed by the U.S. in Europe during the 1980s).

The nuclear warheads mounted on modern long-range ballistic missiles are usually thermonuclear warheads having yields in the range of several hundred kilotons to several megatons. (One kiloton equals the explosive power of one thousand tons of the chemical explosive TNT; one megaton is equivalent to a million tons of TNT.) Those nations that do not possess nuclear weapons mount conventional-explosive warheads on their ballistic missiles.

Proliferation. Ballistic missiles offer the ability to inflict sudden damage on a distant foe. This is the central military motive behind their invention by the U.S. and Soviet Union and behind their more recent development or purchase by many states. The U.S. Department of State estimates that at least 27 nations now possess, or are in the process of developing, ballistic missiles. However, China, France, and the United Kingdom are the only countries beside the U.S. and Russia to possess *long-range* ballistic missiles (i.e., ICBMs and SLBMs): China, 20 ICBMs with 20 warheads; France, 64 SLBMs with 384 warheads; and the UK, 48 SLBMs with 185 warheads.

Of the many countries that possess some type of ballistic missile, only China, France, India, Israel, Pakistan, Russia, the United Kingdom, the United States, and (as of

early 2003) possibly North Korea have nuclear weapons to mount on them. India and Pakistan, which in the 1990s and early 2000s fought several border wars in the last few decades, are engaged in a competitive ballistic-missile development race in which India is distinctly ahead. India has produced an SRBM, the Prithvi (range 155 mi [250 km]), and an IRBM, the Agni (range 1550 mi [2,500 km]); it also has built several space-launch rockets capable of being used as ICBMs. Pakistan manufactures several BSRMBs and SRBMs of its own (the Hatf I, II, and III missiles, all with ranges of 373 mi [600 km] or less) and has purchased M-11 SRBMs from China. Israel's Jericho 2B IRBM (range 930 mi [1,500 km]) can reach southern Russia and much of the Middle East; North Korea's Taep'o Dong 2 IRBM (range 2,480–3,720 mi [4,000–6,000 km]) can reach much of mainland Asia, Japan, the Pacific, and probably Scandinavia. Some states (e.g., Japan, Sweden) are technically capable of building both ballistic missiles and nuclear weapons but have refrained from doing so; however, many more states are likely to develop ballistic missiles in the near future.

FURTHER READING:

BOOKS:

Cimbala, Stephen J. *Nuclear Strategy in the Twenty-First Century.* Westport, CT: Praeger, 2000.

Cochran, Thomas B., William M. Arkin, and Milton M. Hoenig. *Nuclear Weapons Databook: Vol. I, U.S. Nuclear Forces and Capabilities.* Cambridge, MA: Ballinger Publishing Company, 1984.

ELECTRONIC:

"Ballistic Missile Threats." Centre for Defense and International Security Studies, Lancaster University, UK. Aug. 10, 2001. <http://www.cdiss.org/bmthreat.htm>; (March 3, 2003).

Daniel Smith. "A Brief History of 'Missiles' and Ballistic Missile Defense." Center for Defense Information. 2000. <http://www.cdi.org/hotspots/issuebrief/ch2/> (March 3, 2003).

SEE ALSO

Ballistic Missile Defense Organization, United States
Nuclear Weapons
Strategic Defense Initiative and National Missile Defense

Balloon Reconnaissance, History

JUDSON KNIGHT

Just three months after the first manned balloon flights in France in 1783, Benjamin Franklin wrote of the new invention's military capabilities. Over the next 13 decades, balloons would increasingly serve fighting forces both for reconnaissance—particularly in the American Civil War—and later as bombers. The latter application would reach its apex with the German airships of World War I, a conflict in which the airplane proved itself a vastly superior instrument of aerial combat. Thereafter, the principal nation using balloons for surveillance was not Germany, but the United States, which employed them in the Second World War. American use of surveillance balloons and blimps continued even into the Cold War and the early twenty-first century war on drugs and homeland defense efforts.

An American major in the basket of an observation balloon flying over fields near the front lines in France, June 1918. ©CORBIS.

The Principle of Buoyancy

Balloons and airplanes both rise into air, but by very different means. An airplane flies accordance to aerodynamic principles involving the relative pressure and speed of fluids (air and other gases are considered fluids in the terms of physics), and its lift depends heavily on the design of the wing's leading edge—a design borrowed from that which nature has given to the bird's wing. A balloon, on the other hand, rises according to the principal of buoyancy discovered by the Greek physicist and mathematician Archimedes (c. 287–212 B.C.)

According to Archimedes's principle, the buoyant force of an object immersed in fluid is equal to the weight of the fluid displaced by the object. This explains how a

metal aircraft carrier weighing thousands of tons can float. If all the metal were crushed into a ball, it would sink to the bottom of the ocean, but when designed properly, the area inside the hull weighs less than the water it displaces. Similarly, the gases inside the envelope of a balloon must weigh less than the air around them.

Gases for buoyancy. There are three gases practical for use in balloons: hydrogen, helium, and heated air. Hydrogen would be ideal, except for the fact that it is extremely flammable, and helium, which was not discovered in elemental form until the 1860s, is extremely expensive to produce. On the other hand, heated air requires only a reliable heating source.

As French chemist J. A. C. Charles, an early balloon enthusiast, recognized in his famous law of gases, heating a gas increases its volume; thus, the air molecules inside the envelope of a balloon tend to spread apart, reducing the density of the air inside and making the craft buoyant. Ironically, Charles introduced the hydrogen balloon, which would dominate until the 1937 explosion of the *Hindenburg*. Since that time, most balloons have used heated air.

From the late eighteenth century to the U.S. Civil War (1783–1863). French brothers Joseph-Michel and Jacques-Etienne Montgolfier launched the first balloon on June 5, 1783. Later that year, the Montgolfiers sent up the first balloon crew—a sheep, a rooster, and a duck—and on November 21, Jean-François Pilatre de Rozier became the first human being to ascend in a balloon.

The first army air corps was born in revolutionary France in 1794, when a balloon contingent was established for reconnaissance purposes. The French used balloon reconnaissance extensively in the Napoleonic wars, and by the mid-nineteenth century, Britain, Russia, Austria, and Denmark were using balloons for military purposes.

In 1849, the Austrians undertook the first aerial bombardment campaign, using 200 unpiloted hot-air balloons against the Venetians. The effort proved disastrous when winds blew the balloons, whose explosives were set on timers, back to the Austrian side.

Balloons in the early United States. Whereas the Austrians' experience illustrated the problematic nature of balloons as bombers, the American experience in the Civil War showed that balloons had great potential for reconnaissance and purposes other than combat. For several decades, visionary military leaders had called for the use of balloons in warfare. During the Seminole War in Florida (1835–1842), Col. John Sherburne tried unsuccessfully to gain War Department support for a plan to use balloons for spotting Seminole campfires at night. A decade later, in the Mexican War, John Wise, later dubbed "the Father of American Aeronautics," proposed a balloon bombing campaign against the city of Veracruz, although the War Department ignored his proposal.

During the Civil War, Wise was one of several who proposed the use of balloon reconnaissance by the Union, but by far the most successful promoter of balloon reconnaissance was Thaddeus Lowe. While attempting unsuccessfully to cross the Atlantic by balloon, Lowe had found himself behind Confederate lines at the outset of the war, in April 1861. Having observed some military activity, Lowe offered his services to Union leadership, and proved to be the only balloonist the Union seriously considered. On June 17, 1861, Lowe and a telegraph officer ascended 500 feet (152 m) above the Columbia Armory in Washington, with telegraph lines running along the rigging wires and connecting them to the War Department and White House. Lowe's efforts won the support of President Abraham Lincoln, and over the next two years, the Union Army became host to one of the war's great experiments in technology and intelligence.

The Union balloon corps. During the winter of 1861–1862, Lowe gathered around himself an aeronautic crew that included two other ballooning pioneers, brothers Ezra and James Allen. They developed a system of signals from the ground to the air, and a method for getting balloons aloft while avoiding trees. They also found an effective means of transporting balloons, primarily aboard barges. While aloft, aeronauts, sometimes accompanied by military observers, would study details ranging from dust clouds to campfires, counting or if necessary merely estimating the number of enemy troops they saw. With a telescope, they could see as far as 30 miles (48 km) on a clear day.

The Confederates' many attempts to shoot down Lowe's balloons, which earned him the title "most shot-at man in the war," illustrated the effect the balloons had on morale. Years later, Confederate artillery officer E. P. Alexander said, "I never understood why the enemy abandoned the use of military balloons.... Even if the observers never saw anything, they would have been worth all they cost for the annoyance and delays they caused us in trying to keep our movement out of sight." The Southern states attempted to field their own balloons, but in this as in other areas, they lacked the technological means to effectively challenge the North. They finally did send up a balloon, made from silk dresses, but the Union promptly captured it.

Although Lowe's corps had the technological advantage over the enemy, the Union ballooning effort was doomed. Most Union generals failed to see the balloon's usefulness for a reconnaissance, and the fact that Lowe and his crew were civilians only added to the War Department view of them as outsiders. Lowe resigned in April 1863, and although the Allen brothers kept the balloons aloft for a few months, the corps had faded away by that summer. One of their last intelligence reports was of Confederate troops moving from Fredericksburg, Virginia,

toward the Blue Ridge Mountains, the opening movements of a campaign that would lead to the decisive battle at Gettysburg, Pennsylvania.

From the Franco-Prussian War to World War I (1870–1918)

Balloons again proved their effectiveness for the French during the siege of Paris in 1870, when 66 balloons managed to transport 102 people and more than 2 million pieces of mail past the Germans. Impressed, the Germans formed their own balloon corps in 1884, and the Austrians in 1893. Russia opened a school of aeronautic training outside St. Petersburg. Britain, meanwhile, began military balloon training in 1880.

Still, the experience of the French in 1870 illustrated the limits of balloons. First, they could not be steered, and could only go with the wind. Second, the Prussians were rumored to have developed anti-aircraft guns that could shoot them down—which, while not true at the time, boded ill for low-flying craft.

Rise of the airship. By that time, a new variation on the old-fashioned envelope-and-gondola balloon had begun to show promise. This was the airship, an idea whose origins dated back to the Montgolfiers' era. Around the same time as the first balloon launches, another French designer, Jean-Baptiste-Marie Meusnier, began experimenting with a more streamlined, maneuverable model.

It was more than a century before Meusnier's idea became a reality. In 1898, Alberto Santos-Dumont of Brazil combined a balloon with a propeller powered by an internal-combustion engine. Although these men more clearly qualify as the fathers of the airship, they were to be eclipsed in history by a figure whose name became a synonym for it: Germany's Count Ferdinand von Zeppelin.

The Zeppelin. Zeppelin created a lightweight structure of aluminum girders and rings that made it possible for an airship to remain rigid under varying atmospheric conditions. The Zeppelins of World War I were legendary, as terrifying to the enemy as they were inspiring to Germans who sent them aloft.

At first, the German army failed to grasp their potential, so the navy began using them to scout British cruisers in the North Sea. At a time when aircraft were still in their infancy, and when the British fleet used light cruisers for reconnaissance at sea, the Zeppelin was both safer than an airplane and vastly more economical than a cruiser. In 1914, Zeppelin's company was turning out three airships a year; two years later, it was producing more than two a month.

Along the way, the use of Zeppelins as bombers overshadowed their role as reconnaissance craft. In 1915—fully a quarter-century before the Nazis' more famous bombardment—the Germans launched the first air battle of Britain. Far beyond the actual physical damage the Zeppelins wrought was the psychological effect of the dark shapes appearing in the British sky. At 10,000 feet (3,048 m), they were too high for antiaircraft guns of the time to reach them, and therefore they rained terror at will.

Even so, Zeppelins were cumbersome, dangerous craft, and in the final analysis, they were not cost-effective either for reconnaissance or for bombing. By September, 1916, the British had at their disposal explosive bullets that, when fired from an airplane, could shoot Zeppelins from the sky. Even the psychological value of Zeppelins proved a double-edged sword: recruiting posters and anti-German propaganda made heavy use of the Zeppelin as a symbol of the enemy.

Balloons from the 1920s to the Present

For a few years after war's end, airships constituted the luxury liners of the skies, but the *Hindenburg* crash signaled the end of relatively widespread airship transport. In the meantime, the U.S. Navy had taken an interest in airships, several of which were built for it by the Goodyear Tire and Rubber Company during the 1920s and early 1930s. After several mishaps involving rigid airships, the navy switched entirely to nonrigid airships, or blimps.

During World War II, the U.S. Navy was to be the only fighting force on either side to use airships. After the attack on Pearl Harbor, Congress authorized the construction of some 200 airships, which the navy used for photographic reconnaissance, scouting, minesweeping, antisubmarine patrols, search and rescue, and escorting convoys. Some 89,000 ships were escorted by airships during the war, and not a single one was lost. Although they were slow compared to airplanes, balloons could stay aloft for as much 60 hours, a decided advantage in an era before in-flight refueling.

Non-reconnaissance uses of balloons during the war included their employment by the British as protection against bombers, which had to fly over them to avoid their mooring wires, thus placing the Luftwaffe further from their targets and impairing accuracy. The Japanese employed some 1,000 "Fu-Go Weapons," or balloons equipped with bombs, which they sent eastward across the Pacific. These landed in some 16 U.S. states, as well as in Alaska, Canada, and Mexico. They killed only six civilians—a mother and her five children in Lakeview, Oregon, in May 1945—and the fact that the U.S. media agreed not to report news of the bombings greatly blunted their potential psychological effect.

The Cold War: Project GENETRIX. By far, the most significant use of balloon reconnaissance during the Cold War was Project GENETRIX. The program had its origins in a 1951 study by the RAND corporation, and in December 1955,

President Dwight D. Eisenhower gave approval for the U.S. Air Force to launch 516 camera-carrying balloons over Eastern Europe, the Soviet Union, and the People's Republic of China.

GENETRIX proved a disaster in several regards. Only 34 balloons—about 7% of the total—survived and produced usable, useful images. Worse than the poor return ratio was the public-relations opportunity that the project provided to the communist bloc, which protested U.S. spying and used information on GENETRIX for propaganda purposes.

Central Intelligence Agency (CIA) officials called on the air force to halt GENETRIX, which it did in February 1956. At the time, the CIA was planning the launch of U-2 overflights, and they feared that GENETRIX would turn Eisenhower against the concept of overflights. Additionally, they were concerned that the program might negatively affect an effort by the Free Europe Committee, a CIA front based in West Germany, to drop propaganda leaflets over Eastern Europe.

The failure of GENETRIX concealed several successes. The images of the Soviet Union it did produce provided the best available record between World War II and the advent of the U-2 reconnaissance plane and later satellites. Additionally, the high-flying balloons, which averaged an altitude of 45,800 feet (13,960 m), provided data on wind currents that helped scientists determine the best flight paths for the U-2.

Finally, the most curious benefit of GENETRIX was the fact that a steel bar that secured the envelope, cameras, and ballasting equipment happened to measure 2.99 feet (91 cm)—exactly the same size as the wavelength of Soviet radar known as TOKEN to NATO (North Atlantic Treaty Organization) forces. Because it resonated when TOKEN pulses hit it, the bar helped NATO radar operators locate previously unknown radar installations. This, too, aided the U-2 project.

Balloon reconnaissance today. The navy, which had continued its balloon program until 1962, attempted to revive it in the 1980s, but Congress cut off all funding in 1989. Yet, the usefulness of balloons and blimps for surveillance is far from exhausted. Their virtual invisibility with regard to radar has reinvigorated interest in blimps on the part of the U.S. Department of Defense, which has discussed plans to use airships as radar platforms in a larger Strategic Air Initiative.

Meanwhile, the air force employs aerostats, or unmanned, aerodynamically shaped blimps tethered by a single cable, in its Tethered Aerostat Radar System, a counter-narcotics surveillance program along the U.S.-Mexico border. Aerostats offer a number of advantages, including enormous detection range and coverage. Typically occupying an altitude of about 15,000 feet (4,500 m), an aerostat can cover 185 square miles (480 sq km) and track smaller, lower-flying aircraft such as those used by drug smugglers. They can operate virtually without break at low cost, and need come down only for routine maintenance and severe weather. It is calculated that an aerostat can provide surveillance at a cost about 5% as great as that of an airplane. Kept aloft by helium, a highly non-reactive gas, they also have a considerably accident free record of operation.

FURTHER READING:

BOOKS:

Brugioni, Dino A. *From Balloons to Blackbirds: Reconnaissance, Surveillance, and Imagery Intelligence: How It Evolved.* McLean, VA: Association of Former Intelligence Officers, 1993.

Evans, Charles M. *The War of the Aeronauts: A History of Ballooning during the Civil War.* Mechanicsburg, PA: Stackpole Books, 2002.

Lebow, Eileen F. *A Grandstand Seat: The American Balloon Service in World War I.* Westport, CT: Praeger, 1998.

Peebles, Curtis. *The Moby Dick Project: Reconnaissance Balloons over Russia.* Washington, D.C.: Smithsonian Institution Press, 1991.

PERIODICALS:

Fanton, Ben. "View from above the Battlefield." *America's Civil War* 14, no. 4 (September 2001): 22–28.

Nahum, Hazi, and Sheike Marom. "Aerostat-Borne Systems for Defense and Homeland Security." *Military Technology* 26, no. 8 (August 2002): 102–108.

ELECTRONIC:

U.S. Centennial of Flight. <http://www.centennialofflight.gov> (March 13, 2003).

SEE ALSO

Civil War, Espionage and Intelligence
Reconnaissance
U-2 Spy Plane
World War I

Basque Fatherland and Liberty (ETA)

The ETA was founded in 1959 with the aim of establishing an independent homeland based on Marxist principles in the northern Spanish Provinces of Vizcaya, Guipuzcoa, Alava, and Navarra, and the southwestern French Departments of Labourd, Basse-Navarra, and Soule. The Basque Fatherland and Liberty (ETA) group also operates as, or is known as Euzkadi Ta Askatasuna.

Organization activities. The ETA is primarily involved in bombings and assassinations of Spanish government officials, security and military forces, politicians, and judicial figures. ETA finances its activities through kidnappings, robberies, and extortion. The group has killed more than 800 persons and injured hundreds of others since it began lethal attacks in the early 1960s. In November 1999, ETA broke its "unilateral and indefinite" cease-fire and began an assassination and bombing campaign that had killed 38 individuals and wounded scores more by the end of 2001.

The actual size of ETA is unknown, but estimates indicate that ETA may have hundreds of members, plus supporters. The ETA operates primarily in the Basque autonomous regions of northern Spain and southwestern France, but also has bombed Spanish and French interests elsewhere.

ETA members have received training at various times in Libya, Lebanon, and Nicaragua. Some ETA members allegedly have received sanctuary in Cuba while others reside in South America.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Bathymetric Maps

■ ALEXANDR IOFFE

Bathymetric mapping refers to construction of ocean and sea maps—bathymetric maps (BM). Bathymetric maps represent the ocean (sea) depth depending on geographical coordinates, just as topographic maps represent the altitude of Earth's surface at different geographic points. Bathymetric maps are critical to submarine navigation, submarine evasion tactics, and in predicting the location of ocean signal channels.

The most popular kind of bathymetric maps is one on which lines of equal depths (isobaths) are represented. Like geographical maps of the surface of Earth, bathymetric maps are constructed in definite cartography projection. Mercator projection is used perhaps more often in constructing bathymetric maps, and has been used for a long time in constructing sea charts that are used for sailing in all latitudes except Polar ones.

The creation of a bathymetric map of a given region depends above all on the amount of depth measurement data for that region. Before the invention of the echosounder in the 1920s, ocean (sea) depth could be measured only by lead. Such measurements were quite rare; these measurements were made only in isolated points, and creation of bathymetric mapping was practically impossible. Thus, the structure of the ocean floor was virtually unknown. It should be noted, for example, that the most important structure in the Atlantic Ocean, the Middle-Atlantic ridge, was discovered and began to be investigated only after World War II. Another important factor for creating bathymetric mapping is determining geographical coordinates of the point where the depth measurement is made. It is evident that when these determinations are more precise, then the maps are better. As of 2003, the GPS (Global Positioning System) is used for determining the coordinates of the measurement points.

When constructing topographic maps of land, one can always measure the altitude of any point of the surface precisely. However, when constructing a bathymetric map, it is practically impossible to determine the exact depth of any point of the bottom of the sea. Obviously, bathymetric maps are more precise when more data of depth measurement per surface area unit in the given region are available. Currently, the most precise and detailed bathymetric maps result from using data from multibeam echosounding. The multibeam echosounder is a special kind of echosounder, which is located on board of the vessel and measures the depth simultaneously in several points of the bottom. These points are located on the straight line perpendicular to the vessel track. These points themselves are determined by the reflection of several acoustical pulses (beams) directed from one point at different angles to the vertical. The determination of depth in this method is performed regularly within periods of several seconds during the vessel motion. The measurement data are stored in a computer, and using them the map of an isobath of narrow bottom stripe can be represented periodically, or these data can be represented on a monitor.

It should be noted that in addition to the multibeam echosounder, other devices that measure depths simultaneously in several points of the ocean bottom have been developed, but all of them are based on the reflection of sound signals from the bottom.

If there are a lot of measurement data (more precisely this means that the average amount of measurement data

per surface area unit is relatively big, and the measurement points themselves are located uniformly on the surface investigated), then computer methods of isobath construction are used. In this case, two stages of the work are executed: first using the measurement data obtained in arbitrary points of the surface, the values of the depth in knots of a regular grid are calculated (sometimes this stage is known as digital surface model construction), and then using these grid values, coordinates of different isobaths are determined (grid values are used also for other forms of bathometric mapping representations, 3-D views, for example). There are many algorithms of digital model creation, such as the least mean square method, and the so-called Kriging method, as well as algorithms of constructing an isobath of its own using depth grid values. To construct a precise map of the region it is necessary to perform echosounding surveying on it in such a manner that map stripes, obtained in different vessel tracks, would be as close to each other as possible, or even overlap. After performing such surveying, all data are joined together, and the map of the entire region is constructed.

It should be noted that currently, only small part of Earth's ocean bottom (several percent) is covered by such precise measurements. In some places, little data is available in a study area, obtained by one beam echosounder, or there is no data at all. In these cases, scientists try to use results of other geophysical measurements, first of all gravimetric measurements, to determine ocean depth. For example, methods of determination of ocean bottom topography using satellite altimetry or marine gravimetry data are useful. Even with using otherwise accurate satellite technology, indirect geophysical methods for determining the ocean bottom depth can always contain a mistake. The Earth's surface is a very complex formation, so the precise value of the ocean depth at a given point should be determined if necessary only by direct measurement.

In the case where depth measurement data are small in numbers for a given region, indirect methods are used in constructing bathymetric mapping, such as geomorphology analysis, for example. Scientists also take into account geological considerations and even human intuition, which can at times be useful.

Several international organizations are currently working on bathymetric mapping. The unclassified *General Bathymetric Chart of the Oceans* (GEBCO, in the scale 1:5000000), which may be considered a reference map, is one example. In this map, data of many regional bathymetric maps are collected, taking into account the different methods of their construction. There is also a digital version of this map (on CD), where files are represented in different formats, and in ASCII codes in particular, and where isobaths are represented in the so-called vector format.

Bathymetric mapping is finding increasing scientific and commercial use. For example, bathymetric maps are important in forging different underwater communications.

■ FURTHER READING:

BOOKS:

Barnes, J. *Basic Geological Mapping,* 3rd ed. New York: John Wiley and Sons, 1995.

PERIODICALS:

Perez, P. "SPOT Satellite Data Analysis for Bathymetric Mapping." *Image Processing,* vol. 3 (2000):464–467.

Opderbecke, J. "Depth Image Matching for Underwater Vehicle Navigation." *Image Processing,* vol. 2 (1999):624–629.

SEE ALSO

Mapping Technology

Baton Rounds.

SEE *Less Lethal Weapons Technology.*

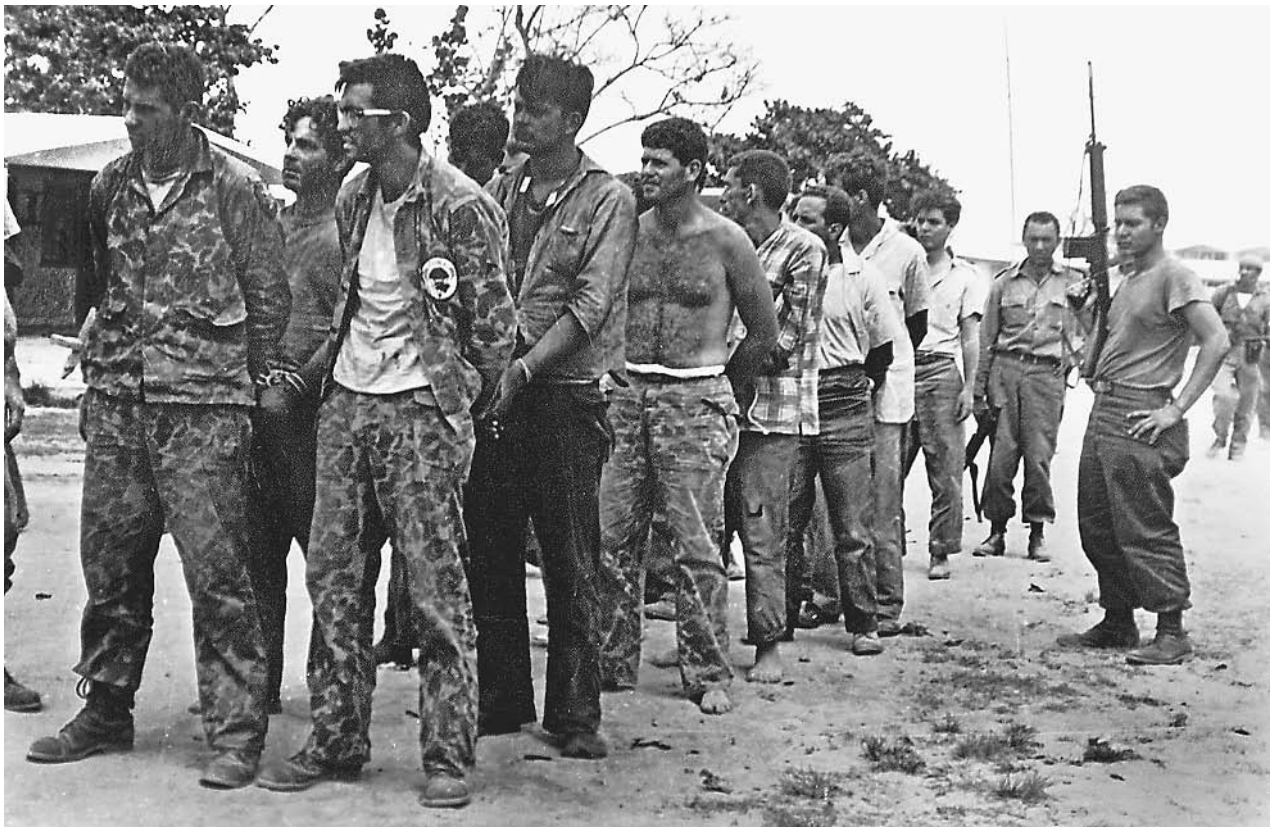
Bay of Pigs

■ LARRY GILMAN

The Bay of Pigs (Bahía de Cochinos) is a small bay on the southern coast of Cuba that was invaded on April 17, 1961 by approximately 1,400 Cuban exiles organized and armed by the United States Central Intelligence Agency (CIA). The invasion was meant to appear to be an attempt by independent Cuban rebels to overthrow leftist Cuban leader Fidel Castro, but became obviously known as an American project, and confirmed when President John F. Kennedy immediately admitted responsibility when the invasion failed. The Bay of Pigs, as the whole episode came to be known, was a major embarrassment for the United States, which was caught deceiving the United Nations and trying to overthrow by force a government which the U.S. itself had officially recognized and which was not attacking the U.S. One hundred and fourteen invaders and 157 Cuban soldiers were killed and 1,189 invaders were taken prisoner.

Fidel Castro became the leader of Cuba's government when his revolutionary forces overthrew the Batista regime in January, 1959. At first, Washington was not hostile to Castro. President Dwight D. Eisenhower recognized his government a few days after Batista's downfall, and Castro even traveled to Washington to meet with Vice President Richard Nixon (later President Nixon). Nixon decided that Castro could not be relied upon to pursue U.S. interests and began to agitate privately for his removal.

In October, 1959, Eisenhower approved a secret program to depose Castro proposed by the CIA and the State Department. Eisenhower told his advisors that "our hand should not show in anything that is done"—in other words, that the operation should be carried out in such a way that



Cuban counter-revolutionaries, members of Assault Brigade 2506, after their capture at the Bay of Pigs, Cuba, in April 1961. ©AFP/CORBIS.

U.S. responsibility could be plausibly denied. To this end, the CIA gathered, funded, armed, and trained an anti-Castro rebel organization in Florida, the Panama Canal Zone, and Guatemala. The CIA began military training of 300 Cuban expatriates in March of 1960, and in May began broadcasting anti-Castro propaganda over the whole Caribbean from a station on a small, disputed territory named Swan Island. The programs were taped in Miami under CIA control, but claimed to be the voice of an authentic Cuban rebel movement without U.S. ties. In September, addressing the General Assembly of the United Nations, Castro accurately accused the U.S. of operating Radio Swan; the U.S. denied the charge.

In July, 1960, the Cuban fighters of "Brigade 2506"—named for the number of a brigade member killed in an accident—were transferred to a training camp in Guatemala built and run by the CIA.

On November 4, 1960, John Kennedy was elected president. Once in office, Kennedy gave his approval for the training of Brigade 2506 to continue. Like Eisenhower before him, however, Kennedy was adamant that U.S. armed forces should not take part in any effort to overthrow Castro. Not only was the whole operation illegal, any hint of U.S. manipulation would alienate potential supporters of the invasion inside Cuba. U.S. planners hoped that when news of the invasion reached the Cuban populace, an anti-Castro rebellion would arise and cast him out. At the very least, planners believed, the invaders could fight their way overland to the Escambray Mountains, about 100 miles west of the landing zone, and join rebel forces already fighting there.

On April 15, 1961, the first part of the invasion plan was carried out. Eight B-29 bombers supplied by the CIA bombed Cuban military aircraft on the ground at several locations. Later, a B-26 bearing Cuban markings and marked with bullet-holes landed at Miami International Airport. The pilots claimed to be defecting Cuban pilots, the goal being to make the raids on Cuba earlier that morning look like an internal action by defecting Cuban pilots. However, reporters on the scene noted that the plane's machine guns had not been fired and that the plane was not of the type actually used by Cuba. Castro, hearing the reports, commented that even Hollywood would not have tried to film such a feeble story. The goal of the bombings themselves was to destroy the Cuban government's small air force at one stroke, eliminating any call for U.S. air support of Brigade 2506 at the landing site. The raid was not completely successful, however.

Two days later, on April 17, a landing was made at Playa Girón (Girón Beach) in the Bay of Pigs. A small beachhead was quickly achieved by Brigade 2506, but one of their freighter vessels, containing food, fuel, medical equipment, and a ten days' supply of ammunition, was quickly sunk. Combat was heavy around the beachhead as

Cuban government forces responded to the attack. The remnants of the Cuban Air Force bombed and strafed the invading forces, as Brigade 2506 had not been supplied with fighter aircraft and President Kennedy categorically refused to allow U.S. fighters to go into combat.

The military situation deteriorated steadily (from the invaders' point of view) over the next 48 hours. On April 18, while the fighting was at its peak, Adlai Stevenson denied to the United Nations, in response to Cuban accusations, that the U.S. was attacking Cuba. Eventually, Kennedy was persuaded to authorize unmarked U.S. fighter jets from the aircraft carrier *Essex* to provide escort cover for the invasion's B-26 bombers, most of which were now being flown by CIA agents in support of the ground invasion (two-thirds of the Brigade pilots were refusing to fly). The jets from the *Essex* missed their rendezvous with the B-26s by an hour due to a misunderstanding about time zones; in the subsequent, unescorted bombing raid over Cuba, two B-26s were shot down and four Americans were killed. The fighting ended on April 20, 1961, with the defeat of Brigade 2506.

The project, most analysts would later conclude, had been hopeless from the beginning. Fidel Castro enjoyed wide support in Cuba and had just consolidated a military victory against the Batista regime; a few thousand lightly-armed invaders could not possibly have taken the island. Furthermore, the idea that the U.S. could keep its role secret had become ridiculous long before the invasion was attempted. The *New York Times* had run a story on March 17, 1961, predicting a U.S. invasion of Cuba in the coming weeks, and another story on April 7, entitled "Anti-Castro Units Trained to Fight at Florida Bases," which noted that invasion plans were in their final stages. Although the *Times* had watered down the latter story considerably at President Kennedy's personal request, when Kennedy saw the paper he exclaimed that Castro didn't need spies; all he had to do was read the news. But Castro, and others, did have spies, and the Soviet Union was fairly well-informed of U.S. invasion plans ahead of time.

The costs of the Bay of Pigs were high, and not only in lives lost. In the wake of the invasion, Castro consolidated his regime, supported by public outrage in Cuba over the U.S.-plotted invasion, and concluded a mutual-defense agreement with the Soviet Union. The Soviet Union exploited this relationship to get Cuban permission to place ballistic-missile launch sites on Cuban soil. These launch sites, detected by U.S. aerial photography, were the immediate cause of the Cuban Missile Crisis of 1962, generally agreed to have been the closest approach to all-out nuclear war that the world has yet ecountered.

■ FURTHER READING:

BOOKS:

Blight, James and Peter Kornbluh. *Politics of Illusion: The Bay of Pigs Invasion Reexamined.* Boulder, CO: Lynne Rienner Publishers, 1998.

Kornbluh, Peter. *Bay of Pigs Declassified: The Secret CIA Report on the Invasion of Cuba.* New York: The New Press, 1998.

SEE ALSO

Cuban Missile Crisis
Kennedy Administration (1961–1963), United States National Security Policy

Belgium, Intelligence and Security Agencies

Officially upholding a declared policy of neutrality, Belgium maintains a small number of defense, intelligence, and military forces. Belgium has three national languages, French, German, and Dutch, all of which are equally recognized for official government use. The nation's central geographic location, varied linguistic structure, and policy of neutrality have aided the growth of Brussels as an international city and financial center. The Belgian capital also serves as the capital of the European Union (EU). With this added international responsibility, the Belgian government restructured many of its intelligence and law enforcement agencies in the early 1990s. National agencies work closely with other EU member nations to provide security in the international capital.

Belgium maintains both military and civilian intelligence forces. The nation's armed forces have various small, strategic intelligence units, but the Permanent Committee for the Control of Intelligence Services coordinates wide-scale military intelligence operations. The central committee, a branch of the Ministry of Defense and the General Intelligence Service, governs various operational divisions responsible for intelligence and security. The committee also coordinates joint operations with military and civilian security services.

The Intelligence Division of the Ministry of Defense manages external intelligence operations. Charged with protecting Belgian national interests at home and abroad, the Intelligence Division cooperates with military intelligence to gather, process, analyze, and act upon information. Mainly focusing on information from and about foreign states, the Intelligence Division maintains a small operational division.

A second operational division in the Belgian intelligence community is the Security Division. Charged with the protection of military security and classified information regarding foreign agreements, the Security Division conducts surveillance of military property and operations. The Security Division also screens government and military officials for various security clearances, granting access to classified materials.

The Security Intelligence Division, the third operational division of Belgian intelligence under the Ministry of Defense, is the nation's primary counterintelligence and counterespionage force. The division protects military operations and Belgian interests by seeking information relating to terrorism, sabotage, and espionage. The Security Intelligence Division sometimes works with other Belgian and European Union intelligence agencies to ensure the safety of EU officials, diplomats, and attaches in the capital and abroad.

Belgium maintains a smaller civilian intelligence force. The Ministry of Justice controls the Federal Intelligence and Security Agency, whose prime mission is the maintenance of state security. In the 1990s, the agency overhauled government information and computer systems to ensure the security of classified material. The agency works closely with law enforcement, and focuses on internal intelligence information.

As terrorist threats against European targets have increased, the Belgian intelligence community has increased efforts to protect EU government interests in Brussels. Belgium also pledged its support to an international anti-terrorism coalition.

SEE ALSO

Counter-Intelligence
European Union

Belly Buster Hand Drill

The "belly buster" hand-crank drill served as an aid to audio surveillance efforts by the United States Central Intelligence Agency (CIA) during the 1950s and 1960s. Designed to drill holes into masonry, the device made it possible to implant audio devices for covert listening.

The field of audio surveillance was already some 90 years old, as evidenced by the enacting of the first state statutes forbidding the interception of telegraphic messages in 1862, when the belly buster hand drill made its debut. It has long since become a museum piece, replaced by more sophisticated electronic drills, yet its genius lay in its sheer simplicity.

The drill, on display in the CIA Museum at agency headquarters in McLean, Virginia, was actually part of a kit that included several bits and accessories, including wire and microphones. The flat, compact kit made it easy to conceal, and once the operator arrived at the site of the intended audio surveillance, it could be assembled rapidly.

Having selected the area of wall to be drilled, the agent held the base of the drill against his stomach, and cranked the handle manually. The difficulty of this operation, and the exertion it placed on the operator's stomach, earned the drill the nickname by which it is known to posterity.

FURTHER READING:

BOOKS:

O'Toole, G. J. A. *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA.* New York: Atlantic Monthly Press, 1991.

Owen, David. *Hidden Secrets.* Buffalo, NY: Firefly Books, 2002.

Pollock, David A. *Methods of Electronic Audio Surveillance.* Springfield, IL: Thomas, 1973.

ELECTRONIC:

"'Belly Buster' Hand-Crank Audio Drill." Central Intelligence Agency. <http://www.cia.gov/cia/information/artifacts/belly.htm> (January 6, 2003).

Berlin Airlift

ADRIENNE WILMOTH LERNER

Following World War II, Germany was partitioned into various zones under the control of Allied nations. Berlin, the nation's key city, was also divided into different occupation areas, despite its location deep into the Soviet sector. Tensions escalated between the Western Allies and the Soviet Union, prompting the Soviets to attempt to take over control of all of Berlin. When France, Britain, and the United States agreed to introduce a new currency into their sectors in West Germany and Berlin, the Soviets declared the new currency void in the eastern partition under their control. Days later, the Soviet government closed supply lines to West Berlin. The United States Air Force and the British Royal Air Force organized a massive effort to deliver needed food, coal, and medical supplies into Berlin to thwart the Soviet blockade. The round-the-clock operation, which became known as the Berlin Airlift, sustained the residents of West Berlin for over a year, and secured the freedom of West Berlin from Soviet control.

The Soviet blockade. Berlin lay more than 100 miles (160 kilometers) inside of the Soviet-controlled eastern sector. The western sectors of the divided city relied on railroads and the Autobahn, the nation's main roadway, for the free transport of goods and supplies into the city. Berlin's eastern sector was controlled by a Soviet installed communist dictatorship, and was already experiencing shortages of essential goods and a fragile economy. West Berlin flourished under the control of the Western Allies,

Berlin children cheer as United States armed forces airlift supplies to West Berlin in 1948 after the Communists sealed off the borders.

who intended to establish a democratic government and market economy, aid Germany in overcoming the legacy of the Nazis, and relinquish control of their sectors. In order to gain full control of Berlin, Soviet and East German forces acted on government decrees to occupy and shutdown essential transport services, effectively laying West Berlin under siege.

On June 15, 1948, the Soviets declared the Autobahn closed, and established roadblocks to prevent Berliners from fleeing the city. Within a week, all traffic between the various sectors of the city was halted. On Jun 21, river barge traffic was outlawed. Two days later, all railroads into and out of West Berlin were closed. Berliners were then at the mercy of the Soviet government to provide food and supplies. On June 24, 1948, the Soviets announced that they would not supply food to residents outside of the Soviet controlled sector. With all other means of transport cut-off, Britain and the United States, with the help of France, organized a massive airlift to feed and supply the sectors of West Berlin under their control.

Military airlift operations. Airlift operations began immediately. On June 26, two days after the Soviet announcement of the blockade, the United States Air Force airlifted the first cargo into Berlin. The American nicknamed the effort, "Operation Vittles," while British pilots dubbed the operation "Plain Fare." In July 1948, the operation was renamed the Combined Airlift Taskforce.

In the first months of the operation, the airlift gained international fame for delivering food and coal to blockaded Berliners. C-54 pilot, Lt. Gail Halverson added bundles of gum and candy to his payload for the crowds of children he noticed near the airfield. Halverson's "candy bombs" gained renown, and soon donations of candy and gum flooded his mailbox. In anticipation of winter, clothing donations were also collected from U.S. citizens and businesses for transport to Berlin. Red Cross medical supplies were shipped in the airlift, and passengers were permitted to travel between West Germany and Berlin on a limited basis.

Airlift operations were conducted daily, often in inclement weather. Squadrons of American C-54s and British Dakotas, Yorks, Sunderland "Flying Boats," and Hastings aircraft delivered tons of goods per day to West Berlin. The sorties flew in tight patterns, landing sometimes as frequently as four planes a minute into one of three Berlin airfields. At the height of the airlift, as preparatory efforts for the winter of 1949 were underway, British forces drafted commercial airliners into service. The maximum effort launched by the Combined Airlift Task Force occurred on April 16, 1949. Known as the "Easter Parade," the airlift delivered 12,940 short tons of cargo, in 1,398 individual sorties, in one day.

Sustained airlift operations required a large-scale military effort not only in the air, but on the ground as well. Since Britain and France were still coping with post-war shortages at home, most supplies were shipped from the United States across the Atlantic in C-82 "Flying Boxcars." Cargo was shipped to American, British, and French bases in West Germany for final transport to Berlin. Once in Berlin, cargo from American C-54s required hand loading and unloading because the modified aircraft could not support palate loads. Sacks of flour, coal, and other goods then were transported to locations established for distribution.

Major General William H. Tunner commanded the operation with the assistance of a deputy officer, RAF Air Commodore, J. F. Merer. Under their direction, the airlift employed increasingly complicated flying maneuvers and sophisticated technology to maximize the amount of cargo delivered to Berlin. The command team was primarily concerned with operational safety, since planes were required to fly at full tonnage, for long flights, in tight flying and landing patterns. Constant revision of safety standards and operational procedures, the instillation of sophisticated ground radar, as well as increased pilot training, aided the success of the Berlin Airlift while minimizing casualties and accidents.

The Soviets made no effort to stop the airlift. Soviet intelligence reported regularly on airlift operations and the condition and moral of West Berlin residents, but Soviet officials believed that the international coalition would fail or eventually abandon their efforts. Also, they were afraid that military intervention to prevent the airlift might result in another war.

On May 12, 1949, the Soviets finally lifted the blockade on Berlin. Train and auto transport was resumed into the city, but were limited at first. West Berliners regained their freedom to travel to West Germany several months later. Airlift operations continued through September of 1949 until supplies regularly reached Berlin via train and truck. In all, the Berlin Airlift delivered 2.4 million tons of

food and supplies in nearly 300,000 missions. Seventy-nine people lost their lives in the international effort to end the Soviet blockade.

Legacy of the Berlin airlift. The Berlin Airlift was the first large-scale, modern humanitarian effort that utilized airplanes as a primary means of delivery. The political effort was the first international humanitarian coalition that used military vehicles, instillations, resources, personnel, and aircraft, instead of relying on civilian aid organizations. Setting the precedent for future aid operations, the success of the Berlin Airlift added a new role to peace and wartime military forces. Modern wartime humanitarian relief operations, as well as nation building policies were forged after World War II.

After the success of airlift operations and the formal end of the Soviet blockade, there was no easing of political tensions between the Soviet Union and the other Allies. The Western Allies united their occupation zones and created a self-sufficient, democratic government in West Germany. The Soviet Union established a communist satellite state. East Germany became the most tightly controlled Soviet satellite nation, aiding Soviet espionage and intelligence operations throughout the Cold War. Berlin remained partitioned between East and West. Soviet and East German troops used increasing force to control the border between East and West Berlin, cutting off the East from Western visitors and influences.

The Berlin Wall was constructed in the early 1960s to permanently partition the city. The wall became a Cold War symbol of the division between East and West, democratic and communist. In 1989, the failing East German government passed a law limitedly opening the border between East and West Berlin. When East German citizens heard of the law, they stormed the Berlin Wall and its guarded gates, demanding their immediate, and full, opening. East Germany, and the Berlin Wall, fell within months. The subsequent reunification of Germany brought the full end to the crisis which began with the Berlin Airlift forty years prior.

FURTHER READING:

BOOKS:

Haydock, Michael D. *City under Siege: The Berlin Blockade and Airlift, 1948–1949*. Washington, D.C.: Brasseys, 2000.

Miller, Roger G. *To Save a City: The Berlin Airlift, 1948–1949.* Seattle,WA: University Press of the Pacific, 2002.

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
Germany, Intelligence and Security
STASI
United Kingdom, Intelligence and Security
United States, Intelligence and Security
World War II

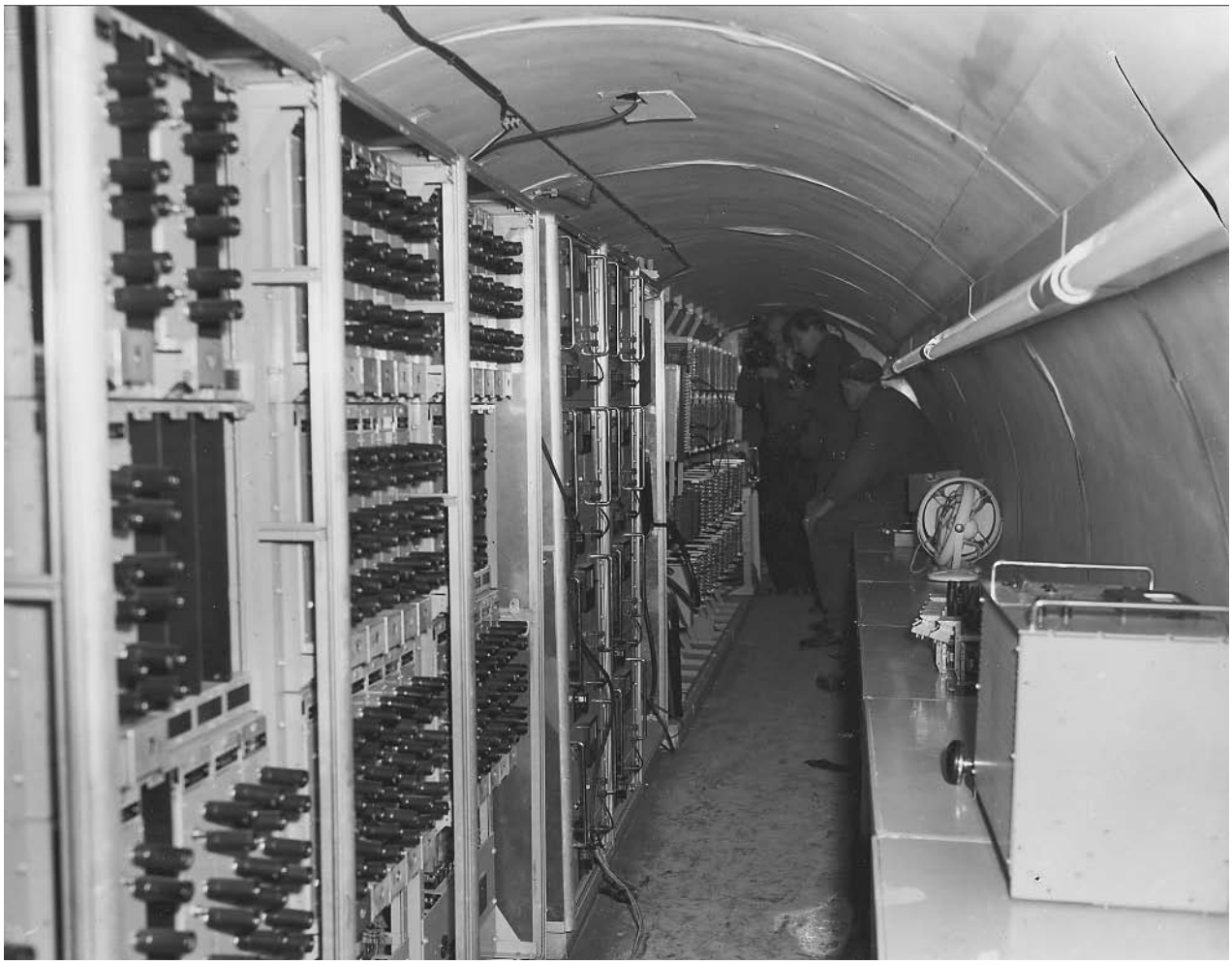
Berlin Tunnel

CARYN E. NEUMANN

The Berlin Tunnel involved an attempt by American and British intelligence to adjust to the late 1940s Soviet shift from wireless transmissions to landlines by tapping Soviet and East German communication cables via a tunnel dug below the communist sector of the German city. The tunnel, which lasted from March 1955 until its discovery by Soviet troops in April 1956, provided difficult-to-obtain military intelligence, as well as information about scientific and political developments behind the Iron Curtain.

The brainchild of the CIA, the Berlin Tunnel aimed to collect Soviet intelligence passed along an underground hub of telecommunications cables adjacent to the U.S. sector of the divided city. While Operation Gold had been conceived in 1951, detailed plans were not in place until August 1953 and the concept did not receive CIA approval until January 1954. The delays centered on the difficulty of discovering exactly which cables were used for Soviet communications and where these cables were located. While the CIA relied upon a number of East German sources to get information, a contact in the long-distance department of an East Berlin post office proved especially useful by providing books that identified cable users. Another contact in the East German Ministry of Post and Telecommunications provided detailed official maps of Soviet cable lines. Tunnel construction then began early in 1954.

The CIA, using the U.S. Army as a front, designed a warehouse that led to a subterranean passageway about 1800 feet long (900 feet into Soviet territory) and 16.5 feet deep. A West Berlin contractor built the warehouse under the misconception that the unusually deep basement and ramps to accommodate forklifts were part of a new and improved quartermaster warehouse design. A detachment of U.S. Army engineers dug the tunnel, but the British army drove the vertical shaft from the end of the tunnel to the target cables and British telecommunications experts made the actual tap. In order to disguise evidence of digging, the army installed washers and dryers on site to clean the fatigues of the construction workers. As a defense against possible Soviet attackers, a heavy torch-proof steel door separated the preamplification chamber, where the signals were isolated for recording, and the vertical shaft of the tap chamber. A microphone in the tap chamber permitted security personnel to monitor any



Soviet authorities find amplifiers and other equipment used to tap Russian telephone lines inside the long tunnel in Berlin, Germany, during the Cold War in 1956. Russian officials discovered the tunnel, and charged that it was dug by the American authorities from their Berlin sector across the border. AP/WIDE WORLD PHOTOS.

activity in the area. Sandbags along the tunnel walls muffled sounds and served as shelves. Construction of the entire tunnel complex ended in March 1955 and the taps began in May.

The KGB soon became aware of Operation Gold through George Blake, a Dutch-born British double agent for the Soviets who entered MI-6 in 1953. Blake, employed in a technical division, gave information about the tunnel to the KGB when the project was still in the planning stages. In order to attack the tunnel, the Soviets would have to compromise Blake and they found it preferable to sacrifice some information rather than their valuable agent. The KGB did not inform anyone in Germany, including the East Germans or the Soviet users of the cable lines, about the taps. When Blake received a transfer in 1955, the Soviets were free to "discover" the tunnel.

Soviet and American accounts of the tunnel discovery do not match, with the Soviets creating a fanciful and widely-circulated account of Soviet technicians surprising Americans as they sipped coffee in the tunnel. In reality, with Blake safely out of the way, Soviet Premier Nikita Khruschchev planned to use the tunnel to score propaganda points but he did not wish to embarrass the British government on the eve of his visit to the island nation. He planned to emphasize the American role in the tunnel while downplaying British involvement. Accordingly, Soviet troops began to dig on the night of April 21, 1956. American personnel, using night vision equipment, detected 40 to 50 Soviet soldiers digging at three to five foot intervals. Given ample warning, the Americans retreated behind the steel door. The Soviets, unable to open the door, dug through an adjacent wall to get into the preamplification chamber. Once inside, they cut the tap cables and the microphone went dead.

Although it came to an embarrassing end, the Berlin Tunnel counts as a successful intelligence operation. The American and British governments used 50,000 reels of tape to capture 443,00 fully transcribed conversations

(368,000 Soviet and 75,000 East German), which in turn led to 1,750 intelligence reports. Besides revealing the latest developments in Soviet atomic research, the tapes indicated disagreements between the Soviets and the East Germans over the status of West Berlin. Despite Soviet claims to the contrary, the tunnel provided much more than carefully planned misinformation.

■ FURTHER READING:

BOOKS:

Miller, Nathan. *Spying for America: The Hidden History of U.S. Intelligence.* New York: Paragon House, 1989.

Murphy, David E., Sergei A. Kondrashev, and George Bailey. *Battleground Berlin: CIA vs. KGB in the Cold War.* New Haven: Yale University Press, 1997.

SEE ALSO

CIA (United States Central Intelligence Agency)
Cold War (1950–1972)
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*
MI6 (British Secret Intelligence Service)

Berlin Wall

■ DAVID TULLOCH

In the early hours of August 13, 1961, the border crossings between the eastern Soviet Occupied Zone of Berlin and the western American, British and French controlled sectors began to be sealed. At first barbed wire was used to separate East from West Berlin, but over time this was replaced by concrete slabs and a deadly no man's land that became known as the Berlin Wall. The Wall split a city, a people, and the world, tearing apart families and friends for decades, and becoming a powerful symbol of the Cold War, representing the deepening divide between East and West, physically, politically, and philosophically.

After the Second World War

Well before the D-Day invasion of mainland Europe, the three main Allied powers, Britain, the United States, and the Soviet Union, held high-level discussions to determine how to administer Germany after it had been defeated. Eventually it was decided that Germany would be split into four administrative zones, one each for the Soviets, the American, the British, and the French. Berlin, as the German capital, was also to be divided into four administrative zones. However, Berlin was located deep within the zone allocated to the Soviets, 180 kilometres (110 miles) from the western zones, and this geographical fact was to haunt post-war Germany for many decades.

Immediately after the war, the major concerns of the administrative powers were feeding the populace, and coping with the severe winter of 1947. The major political discussions were disagreements over the amount of reparations Germany could pay while still leaving it with sufficient resources for recovery. However, the "Berlin Problem," as it came to be known, was also beginning to surface.

Post-war military rule by the four powers was intended to be a short term measure, as it was assumed a suitable German civilian government would be quickly formed, and the Allies would then sign a peace treaty with this new authority and withdraw their troops. As a result, there was little or no long-term planning in regards to the peculiar problems of Berlin. Access routes from the western zones were only tenuously agreed upon with the Soviets. The notion that both Germany and Berlin would remain divided for an extended period was just not considered. When relations between the Soviet Union and the Western powers began to deteriorate, all sides found themselves with a geographical problem that caused political problems.

The Cold War heats up. The first major crisis between East and West regarding post-war Germany began on June 24, 1948, when Western land access to Berlin was blocked by the Soviets. Berlin relied on shipments of almost every good its population used, from food and medicine to coal for heating and power generation. At first it appeared that the Western powers would be forced to either abandon their sectors of Berlin, or open a land passage to Berlin through military confrontation, risking a possible Third World War. Unexpectedly, however, it proved possible to supply Berlin with the bare essentials (and no more) through a massive airlift operation. The New York Treaty of May 4, 1949 effectively ended the Berlin blockade, and the Western counter-blockade, and supplies quickly returned to normal levels.

The blockade effectively ended the charade of four power cooperation in the administration of Germany and Berlin, with the Soviet sector eventually becoming the German Democratic Republic (GDR) and the Western sectors eventually becoming the Federal Republic of Germany (FRG). In both cases, however, Berlin was considered the capital city of these new countries, but a Berlin divided between the Soviets and the West. The events of the blockade were also a fundamental impetus behind the formation of the North Atlantic Treaty Organisation (NATO), and its Eastern counterpart, the Warsaw Pact, further defining the divisions of the Cold War.

Refugees. The 1950s saw both sides of Berlin turned into political and social showrooms for the competing doctrines. West Berlin developed into a capitalist Mecca, while the East of the city transformed into a model socialist city. While the border between the two areas was sealed in 1952, this did not stop half a million people

The Brandenburg Gate was sealed off by the Soviets in the Soviet-occuppied sector of East Berlin in 1961. Located at the center of the German capital, the gate stood at the divide between East and West Berlin until the wall was torn down by German authorities and citizens in 1989. AP/WIDE WORLD PHOTOS.

crossing the borders each day. Many East Berliners worked in the West, where they could make more money and so enjoy a higher standard of living than those working in the East, a situation that led to resentment from some. Berliners from the West enjoyed the extra spending power their currency offered in the East, crossing the border for less expensive haircuts, clothes, and other goods and services. Relatives living on opposite sides of the city could visit each other, students crossed to attend schools and universities, and many people crossed the border to attend concerts and sporting fixtures. There were some measures introduced to make crossing the border difficult and frustrating, such as police controls on many crossing points, and the barricading of some streets, but over 80 access points still remained open, and the underground railway (S-bahn) still crossed regularly.

However, there were a large number of people crossing from the East who simply did not return. Towards the end of the Second World War there had been a flood of refugees fleeing from the East to the West ahead of the advancing Soviet army. While the tide slowed after the end of the war, there remained a steady stream of Germans who left the East of the country and resettled in the West. It is estimated that more that two and a half million East Germans fled into the West between 1946 and 1961, yet the entire population of East Germany was only 17 million. The East German authorities attempted to restrict their citizens crossing by introducing passes and making "fleeing to the Republic" a crime with potential jail sentence of up to four years.

There were many factors driving the refugees. Some were as basic as seeking a better job, more food, or more material goods. The numbers of refugees spiked upwards during times of hardship in the East, when food and other essential resources were scarce. The social and political changes that had taken place in the Soviet zone, such as the educational reforms and the removal of many judges from their positions, resulted in many educated and wealthy persons moving to the West. The refugee problem grew and became an embarrassment for both sides. The East

viewed those leaving as traitors and the West could not cope with the scale of the human tide. In the first seven months of 1961, over 150,000 East Germans left for the West. Walter Ulbricht (1893–1973), the leader of East Germany, repeatedly requested that he be able to take radical measures to stop the problem, but he was denied, at least for the time being.

The Berlin crisis. Aside from the refugee problem, there were political troubles that threatened not only the peace and stability of Berlin and Germany, but also the world. In 1958, the Soviet Leader, Nikita Khruschev (1894–1971) demanded that several thorny post-war issues be resolved within a six-month period. The Soviets wanted negotiations on European security, an end to the four-power occupation of Germany, a final peace treaty signed with a reconstituted Germany, and the creation of a nuclear-free Germany to act as a buffer zone between the two superpowers.

The Soviets threatened that if their demands were not met then they would sign a separate peace treaty with East Germany, officially splitting Germany in two (even if in practice it already was so.) Summit talks were held in Geneva (May-August 1959), Paris (May 1960), and with the newly elected President John F. Kennedy (1917–1963) in Vienna (June 1961), but no agreements were forthcoming.

On the night of August 12, 1961, on the Eastern side of Berlin, large numbers of army units, militiamen, and People's Police (Vopos) began to assemble near the border. Beginning shortly after one in the morning the troops were posted along the border, and the wire and posts were deployed to seal East from West Berlin. Traffic was prevented from crossing, including the underground railway trains. When Berliners awoke on the morning of August 13 their city had been split in two.

The closure of the border between the two halves of Berlin came as a surprise to Western intelligence agencies. After the fact, a number of reports and individuals surfaced claiming to have foreseen the events of August 13, but at the time there was no credible source that was believed by the West. Some historians have suggested there was an overload of information at the time, with too many spies and informers supplying information. Sorting through the sheer volume of reports was one problem, as well as sorting the useful signals from the noise of half-rumor and disinformation. Reports from civilians who noticed that something "big" was occurring before the border was sealed were dismissed, as they were considered less reliable than the professional spies and informers. Credit must also be given to the secret planning and execution of Ulbricht, Erich Honecker (1912–1994), and their forces, who managed to stockpile 40 kilometres of barbed wire and thousands of posts without arousing suspicion. Even as the border was being sealed, many people on both sides had no idea what the ultimate purpose was, including those laying out the barbed wire.

The initial Western lack of response was baffling to many, who expected a more aggressive approach from the Western military in Berlin. The Kennedy administration appeared to accept that the Soviets had a natural right to protect their borders, and the other Western leaders followed his lead. Despite the fact that the East German actions violated the agreements the Four Powers had made after the Second World War, the United States only protested in a feeble manner. While Kennedy has been criticized heavily by biographers and historians for doing nothing, in effect, the lack of an active Western response stabilized the situation. While tension remained high for the next two years, the walling of the Berlin border did not threaten to boil over into armed conflict in the same manner as the Berlin Blockade had done.

If there had been too much intelligence information before the Wall, after the border was sealed there was the opposite problem. Before the Wall, spies crossed as easily as anyone else did. The massive tide of refugees that moved to the West Berlin before the sealing of Berlin caused many intelligence problems, as it was simply not possible to effectively screen all potential communist agents when the numbers crossing were high. After the wall, it became much harder to send spies across the border, simply because there was no longer any civilian traffic. Potential spies were now much easier to spot, and security forces on both sides could now shadow all suspected persons in official parties who crossed the divide.

Over the years, the East Germans modified and added to the initial barbed wire fence between the two Berlins. As soon as it became obvious that the West was not challenging the erection of the barricades, the first concrete sections were moved into place. Within the first few months, the Wall began to take on a more permanent shape, consisting of concrete sections and square blocks. Weak points were quickly identified and sealed. In mid-1962, modifications were made to strengthen the Wall, and in 1965, a third generation of Wall building began, using concrete slabs between steel girders and concrete posts. The last major reconstruction of the Wall began in 1975, when interlocking concrete segments were used.

The border fencing off West Berlin from East Germany was 155 km. (96 mi.) in length. The actual concrete structure that became infamous was only 107 km. (66.5mi.) in length, the remainder of the border was sealed off by wire and fences. More than 300 watch towers were built along the border, as well as 105 km. (65 mi.) of anti-vehicle ditches, more than 20 concrete bunkers, and all patrolled by several hundred dogs and more than ten thousand guards.

While the Wall was a formidable barrier that did not stop many East Germans from trying to cross it. In the first few days and weeks of its construction there were many gaps in the border. Escapees jumped, burrowed, climbed, and swam their way through weak points in the fence. Some East German residents lived in apartments that had windows and doors that opened into the West. Some fled to West Berlin simply by walking through their front doors,

and when they were sealed, by climbing out the windows. Over time the holes and weak points in the Wall were found and blocked. Those attempting to escape in later years faced many more hazards, and while some were successful, many were wounded or killed in the attempt.

The fall of the Wall. The collapse of the Wall was an even greater surprise than its construction, catching the East German politicians and border guards unaware. In 1989, there had been growing unrest in the GDR, with a number of mass demonstrations in East Berlin. A new refugee crisis was also causing problems for the East German authorities. The August, 1989, the opening of the Hungarian border with Austria provided a new gateway to the West. In just three days of September, 1989, over 13,000 East Germans fled to the West via Hungary. The East German authorities rushed through a number of stop-gap measures in an attempt to stem the flow of refugees, including the forced resignation of Honecker on October 18, and giving amnesty to those who had attempted to cross the border illegally. However, the unrest continued, and the refugees still fled.

Then on November 9, 1989, Politburo member Guenter Schabowski gave a television interview in which he announced that East Germans would be able to travel abroad. When a reporter asked when this would apply Schabowski seemed unsure, but then said "immediately." Within minutes, crowds gathered at the border demanding to cross, but the guards refused to let them pass without orders. The East German authorities had intended for the new travel conditions to apply the next day, but in order to avoid violent confrontations, the border was opened. Huge crowds crossed the border, and an impromptu celebration erupted in both sides of Berlin. The Wall had been breached, and would not be closed again.

■ FURTHER READING:

BOOKS:

Hilton, Christopher. *The Wall: The People's Story.* Stroud, Gloucestershire: Sutton Publishing, 2001.

Read, Anthony and David Fisher. *Berlin: The Biography of a City.* London: Pimlico, 1994.

Tusa, Ann. *The Last Division: A History of Berlin 1945–1989.* Reading, MA: Addison-Wesley Publishing, 1997.

ELECTRONIC:

Berlin Wall Online. <http://www.dailysoft.com/berlinwall/> 2003.

Deutsches Historisches Museum Berlin <http://www.wall-berlin.org/>.

SEE ALSO

Berlin Airlift
Berlin Tunnel
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union

Biochemical Assassination Weapons

■ JUDYTH SASSOON

Assassination is usually defined as politically inspired murder. The term is probably derived from the Arabic word for hemp (Hashish), which was apparently used by Hasan-ban-Sabah (c. 1034–1124) to induce motivation in his followers. These "hashishins" or assassins were assigned to carry out political and other murders, usually at the cost of their own lives. Thus, at the etymological level, there is already a connection between assassination and compounds derived from nature.

Biochemicals in the context of assassination involve mostly plant-derived drugs or toxins. They can be organic compounds such as alkaloids, diterpenes, cardiac and cynogenic glycosides, nitro-containing compounds, oxalates, resins, certain proteins and amino acids. A selection of these biochemicals were effectively used in assassination attempts throughout history.

The ancient civilizations of the Near East, Greece and Rome developed the use of poisons in political homicide to a high degree of efficiency. In classical Rome, mushroom poisons were expertly administered by Agrippina (A.D.16– A.D. 59.), wife of Emperor Claudius and mother of Nero. She successfully disposed of several political rivals, including Marcus Silanus who was to succeed Claudius, and eventually Claudius himself. Agrippina probably employed the properties of the amanita species, which contain amanitin polypeptides that produce degenerative changes in the liver, kidney, and cardiac muscles. In ancient Egypt, Queen Cleopatra in her search for a suitable suicide compound became familiar with the properties of henbane (*Hyoscyanus niger*) and belladonna (*Atropa belladonna*), although she judged death by these plants to be rapid, but painful. Cleopatra was also disappointed with *Strychnos nux-vomita* (a tree whose seeds yield strychnine). Strychnine causes stimulation of the central nervous system, produces generalized convulsions, and distorted facial features at death. The latter did not suit Cleopatra, who eventually settled for the bite of an asp (Egyptian cobra), which produced a more serene and prompt death worthy of a queen.

Hemlock is another notorious biochemical used in political murders. The hemlock plant contains coniine, an alkaloid, and was used to execute the Greek philosopher Socrates (c.479 *B.C.*–399 *B.C.*). The drug causes progressive motor paralysis extending upwards from the extremities until death results from respiratory failure. Some of the deadliest political poisons were concocted by the alchemists of the Middle Ages. La Cantrella was a secret assassination weapon used by Cesare Borgia (1476–1507) and Lucrezia Borgia (1480–1519) to despatch their enemies. Even today, its exact composition is not known, but

Senator Frank Church, left, chairman of the Senate Select Intelligence Committee, displays a poison dart gun as co-chairman Senator John Tower watches during the panel's probe of the activities of the Central Intelligence Agency in 1975. AP/WIDE WORLD PHOTOS.

it was most probably a mixture of naturally derived copper, arsenic and crude phosphorus.

In later times, cyanide became more widely used as a homicidal poison. Today, cyanide is usually derived in large quantities from industry, but it has its source in biochemical processes involving cyanogenic glycosides. Amygdalin is one of the most widely distributed glycosides, yielding hydrocyanic acid (HCN) as a product of hydrolysis. It is present in the rosaceae plant family and found in the seeds of apples, cherries, peaches and plums. HCN inhibits the action of the enzyme cytochrome oxidase and prevents the uptake of oxygen by cells. As little as 0.06 g can cause death in humans. Consumption of a lethal dose of HCN is usually followed by collapse and death within seconds. As an assassination weapon, it was famously employed in the killing of the Russian monk Gregory Efimovich Rasputin (c.1872–1916). Legend has it that Rasputin's unnaturally strong constitution allowed him to ingest enough cyanide to kill six men, yet he continued to breathe and eventually received his *coup de grace* from a gun shot.

Ricin is a political poison of twentieth-century origin. It is found in the shell casing of castor beans and is easily produced, thus having the potential to be a large-scale murder weapon. Ricin came to public attention in 1978 when it was used in the assassination of Bulgarian dissenter Georgi Markov in the United Kingdom. Markov worked as a broadcaster for the British Broadcasting Corporation, and relayed pro-Western material to his communist homeland. Markov died several days after being jabbed by an umbrella at a bridge in London. The poison-tipped umbrella injector was designed by the Soviet intelligence agency KGB, whose Bulgarian agent carried the umbrella and delivered the Ricin to the victim. An autopsy revealed that a platinum-iridium pellet the size of a pinhead had been implanted in Markov at the site of his injury. The pellet was cross-drilled with 0.016-inch holes to contain the Ricin. A short time earlier, a similar attempt had been made in Paris against another Bulgarian defector, Vladimir Kostov. This attempt proved unsuccessful because his heavy clothing prevented the steel ball from entering any farther than his subcutaneous tissue. Kostov read of his comrade's death and went for a medical examination during which the pellet was found and removed before any of the toxin could be absorbed. Ricin is an extremely toxic poison. It is estimated that Markov was killed by only a 425 mg. dose contained in the pellet. Ricin is deadly because it can be inhaled, ingested or swallowed and is quickly broken down in the body and is virtually undetectable. Markov's assassination was only detected because the pellet carrying the poison had not dissolved as expected. There is currently no antidote to Ricin although a vaccine has been developed that has been successfully tested in mice.

Apart from the poison pellet umbrella, the KGB is known to have designed several other imaginative devises to deliver biochemical poisons. One was a pen-sized assassination weapon that could deliver gas or liquid poisons. Another was a cigarette case, surrendered by KGB assassin Nikolai Khokhlov upon his defection to West Germany in 1954. The device could fire poison filled hollow-point bullets through the false cigarettes at the opening of the case. Khokhlov, who had been sent to assassinate anti-Soviet émigré Georgi Sergeyevich Okolovich, defected rather than carry out his mission.

In the 1950s and 1960s, a talented chemist and poisons expert worked for the United States Central Intelligence Agency (CIA). He was Sidney Gottlieb (1918–) and also operated under the name Joseph Scheider. In the 1960s, Gottlieb was involved in various chemical and biochemical projects, none of which was apparently successful. Gottlieb created devises that could deliver poisons by which the CIA could carry out assassinations of political leaders who were assumed to be a threat to U.S. national security. One of these leaders was Fidel Castro, whose liking for Havana cigars was considered to be a possible means of administering poison pellets. Gottlieb is thought to have inserted poison into Havana cigars that were sent to Castro, but which were somehow intercepted and never arrived. Gottlieb then tried to create a poisoned wetsuit, which Castro never wore. Another assassination attempt involving Gottlieb was planned by the CIA on General Abdul Karim Kassem of Iraq by planting a poisoned handkerchief in his suit pocket, but this plan also failed. Gottlieb adopted a slightly different tactic in the planned assassination of African leader Patrice Lumumba, the leftwing prime minster of the Congo (now Zaire). In September 1960, he constructed an assassination package that included a biological agent able to induce tularemia (rabbit fever), brucelloisis (undulant fever), anthrax, smallpox, tuberculosis and Venezuelan equine encephalitis (sleeping sickness). This agent was mixed with toothpaste and placed in a tube that could be slipped into Lumumba's traveling kit. Gottlieb delivered this package to Lawrence Devlin, the CIA station chief, instructing him to kill Lumumba. However, the operation also did not achieve its aim, as Lumumba's enemies in the Congo murdered him first in January, 1961.

FURTHER READING:

BOOKS:

Klaassen, C. D. *Toxicology: The Basic Science of Poisons.* McGraw-Hill Companies, 2001.

PERIODICALS:

Benomran, F. A., and J. D. Henry. "Homicide by strychnine poisoning." *Med Sci Law* 36 (1996): 271–3.

Dally, S. [Non-accidental criminal poisonings] *Rev Prat* 50 (2000): 407.

Knight, B. "Ricin—A Potent Homicidal Poison." *Br Med J.* 1 (1979): 350–1.

Vetter, J. "Plant Cyanogenic Glycosides." *ToxiconChem* 38 (2000):11–36.

Zhan, J., and P. Zhou. "A Simplified Method to Evaluate the Acute Toxicity of Ricin and Ricinus Agglutinin." *Toxicology* 186 (2003): 119–23.

SEE ALSO

Anthrax, Terrorist Use as a Biological Weapon
Toxicology
Toxins

Biocontainment Laboratories

BRIAN HOYLE

A biocontainment laboratory is a laboratory that has been designed to lessen or completely prevent the escape of microorganisms.

There are four levels of biocontainment laboratories. Each level must meet certain design criteria, and each is designed for research involving certain microbes. The four levels are designated as Biosafety Level (BSL) 1, 2, 3, and 4.

Types of Biosafety Level Laboratories

The typical university research laboratory is a BSL-1 facility. Such a laboratory has few restrictions on who may enter, connects directly with the remainder of the building, and, other than the wearing of lab coats and observing normal lab hygienic practices, has few specialized safety features. For example, work is done on open-air bench tops without specialized equipment designed to contain the organisms (e.g., fume hood).

The safety features that are in place in a BSL-1 facility are routine. Examples include hand washing before and after work in the lab, decontamination of bench tops before and after use, restrictions on food and drink, and sterilization of all materials that have been in contact with microorganisms. The work space is constructed with sealed seams and a crevasse-free surface, to lessen the chances that microorganisms will pool in a hard-to-reach location and grow.

Personnel in a BSL-1 laboratory are trained in the techniques necessary to prevent contamination of the experiment or themselves. These techniques are not complex and undergraduate students can safely study in a microbiology teaching BSL-1 lab.

BSL-2 Laboratory. A BSL-2 laboratory is similar in design and operation to a BSL-1 lab. However, some additional

A research technician conducts experiments that include challenging insects with a virus mixed with blood at the U.S. Department of Agriculture Arthropod-Borne Animal Diseases Research Laboratory, a biocontainment laboratory that specializes in animal diseases that are transmitted by insects, including plague, West Nile, and tularemia. AP/WIDE WORLD PHOTOS.

safety features are in place to allow microorganisms that are potentially hazardous to health to be studied. For example, lab personnel are trained in the handling of specific disease-causing microorganisms, more care is taken when handling the microbes (i.e., wearing sterile gloves). Access to the BSL-2 lab is restricted and the doors remain closed when experiments are in progress.

Because of the presence of microorganisms that can pose an increased health threat, people who are known to have a less efficiently operating immune system are not allowed inside the laboratory. Even those with normal immune systems are tested regularly for evidence of infection, or can be vaccinated against the microbes they work with.

Procedures like blending and centrifugation create the opportunity for organisms to become airborne. Special protective clothing such as a facemask is worn, and biological safety cabinets are present. The location of the specialized equipment must be approved (i.e., a safety cabinet is not allowed to be by an open window or the door to a hallway).

There are no specific ventilation requirements for a BSL-2 laboratory. Air enters and exits the lab via the building's ventilation system. If windows are present, they can be opened.

BSL-3 Laboratory. This facility is designed for work with microorganisms that can easily become airborne and that carry a great risk of infection. Often a BSL-3 laboratory is in a hospital or an infectious disease research facility.

One distinguishing characteristic of a BSL-3 laboratory, compared to BSL-1 and BSL-2 labs, is the requirement that work with the microorganisms be done within biological safety cabinets or other containment equipment, or by personnel wearing protective clothing (i.e., wrap-around gowns, scrub suits, coveralls, gloves that are changed frequently). Another characteristic is increased restrictions for access to the lab. For example, newer facilities must have double doors, which are sealed around their edges. The first door that connects to the outside of the lab must be fully closed before the door to the BSL-3 lab is opened.

Ventilation systems in the BSL-3 lab are independent from the rest of the building's ventilation system. The air from the laboratory is exhausted directly to the outside and not into the general building circulation. The exhaust air is also filtered to remove microorganisms. Also, ideally the airflow through the laboratory should be balanced (i.e., the air flow into the room is the same as the air flow out of the room) and should flow from areas that are not used for experimental work such as office space to areas containing the microorganisms.

The floors and walls of a BSL-3 laboratory are designed to be free of cracks, impermeable to fluids, and chemical resistant. While windows are permitted, they cannot be opened.

The satisfactory performance of all equipment and personnel in the lab is regularly monitored and recorded for inspection. The lab and the personnel are re-verified each year.

BSL-4 Laboratory. The BSL-4 facility is designed for work with microorganisms that pose a dire health threat. The most infectious microorganisms (i.e., Ebola virus, *Bacillus anthracis* (the cause of anthrax), the Marburg virus, and Hantavirus) can be handled only in a BSL-4 laboratory. A newly discovered microorganism that is genetically related to a known extreme pathogen will also be handled in a BSL-4 lab until, when, and if it is demonstrated that the organism does not pose a threat to health or life.

Two hallmarks of the microorganisms that can be handled only in a BSL-4 laboratory is their ability to be easily transmitted from and to people via the air, and from person to person (they are highly infectious). The design of a BSL-4 laboratory prevents the release of these microorganisms into the environment and protects the researchers from infection.

An example of a BSL-4 laboratory is the one that is present in the United States Army Research Institute of Infectious Diseases, in Fort Detrick, Maryland. At 10,000 square feet, the USAMRIID BSL-4 facility is the largest highest-level biocontainment laboratory in the United States. As of 2002, three other BSL-4 labs exist in North

America. The others are at the Centers for Disease Control and Prevention in Atlanta, Georgia, San Antonio, Texas, and Winnipeg, Manitoba, Canada.

A fourth BSL-4 laboratory is planned for the National Institute of Allergy and Infectious Disease's Rocky Mountain Lab in Hamilton, Montana.

The personnel who work in a BSL-4 laboratory have been highly trained and certified. They are experts in microbiological techniques and in the containment of infections. Only these lab personnel are allowed into the laboratory.

Entry to the Level 4 area requires passage through several checkpoints and the keying in of a security code that is issued only after the person has been successfully vaccinated against the microorganism under study.

All work in the level 4 lab is done in a pressurized and ventilated suit. Air for breathing is passed into the suit through a hose and is filtered so as to be free of microorganisms.

Standard operating procedures are in place for every technique and operation in a BSL-4 laboratory (i.e., changing a filter on a reverse osmosis filtration device), and all work done in the laboratory is documented.

A BSL-4 laboratory is completely isolated from the rest of the rooms in the building. Ideally, the lab is located in a separate building. The laboratory is designed to be a secure facility with respect to the escape of microorganisms. Until now, security against sabotage or deliberate damage has not been a design feature. However, this is changing. The BSL-4 laboratory proposed for Hamilton, Montana, will be in a fenced and guarded space, and will be equipped with observation cameras, multi-levels of secured access, and complete illumination of the exterior of the lab at night.

■ FURTHER READING:

BOOKS:

Richmond, Jonathan Y., and Robert W. McKinney (eds.) *Biosafety in Microbiological and Biomedical Laboratories, 4th edition.*Washington, D.C.: U.S. Government Printing Office,1999.

ELECTRONIC:

National Institute of Allergy and Infectious Diseases. "An Integrated Research Facility at Rocky Mountain Laboratories: Questions and Answers." Office of Communications and Public Liason. November 5, 2002. <http://www.niaiad.nih.gov/dir/infobs14/bs14faq.htm>(06 December 2002).

USAMRIID. "Welcome to USAMRIID." The U.S. Army Medical Research Institute of Infectious Diseases. Fort Detrick, MD. July 25, 2002. <http://www.usamriid.army.mil/>(25 November 2002).

SEE ALSO

Biological Weapons, Genetic Identification
Bioterrorism
Microbiology: Applications to Espionage, Intelligence and Security
Pathogens

Biodetectors

■ JUDYTH SASSOON

Biodetectors are analytical devices that combine the precision and selectivity of biological systems with the processing power of microelectronics. Biodetectors act as powerful analytical tools in medicine, environmental diagnostics, and food industries, as well as forensic analysis and counterterrorism. Biodetectors usually consist of a biological recognition system, typically enzymes or binding proteins immobilized on a surface acting as a physicochemical transducer. One typical example of a biodetector is the immunosensor, which uses antibodies as the biorecognition system. In addition to enzymes and antibodies, the recognition systems can consist of nucleic acids, whole bacteria and single cell organisms and even tissues of higher organisms. Specific interactions between the target molecule or analyte and the complementary biorecognition layer produce a detectable physico-chemical change, which can then be measured by the detector. The detection system can take many forms depending upon the parameters being measured. Electrochemical, optical, mass or thermal changes are the most common parameters providing both qualitative or quantitative data.

The sensitivity of biodetectors allows them to be of considerable use as early detection systems against chemical or biological attacks. They are employed to monitor the environment and can respond to low concentrations of any harmful substances that may be present. Biowarfare agents are frequently colourless and odourless and can sometimes take days to cause symptoms. Early detection of these agents is particularly important as they can trigger symptoms, such as fever or nausea that might be initially mistaken for relatively benign conditions like influenza. Biological agents become weapons of mass destruction when they are disseminated through the air as breathable aerosols. Droplets containing the agents can travel through the air over long distances. A healthy human being breathes on average six litres of air per minute and some of the most lethal pathogens are capable of causing disease if as little as ten organisms are inhaled. To be useful as an early warning device, a biodetector must therefore, have a sensitivity that can detect fewer than about two organisms per litre of air.

The biodetectors now under development for use in counterterrorism fall into three broad categories: biochemical systems detecting a DNA sequence or protein unique to the bioagent through interaction with a test

molecule; tissue-based systems, in which a bioagent or toxic chemical affect living mammalian cells, causing them to undergo some measurable response; and chemical mass spectrometry systems, which break samples down into their chemical components whose weights are then compared to those of known biological or chemical agents.

In recent years, researchers have been sequencing the DNA of a number of potential biowarfare agents in an effort to make them available for DNA based biodetector technologies. A microarray of gel-immobilized, fluorescence-labeled nucleic acids has been developed by Argonne National Laboratory. One application of array systems would be to develop a "bacillus microchip" for detecting *Bacillus anthracis* (the anthrax agent). It would distinguish *B. anthracis* from other related bacteria, such as *B. thuringiensis, B. subtilis,* and *B. cereus* and also indicate whether the organism is alive or dead by detecting DNA when there are no RNA matches.

A number of new, fast, reliable, and portable DNA detection devices have been developed that can prepare and test samples within a very short time. Devices consisting of cell disruptors, capable of breaking bacterial spores and extracting DNA, which is then used to identify the species of organism, are being tried. Some companies have incorporated an automated sample preparation scheme and coupled it with a microfluidic "lab on a chip" device for detecting microorganisms on the basis of their DNA sequence. The system is said to reduce a laboratory preparation procedure that can take six hours to just 30 minutes. The chip contains tiny channels, valves, and chambers through which milliliters of sample can be pumped and concentrated into a microliter volume. Any bacterial cells are broken ultrasonically and their DNA is extracted, amplified by PCR (polymerase chain reaction) and sequenced.

A DNA-based biochip designed by Northwestern University detects DNA sequences that are specific for pathogenic microorganisms. The chip initially contains very short single strands of DNA between two small electrodes. The DNA strands are complementary to DNA sequences from a specific pathogen. When DNA from that pathogen comes into contact with the chip, it hybridizes with the DNA on the chip. To detect the hybridization, further pieces of DNA are added to the system and these are complementary to the sections of pathogen DNA that have not hybridized. The additional DNA pieces contain gold particles that, on successful hybridization, form a bridge of conducting metal linking the two electrodes. The bridge completes an electrical circuit which raises an alarm.

FURTHER READING:

PERIODICALS:

Behnisc, P.A. "Biodetectors in Environmental Chemistry: Are We at a Turning Point?" *Environ Int* 27(2001):441–2.

Casagrande, R. "Technology against Terror." *Scientific American.* 287 (2002):59–65.

"Early Warning Technology." *Med Device Technol* 13 (2002): 70–2.

SEE ALSO

Biological and Toxin Weapons Convention
Biological Warfare
Biological Warfare, Advanced Diagnostics
Biological Weapons, Genetic Identification
Biosensor Technologies
Chemistry: Applications in Espionage, Intelligence, and Security Issues
Forensic Science
Isotopic Analysis
Microbiology: Applications to Espionage, Intelligence and Security
Molecular Biology: Applications to Espionage, Intelligence and Security Issues

Bio-Engineered Tissue Constructs

For several decades, scientists have cultured individual cells and single layers of cells in media outside the body. Information on cell growth, function, and pathology has accumulated from studying these tissue cultures. Very recently, the technology for growing three-dimensional cultures, called tissue engineered constructs (TCE), has evolved. This new technology relies on growing tissues in low gravity fields, in the presence of tissue-specific scaffolding or in highly precise flow or tension environments. The disciplines of biology, physics, and engineering are combined in this new field of tissue engineering (TE). Successful TCE have been used to treat bone disease, replace cartilage and tendons and to repair fascia in hernias. Though there are still many technical problems that must be solved, one of the ultimate goals of TE is to engineer entire organs and to implant them in patients to replace diseased tissues.

Military interest in ETC focuses on using engineered tissue to study and perhaps cure diseases associated with bioterrorism threats. For example, the development of organs that simulate the immune system provide an excellent clinical model on which new vaccines that provide better defense against bioterrorism agents may be tested. Alternatively, artificially engineered lymph nodes or other organs of the immune system could eventually be implanted in humans, inducing a powerful immune response against such biological agents as anthrax, plague, smallpox and other viruses.

In 2002, the Defense Advance Research Projects Agency (DARPA) announced an Engineered Tissue Constructs Program providing funding to research and private institutions to study ETC. The project has two stages. The first is to demonstrate that stem cells can be differentiated into a variety of different types of immune cells within a

three-dimensional tissue construct. Funds for this stage have already been awarded. The second stage is a continuation of the first in which successful tissue engineered constructs are validated for appropriate immune responses.

FURTHER READING:

BOOKS:

Lanza, Robert P., Robert Langer, and Joseph P. Vacanti. *Principles of Tissue Engineering.* Academic Press, 2000.

ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office <http://www.darpa.mil/dso/thrust/biosci/etc.htm.> (March 3, 2003).

Aastrom Biosciences, Inc., 24 Frank Lloyd Wright Drive, Ann Arbor, MI 48105. <http://www.aastrom.com.> (March 3, 2003).

Sciperio, Inc., 5202–2 N. Richmond Hill Road, Stillwater, OK 74075. <http://www.sciperio.com/bio.html> (March 3, 2003).

The Regional Medical Physics Department of the United Kingdom's National Health Service. "Tissue Engineered Synthetic Scaffolds." <http://www.rmpd.org.uk/research/bioengineering/tissue_engineered_synthetic_scaffolds.htm> (March 3, 2003).

SEE ALSO

Biological Warfare
Bioterrorism
Smallpox
Vaccines

Bio-Flips

Bio-flips are specialized microprocessors that can be implanted in the body and that are capable of configuring and calibrating themselves internally via biological feedback (e.g., a response to a set of biological conditions or parameters). Bio-flip type microprocessors can also be used in external biosensors through which bodily fluids or gases are passed.

The advantage of bio-flip technology is that such microprocessors allow accurate, real-time monitoring of specific physiological processes. For example, one class of bio-flip microprocessors are being designed to take small samples of fluids, analyze those samples, digitize the data, and report results to an external monitor. Bio-flip microprocessors that are capable of monitoring bodily process also offer the potential to allow fine control of these processes.

The United States Department of Defense currently funds research into bio-flip technology because of the potential uses in the monitoring of drug and hormone levels that are often critical in treatment of disease and injury. Such dynamic implants would, for example, allow more rapid and precise regulation of medication levels at the site of injured tissues. It is anticipated, however, that the widest potential usage of bio-flip technology will be in the development of new drugs and other pharmacogenetic applications. Bio-flip technology also holds the potential to improve genetic testing.

As of 2002, a wide variety of fixed-assay or passive chips are utilized in biosensor technology. Because these passive chips are not capable of reconfiguration or self-recalibration they are often rendered inaccurate when subjected to biological extremes. For example, passive microprocessors are often incapable of yielding accurate biosensor data because of either a deviation from the normally expected baseline function (e.g., the normal or baseline level of a particular gas in the blood) or in situations where there is an excess of a particular substance (e.g., a chemical present in far greater quantities than normally expected).

Microprocessors that can reconfigure and recalibrate will also enhance the accuracy of microarrays utilized for DNA analysis and of biosensors currently capable of performing chemical analysis via capillary electrophoresis or other microfluidic analysis (examination of small samples of fluids).

The task of analyzing massive amounts of data generated by DNA microarrays is often daunting. Bio-flip technologies along with specialized algorithms and specialized computer programs offer scientists hope of improved abilities to detect variation in genetic structure. Accordingly, improvement in bio-flip like microprocessors should improve genotype analysis and improve identification of more DNA biomarkers (e.g., single nucleotide polymorphisms (SNP)) that can be used in determining genetic relatedness, disease susceptibility risk, and the effectiveness (efficacy) of drug treatments.

Advances in bio-flip microprocessors depend on advances in both microprocessor design and microfabrication technology.

SEE ALSO

Biodetectors
Bio-Engineered Tissue Constructs
Biological and Biomimetic Systems
Biological Input/Output Systems (BIOS)
Biological Warfare, Advanced Diagnostics
Biological Weapons, Genetic Identification
Biomedical Technologies
Bio-Optic Synthetic Systems (BOSS)
Biosensor Technologies
Chemical and Biological Detection Technologies
DNA Fingerprinting
DNA Recognition Instruments
Genomics
Microchip
Nanotechnology
Pathogen Genomic Sequencing
Polymerase Chain Reaction (PCR)
Telemetry
Tissue-Based Biosensors

Biological and Biomimetic Systems

JUDYTH SASSOON

Animals depend on a variety of adaptations and behaviors for reacting to their environment including locomotion, navigation, and the compilation of sensory input into recognizable patterns. The success of these various behaviors is determined by an animal's fitness, which is defined in evolutionary terms as the number of offspring that live to reach reproductive age. Among other effects, these adaptations and behaviors may increase the amount of food an animal forages; increase the number of mates an animal has; or decrease the number of predators an animal encounters. These strategies, which animals have developed through evolutionary pressures, are ideal for incorporation into military systems that navigate, maneuver, sense, analyze, and respond to complex environments.

The Defense Advance Research Projects Agency (DARPA) of the United States government supports a program called Controlled Biological and Biomimetic Systems, whose goal is to incorporate biological evolutionary strategies into new animals or robots that can detect and report the presence of environmental dangers. Some of the applications of the program include developing the capability for mapping the concentration and distribution of toxins within the air, land or water in real time; gathering information on environmental conditions in inaccessible locations or using biological organisms to make the environment more hospitable for troops. The program's aims are entirely defensive. Both private corporations and public laboratories and institutions have been awarded grants within the program.

There are currently three major thrusts of research in the Controlled Biological and Biomimetics Systems program. The goal of the vivisystems program is to exploit live animals, in particular insects, as sentinels for reporting on environmental dangers, including biological weapons. The hybrid biosystems program focuses on developing neural probes that can be used to extract sensory information from animals, in particular insects. The objective of the biomimetics program is to synthesize the biomechanics, neural systems and materials found in organisms for the use in robotic systems.

FURTHER READING:

ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office <http://www.darpa.mil/dso/thrust/biosci/etc.htm.> (March 11, 2003).

Controlled Biological Systems <http://www.darpa.mil/dso/thrust/biosci/cbs/index.html.> (March 11, 2003).

SEE ALSO

Biodetectors
Bio-Engineered Tissue Constructs
Biological Input/Output Systems (BIOS)
Biological Warfare
Biological Warfare, Advanced Diagnostics
Bio-Optic Synthetic Systems (BOSS)
Biosensor Technologies

Biological and Toxin Weapons Convention

K. LEE LERNER

The Biological Weapons Convention (also more properly, but less widely known as the Biological and Toxin Weapons Convention) is an international agreement that prohibits the development and stockpiling of biological weapons. The language of the Biological Weapons Convention (BWC)—drafted in 1972—describes biological weapons as "repugnant to the conscience of mankind."

According to the United States Bureau of Arms Control, as of December, 2003, there were 147 countries that were parties to the Biological Weapons Convention. An additional 16 countires were listed as signatory countries who had signed but not yet ratified the BWC.

The BWC broadly prohibits the development of pathogens—disease causing microorganisms such as viruses and bacteria—and biological toxins that do not have established prophylactic merit (i.e., no ability to serve a protective immunological role), beneficial industrial use, or use in medical treatment.

The United States renounced the first-use of biological weapons and restricted future weapons research programs to issues concerning defensive responses (e.g., immunization, detection, etc.), by executive order in 1969.

Although the BWC disarmament provisions stipulated that biological weapons stockpiles were to have been destroyed by 1975, most Western intelligence agencies openly question whether all stockpiles have been destroyed. Despite the fact that it was a signatory party to the 1972 Biological and Toxin Weapons Convention, the former Soviet Union maintained a well-funded and high-intensity biological weapons program throughout the 1970s and 1980s that worked to produce and stockpile biological weapons including anthrax and smallpox agents. U.S. intelligence agencies openly raise doubt as to whether successive Russian biological weapons programs have been completely dismantled. In June, 2002, traces of biological and chemical weapon agents were found in Uzbekistan on a military base used by U.S. troops fighting

in Afghanistan. Early analysis dates and attributes the source of the contamination to former Soviet Union or successive Russian biological and chemical weapons programs that utilized the base.

Evidence of continued biological weapons development and use in Iraq and Iran—both BWC signatory countries—became widely evident during their war in the 1980s. In the wake of the Gulf War, evidence of Iraqi development of prohibited biological weapons mounted throughout the 1990s. Although some weapons were subsequently destroyed by United Nations mandate, in January 2003 the United States Secretary of State Colin L. Powell presented to the United Nations Security Council alleged evidence of Iraq's continued development of prohibited biological weapons.

As of February, 2003, intelligence estimates compiled from various agencies provide indications that more than two dozen countries are actively involved in the development of biological weapons. The U.S. Office of Technology Assessment and the United States Department of State have identified a list of potential enemy states developing biological weapons. Such potentially hostile nations include Iran, Iraq, Libya, Syria, North Korea, and China.

The BWC prohibits the offensive weaponization of biological agents (e.g., anthrax spores). The BWC also prohibits the transformation of biological agents with established legitimate and sanctioned purposes into agents of a nature and quality that could be used to effectively induce illness or death. In addition to offensive weaponization of microorganisms and/or toxins, prohibited research procedures include the concentrating a strain of bacterium or virus, altering the size of aggregations of potentially harmful biologic agents (e.g., refining anthrax spore sizes to spore sizes small enough to be effectively and widely carried in air currents), producing strains capable of withstanding normally adverse environmental conditions (e.g., disbursement weapons blast), and/or the manipulation of a number of other factors that make biologic agents effective weapons.

Although there have been several international meetings designed to strengthen the implementation and monitoring of BWC provisions, BWC verification procedures are currently the responsibility of an ad hoc commission of scientists. Broad international efforts to coordinate and strengthen enforcement of BWC provisions remains elusive.

FURTHER READING:

BOOKS:

Cole, Leonard A. *The Eleventh Plague: The Politics of Biological and Chemical Warfare.* New York: WH Freeman and Company, 1996.

Dando, Malcolm. *Biological Warfare in the 21st Century.* New York: Macmillan, 1994.

Roberts, Brad. *Biological Weapons: Weapons of the Future?* Washington, D.C.: Center for Strategic and International Studies, 1993.

PERIODICALS:

DaSilva, E., "Biological Warfare, Terrorism, and the Biological Toxin Weapons Convention." *Electronic Journal of Biotechnology.* 3(1999):1–17.

Dire, D. J., and T. W. McGovern. "CBRNE—Biological Warfare Agents." *eMedicine Journal* 4(2002):1–39.

ELECTRONIC:

United States Department of State. "Parties and Signatories of the Biological Weapons Convention" December 11, 2002. <http://www.state.gov/t/ac/bw/fs/2002/8026.htm> (February 25, 2003).

SEE ALSO

Biological Warfare
Biological Warfare, Advanced Diagnostics
Biological Weapons, Genetic Identification
Bioterrorism, Protective Measures
USAMRIID (United States Army Medical Research Institute of Infectious Diseases
Vozrozhdeniye Island, Soviet and Russian Biochemical Facility
World War I

Biological Input/Output Systems (BIOS)

The Biological Input/Output Systems program, also called BIOS, was funded by the Defense Advance Research Projects Agency (DARPA) in 2002. Its goal is to develop and incorporate specific genes into plants, bacteria, yeasts, and prokaryotes that will induce these organisms to act as remote sentinels indicating the presence of biological and chemical substances. These "plug and play" sequences of DNA represent an important step in the development of technology that allow for the assembly of engineered biological pathways within living organisms. For example, an engineered receptor on the exterior of a cell's surface that binds a biological toxin and then signals another pathway within the organism so that it turns different color, activated a fluorescent protein, synthesized a gene product or rearranged a segment of DNA is of particular interest to BIOS. The project aims to produce proof-of-concept examples within three years of initial funding.

An example of a project funded under the BIOS program involves embedding canine olfactory genes that are used in detecting TNT along with the DNA that codes for the pheromone sensing pathway into a yeast's DNA. The potential result is a genetically engineered yeast that can detect explosives. Eventually, these biological sentinels will be grown on sheets that can be deployed in the field.

Another BIOS project focuses on engineering new molecular pathways that result in pigment changes in bacteria upon exposure to a variety of bacterial and viral pathogens. A separate project seeks to engineer biological circuits in the *E. coli* bacterium for sensing biological agents based on the well-known *lac* and *mal* operons as models.

FURTHER READING:

ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office <http://www.darpa.mil/dso/thrust/biosci/etc.htm.> (March 11, 2003).

SEE ALSO

Biodetectors
Bio-Engineered Tissue Constructs
Biological and Biomimetic Systems
Biological Warfare
Biological Warfare, Advanced Diagnostics
Bio-Optic Synthetic Systems (BOSS)
Biosensor Technologies

Biological Warfare

JUDYTH SASSOON

Biological warfare, as defined by the United Nations, is the use of any living organism (e.g. bacterium, virus) or an infective component (e.g., toxin), to cause disease or death in humans, animals, or plants. In contrast to bioterrorism, biological warfare is defined as the "state-sanctioned" use of biological weapons on an opposing military force or civilian population. Biological weapons include pathogenic viruses, bacteria, and biological toxins. Of particular concern are genetically altered microorganisms, which are engineered to target a specific group of people.

Early History of Biological Warfare

Examples of the use of biological weapons exist in ancient records. In the sixth century B.C., Assyrians poisoned enemy wells with ergot, a toxin derived from mold that grows on rye. Other records of battles document the use of diseased corpses to poison wells. In 1346, plague-infected corpses and carcasses were catapulted into Kaffa, a city in current day Crimea, by the Tartar army. The epidemic that resulted may have eventually led to the great Black Plague that afflicted Europe. In 1710, the Russian army used a similar military strategy when it invaded Sweden. The Spanish are reported to have contaminated French wine with blood taken from people suffering from leprosy in the mid-1400s. In the seventeenth century, a Polish general filled artillery shells with the saliva from rabid dogs.

Chemical/biological warfare agent R400 aerial bombs, destroyed by the United Nations weapons inspectors after the 1991 Persian Gulf War, are seen at the Muthanna State Establishment in Iraq in 1998. AP/WIDE WORLD PHOTOS.

Smallpox was used as a biological weapon several times during the colonization of the Americas. The Spanish explorer Pizarro gave blankets infested with the virus to natives in South America in the fifteenth century. Sir Jeffery Amherst presented blankets contaminated with the smallpox virus to native Americans during the French and Indian war between 1754 and 1767. The epidemic that followed resulted in the surrender of a strategic fort to the English. A Southern doctor is reported to have sold clothing contaminated with smallpox to the Union Army during the Civil War.

Modern History of Biological Warfare

During the twentieth century, modern scientific methods led to the development, refinement, and stockpiling of weapons of biological warfare by governments throughout the world. During World War I, Germany developed a

biological warfare program based on the bacterium *Bacillus anthracis* and a strain of *Pseudomonas* known as *Burkholderia mallei*, which causes glanders disease in cattle. Dr. Anton Dilger, a German agent living in Washington D.C., reportedly grew anthrax and glanders bacteria in his home and then inoculated thousands of horses and cattle that were shipped to Allied troops in Europe. Many of the animals perished and hundreds of the troops exposed to these animals were secondarily infected by the diseases.

During World War II, prisoners in German Nazi concentration camps were infected with pathogens, such as Hepatitis A, *Plasmodia* spp., and two types of *Rickettsia* bacteria, during studies allegedly designed to develop vaccines and antibacterial drugs. A large reservoir in Bohemia was poisoned with sewage by the German army in 1945.

Between 1918 and 1945, the Japanese government conducted extensive biological weapon research at Unit 731 in occupied Manchuria, China. Prisoners of war were infected with a variety of pathogens, including *Neisseria meningitis* (meningitis), *Bacillus anthracis* (anthrax), *Shigella* spp. (shigellosis), and *Yersinia pestis* (black plague). Estimates are that over 3,000 prisoners died as a result of infection by these biological pathogens or execution following such infections. In 1941, the Japanese released an estimated 150 million potentially plague-infected fleas from aircraft over cities in China and Manchuria. After these infectious agents were released, outbreaks of plague occurred in many Chinese villages. In addition, approximately 10,000 illnesses and 1,700 deaths occurred among Japanese troops.

Driven by reports of Japanese and German programs to develop biological weapons, the Allies embarked on vigorous efforts to develop their own biological weapons during World War II. Britain produced five million anthrax cakes at the UK Chemical and Biological Defense Establishment at Porton Down with the intent of dropping them on Germany to infect the food chain. These weapons were never used. British open-air testing of anthrax weapons in 1941 on Gruinard Island in Scotland rendered the island inhabitable for five decades.

The United States government's biological warfare facility was headquartered at Fort Detrick in Maryland beginning in 1942. Weapons were also tested and produced in Colorado, Arkansas and Utah. Many different agents were studied including the bacteria that cause anthrax, plague, botulism, Q fever, and staphylococcal infections. Several viruses were also included in the research. The U.S. Army conducted a study in 1951–1952 called "Operation Sea Spray" to study wind currents that might carry biological weapons. As part of the project design, balloons were filled with *Serratia marcescens* (then thought to be harmless, but easily identifiable) and exploded over San Francisco. Shortly thereafter, there was a corresponding dramatic increase in reported pneumonia and urinary tract infections in the region.

The former Soviet Union was implicated in several incidents involving the development and release of biological agents. In 1979, an accidental release of a small amount of anthrax spores occurred at a bioweapons facility near the Soviet city of Sverdlovsk. At least 77 people were sickened and 66 died. All the affected people were some 4 kilometers downwind of the facility. Sheep and cattle up to 50 kilometers downwind became ill. Immediately following the incident, the Soviet government declared that the cause of the illnesses was contaminated meat. However, in 1992 Russian President Boris Yeltsin took responsibility, stating that the accident was the result of military research at the microbiology facility. Between 1975 and 1983, Soviet forces allegedly used "yellow rain" in military operations in Laos, Cambodia and Afghanistan. This substance, T2 toxin or trocothecene mycotoxin, is derived from the *Fusarium* fungi and is extremely damaging to the intestinal tract. The Soviet government has denied the use of T2 toxins, claiming that the yellow rain was the result of defecating bees.

In 1991, the Iraqi government admitted the existence of a biological weapons program within their military. They built bombs containing the botulinum toxin, anthrax and aflatoxins. Iraqi scientists also studied the uses of wheat cover smut, ricin and the toxins produced by *Clostridium perfringens* for biological weapons.

Diplomacy and biological warfare. The first diplomatic effort to limit biological warfare was the Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare. This treaty, ratified in 1925, prohibited the use of biological weapons; however, it was not effective as Germany, the United States, Britain, and the Soviet Union all had biological weapons programs up to the 1960s. More than 140 countries, including the United States, signed the Convention on the Prohibition of the Development Production, and the Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, also called the Biological Weapons Convention (BWC) in 1972, with limited success. Although the United States formally stopped biological weapons research in 1969 (by executive order of then President Richard M. Nixon), the Soviet Union carried on biological weapons research until its demise. Despite being a signator to the BWC, the Iraqi government allegedly continued its buildup of biological weapons into the twenty-first century.

Following the Iraqi war, however, anticipated stockpiles of biological weapons were not immediately found.

■ FURTHER READING:

ELECTRONIC:

Rhode Island Department of Health: Bioterrorism Preparedness Program "History of Biological Warfare and Current Threat" <http://www.healthri.org/environment/biot/history.htm> (March 12, 2003).

Arizona Department of Health Services: Epidemiology and Surveillance "History of Biowarfare and Bioterrorism" <http://www.hs.state.az.us/phs/edc/edrp/es/bthistor2.htm> (March 12, 2003).

SEE ALSO

Anthrax Weaponization
Biological and Toxin Weapons Convention
Bioterrorism
Chemical Warfare
Infectious Disease, Threats to Security
Viral Biology
Weapons of Mass Destruction

Biological Warfare, Advanced Diagnostics

The Advanced Diagnostics Program is funded by the Defense Advanced Research Projects Agency of the United States government (DARPA). Its objective is to develop tools and medicines to detect and treat biological and chemical weapons in the field at concentrations low enough to prevent illness. Challenges to this task include minimizing the labor, equipment, and time for identifying biological and chemical agents.

One area of interest includes development of field tools that can identify many different agents. To accomplish this goal, several groups funded under the advanced diagnostics program have developed field-based biosensors that can detect a variety of analytes including fragments of DNA, various hormones and proteins, bacteria, salts, and antibodies. These biosensors are portable, run on external power sources, and require very little time to complete analyses.

A second focus of the advanced diagnostics project is the identification of known and unknown or bioengineered pathogens and development of early responses to infections. Many viruses act by destroying the ability of cells to replicate properly. One group funded under the advanced diagnostics program is studying the enzyme 5′-monophosphate dehydrogenase (IMPDH), which produces products that are required for synthesizing nucleic acids, such as RNA and DNA, both of which are essential for proper cell replication. This group seeks to develop novel drugs based on IMPDH, which can cross into cells and thwart viral infection.

A final goal is to develop the ability to continuously monitor the body for evidence of infection. Researchers are addressing this goal in two ways. The first involves engineering monitoring mechanisms that are internal to the body. In particular, groups funded under the initiative are developing bioengineered white blood cells to detect infection from within the body. Often genetic responses to infection occur within minutes of infection so analysis of blood cells provides a very quick indication of the presence of a biological threat. The second method involves the development of a wearable, non-invasive diagnostic device that detects a broad-spectrum of biological and chemical agents.

FURTHER READING:

ELECTRONIC:

Advanced Diagnostics (DARPA) <http://www.darpa.mil/dso/thrust/biosci/ADVDIAG/index.html> (March 13, 2003).

Defense Advanced Research Projects Agency, Defense Sciences Office <http://www.darpa.mil/dso/thrust/biosci/advdiagn.htm.> (March 13, 2003).

SEE ALSO

Biodetectors
Biological Warfare
Biomedical Technologies
Biosensor Technologies
Bioterrorism
Bioterrorism, Protective Measures

Biological Weapons, Genetic Identification

Biological weapons are weapons whose payload consists of microorganisms that can cause infections, or the toxic components of the microorganisms. Examples of microorganisms include viruses (e.g., smallpox, Ebola, influenza), bacteria (e.g., *Bacillus anthracis*, *Clostridium botulinum*, *Yersinia pestis*) and protozoa. The most prominent example of a toxic component is the variety of toxins produced and released from bacteria (e.g. neurotoxins produced by *Clostridium*).

Genetic technologies can be useful in the detection of biological weapons. Of particular note is the polymerase chain reaction, or PCR, which uses select enzymes to make copies of genetic material. Within a working day, a target sequence of genetic material can be amplified to numbers that are detectable by laboratory tests such as gel electrophoresis. If the target sequence of nucleotides is unique to the microorganism (e.g., a gene encoding a toxin), then PCR can be used to detect a specific microorganism from among the other organisms present in the sample.

Hand-held PCR detectors that have been used by United Nations inspectors in Iraq during their weapons inspections efforts of 2002–2003 purportedly can detect a single living *Bacillus anthracis* bacterium (the agent of anthrax) in an average kitchen-sized room.

The sequence of components that comprise the genetic material (genome) of a microorganism can also be deduced using techniques such as electrophoresis. Once a sequence is known, it can be compared to the many bacterial, viral, protozoal, and other microbial sequences in databases, in order to determine if the deduced sequence resembles a catalogued sequence. In this way, the nature and identity of biological weapons can be determined.

Genetic engineering has also made possible the splicing of the genetic determinants for a lethal agent from one microorganism or other life form into another microbe. For example, the former Soviet Union experimented with the instillation of the gene responsible for the production of cobra toxin into normally harmless bacteria that reside in the intestinal tract.

While recent events in the United States and in other countries, in particular Iraq, have brought biological weapons into prominence, the military use of biological weapons is centuries old. The bloated bodies of disease victims were routinely dumped into wells to poison the drinking water, or were even catapulted over the walls of fortified cities that were under siege.

More recently, biological warfare was an accepted part of the military campaigns of governments around the world. During World War I, for example, Germany actively explored the weaponization of *Bacillus anthracis* and *Burkholderia mallei*. The latter causes Glanders disease in cattle. Its' use was intended to cripple the agriculture base of the enemy.

During World War II, Britain also intended to cripple German agriculture by airdropping discs (or cakes) of anthrax. Indeed, five million anthrax cakes were ultimately produced, although they were not used. Also during this war, German and Japanese prisoners were used as guinea pigs in the testing of microbial weapons, including hepatitis A, *Plasmodia* species, *Rickettsia*, *Neisseria meningitis*, *Bacillus anthracis*, *Shigella* species, and *Yersinia pestis*. The U.S. had an active biological weapons program during World War II, and extending even into the 1960s. This program was finally terminated in 1968 by the order of then president Richard Nixon.

The production of biological weapons can be accomplished with relatively unsophisticated microbiological technology and by a typically trained microbiologist. Furthermore, the equipment necessary to accomplish weaponization (i.e., incubators, autoclaves, fermenters, centrifuges, refrigerators, and lyophilizers) can be housed in only a few thousand square feet. Thus, biological weapons manufacture is not difficult to conceal.

Furthermore, while biological weapons can be deployed in traditional weaponry (i.e., rockets), the weapons can also be literally carried in someone's pocket to the target site. This can make the deployment of biological weapons virtually impossible to stop, unless the carrier passes near an instrument designed to detect the biological agent.

Microorganisms are very light and so can be dispersed easily in air currents. This is especially true for bacterial spores, which, when dried, are powdery in texture. Furthermore, because exposure to only a few spores can be sufficient to cause disease (e.g., the inhalation form of anthrax, which is caused by spores of *Bacillus anthracis*), the biological weapon can be easily delivered to the target. The anthrax-containing letters that were mailed in the United States in the latter part of 2001 attest to the ease of delivery.

Bacillus anthracis and *Clostridium botulinum* are two prominent examples of spore-forming bacteria that have been used as bioweapons. Spore forming bacteria normally grow and reproduce as "vegetative" cells. But, in harsh environmental conditions that threaten the survival of the bacteria, the microbes have evolved the ability to transform into an almost dormant form known as a spore. The spore is surrounded by a resilient coat that allows it to persist for decades, perhaps even centuries. When conditions again become favorable for growth and reproduction, the spore resuscitates into the vegetative form. Thus, if spore biological weapons do not kill immediately, the residual spores can persist to cause illness many years later.

The microbial agents used as biological weapons are typically highly infectious. The direct exposure of even a small number of people to the weapon can quickly lead to a large number of illnesses or casualties. Bacteria such as *Clostridium botulinum* and various species of *Salmonella* readily cause contamination, either by their growth in food or by the production of potent toxins. Such foodborne microbial threats are also considered to be biological weapons. Indeed, in the aftermath of the U.S. anthrax attacks in 2001, the vulnerability to sabotage of the food production and supply systems in many countries has become evident.

Ironically, the features that make biological weapons attractive to those who wage war or terrorism, namely their ease of dispersal, particularly via air, and their infectivity, has also proved to be a stumbling block to their use. A shift in the prevailing wind can carry the lethal payload back to those who deployed it, similar to the chemical warfare casualties that occurred during World War I. For example, the open air testing of anthrax on Gruinard Island off of the coast of Scotland in 1941 made the island inhabitable for decades afterwards. In a second example, as part of the U.S. Army's "Operation Sea Spray" in 1951–1952, balloons filled with *Serratia marcescens* were exploded over San Francisco, to evaluate the effectiveness of aerial biological warfare on a major urban center. The organism, which up until then was thought to be innocuous, allegedly produced an increase of pneumonias and urinary tract infections in the citizens of the city. As a final example, an accidental release of anthrax spores from a bioweapons facility in 1979 killed 66 people and sickened over 70 who were 4 kilometers downwind, in the city of Sverdlovsk, in the former Soviet Union. Sheep and cattle up to 50 kilometers downwind became ill.

FURTHER READING:

BOOKS:

Cirincione, Joseph, Jon B. Wolfsthal, Miriam Rajkuman, and Jessica T. Mathews. *Deadly Arsenals: Tracking Weapons of Mass Destruction.* Washington, D.C.: Carnegie Endowment for International Peace, 2002.

Hamzah, Khidr Ald Al-Abbis, and Jeff Stein. *Saddam's Bombmaker: The Terrifying Inside Story of the Iraq Nuclear and Biological Weapons Agenda.* New York: Scribner, 2002.

Lavoy, Peter R., Scott D. Sagan, and James J. Wirtz. *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons.* Cornell University Press, 2001.

SEE ALSO

Anthrax Weaponization
Biocontainment Laboratories
DNA
Infectious Disease, Threats to Security
Pathogens

Bio-Magnetics

In 2002, the Defense Advance Research Projects Agency (DARPA) funded an initiative to research the use of magnetic technologies in the detection, manipulation and control of cells, molecules and nanomolecules called BioMagnetics Interfacing Concepts (BioMagnetICs). Living cells and biological molecules are not particularly polar, therefore using magnetic markers as tags represents a highly specific and easily detectable signal for measuring cellular response to environmental conditions, including the presence of biological and chemical toxins. The function of cells and tissues are, to a large extent, managed by the flow of chemical information across membranes via membrane receptor molecules. These membrane receptors are extremely specific, controlling exactly which molecules pass in and out of the cell and at what rate. DARPA's bio-magnetics program seeks to exploit these molecular functionalities by building stable, accurate and sensitive sensors that detect and monitor cellular functions such as protein synthesis, DNA expression, cell death and pigment generation.

The BioMagnetICs program has three major goals. First, it hopes to develop new magnetic tags, or ferrofluids, which have a strong magnetic signal and which can be attached to specific cells and biological molecules. Second, research within the BioMagnetICs program will focus on developing highly sensitive magnetic tags for attachment to fragments of molecules with diameters less than 100 nm within living cells. The final objective of the BioMagnetICs program is to develop magnetic tweezers that can manipulate single molecules and fragments of molecules with precision on the order of nanometers.

One of the expected technologies resulting from the BioMagnetICs program includes bio-detection devices that can detect several different analytes very quickly and with minimal preparation of samples. These magnetic readers have the capacity to provide 10 to1000 times more sensitivity than is possible using current analysis techniques. In addition, these devices are expected to detect toxins with a specificity that is greater than 99%. Because biological and chemical toxins can be dangerous in extremely low concentrations, speed, sensitivity and specificity are extremely important for ensuring the safety of troops in regions where weapons of mass destruction may play an important role.

FURTHER READING:

ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office <http://www.darpa.mil/dso/thrust/biosci/biomagn.htm> (March 20, 2003).

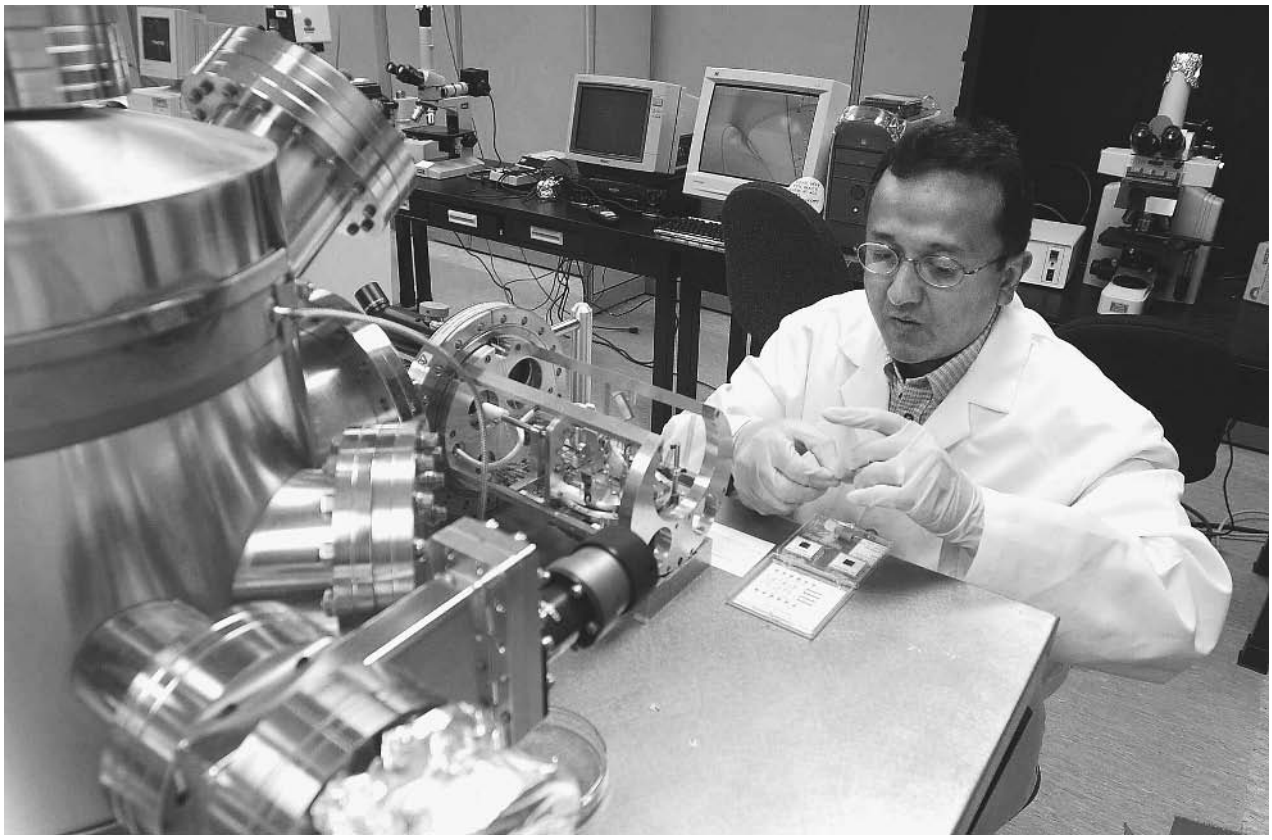
SEE ALSO

Biodetectors
Biological Warfare
Biological Warfare, Advanced Diagnostics
Biosensor Technologies

Biomedical Technologies

In 1993, the Defense Advance Research Projects Agency (DARPA) initiated a program to develop biomedical technologies for use on the front line of the battlefield in 1993. Research had shown that even though medical care has greatly improved during the last three decades, the number of casualties on the battlefield has essentially remained constant. The focus of the Advanced Biomedical Technologies Program (ABMT) was to apply techniques in robotics, virtual reality, three-dimensional visualization, telesurgery, microelectromechanical systems (MEMS), informatics and multi-media simulation to producing products for the care of wounded personnel on the front lines of war. Achievements were made in each of the projects three major research areas: diagnostics, therapeutics, and education and training.

ABMT developed several technologies to improve diagnosis of wounded soldiers on the battlefield, including a Personal Status Monitor (PSM) that continuously monitors vital signs and location and reports this information to medical units. When a soldier is injured, medical personnel can quickly detect his or her location and the seriousness of the wounds. In the near future, troops will wear smart tee shirts, which will have sensors woven into



A Purdue University professor demonstrates an atomic force microscope, used to view biochips, a technology aimed at making diagnostic devices that can be used to quickly analyze samples with high sensitivity. AP/WIDE WORLD PHOTOS.

the fabric that monitor and transmit vital signs and location to medics in real-time. ABMT has also developed hand-held sensors for taking ultrasounds, measuring blood gases and body chemistry, and producing digital pathology reports in the field.

ABMT has also developed new therapeutic technologies for use on the front lines. The Life Support for Trauma and Transport (LSAT) unit is a commercially available stretcher that performs all of the functions of a portable intensive care unit. Medics evacuate wounded soldiers to LSAT units where they can administer IV fluids, intubate and ventilate lungs, and medicate and monitor the soldier until they reach a hospital unit. In addition, ABMT developed several systems for performing telesurgery in remote locations using telemedicine, robotics, and miniaturization.

The final focus of AMBT was to develop novel educational and training tools for troops. Virtual reality (VR) programs simulate battlefield situations and give soldiers first-hand experience for assessing the status of a wounded soldier and deciding on the best way to diagnose, treat, and evacuate the injured individual. Multi-media simulations teach an array of surgical and medical techniques focusing on the procedures that medics are most likely to encounter on the front lines of the battlefield.

FURTHER READING:

ELECTRONIC

Defense Advanced Research Projects Agency, Defense Sciences Office "Advanced Biomedical Technologies" <http://www.darpa.mil/dso/trans/abt.htm> (March 24, 2003).

SEE ALSO

DARPA (Defense Advanced Research Projects Agency)

Biometrics

K. LEE LERNER

Biometrics refers to the measurement of specific physical or behavioral characteristics and the use of that data in identifying subjects. With wide application, biometric-based identification techniques are increasingly an important part of physical and financial security infrastructure because biometric data is difficult, if not impossible, to

duplicate or otherwise falsify. Accordingly, biometric systems offer highly accurate means of comparison of measured characteristics to those in a preassembled database.

Biometric identification points include gross morphological appearance that is most often subjectively interpreted upon superficial examination (e.g., gender, race or color of skin, hair and eye color). Other gross biometric data can include more quantifiable—and therefore less subjective—data (e.g., weight, height, location of scars or other visible physical markings).

Some biometric data are easily changeable and therefore not reliable (e.g. presence of facial hair, wearing of glasses, etc.).

Because even objective features such as weight can change over time, systems of identification that rely on changeable or gross features are not as reliable as biometric systems that measure more stable anatomical and physiological characteristics such as fingerprints, retinal blood vessel patterns, specific skull dimensions; dental and skeletal x-rays, earlobe capillary patterns and hand geometry.

The most specific and reliable of biometric data are obtained from DNA sequencing.

More controversial and, at present, less reliable biometric studies seek to enhance quantification of social behaviors, voice characteristics—including language use patterns and accents—handwriting and even keystroke input patterns.

Biometric data can be encoded into magnetic stripes, bar codes, and integrated circuit "smart" cards.

On a global scale, biometric data interchange and interoperability standards are at present fragmented into different measurement and input format schemes. The Common Biometric Exchange File Format (CBEFF), in development by the International Biometric Industry Association (IBIA), seeks to integrate such measurement schemes to enhance reliability and use of biometric data. Other integration efforts include the Biometric Application Programming Interface (BioAPI) specification program used by the United States Department of Defense. The Department of Defense has also established a Biometrics Management Office (BMO). BioAPI protocols are also being used by other governmental agencies and the financial service industry in the development of smart cards.

In the private sector, specific organizations regulate need-driven biometric integration schemes. For example, the American National Standards Institute (ANSI) establishes specific biometric standards for the financial industry.

One system already with broad integration is used by the American Association for Motor Vehicle Administration (AAMVA). The Driver's License and Identification (DL/ID) standards are used to provide rapid and accurate identification based upon data gathered during the issuance of a driver's license within Canada or the United States.

The National Institute of Standards and Technology (NIST) also has programs dedicated to biometric research and exchange. NIST developed the initial data protocols used in the Face Recognition Vendor Test (FRVT) and established the format for data collection used by most face recognition technologies.

FURTHER READING:

BOOKS:

Jain, A., A. Bolle, and S. Pankanti. *Biometrics, Personal Identification in Networked Society.* Norwell, MA: Kluwer Academic Publishers, 1999.

PERIODICALS:

Podio F., et al. "Common Biometric Exchange File Format (CBEFF)." *NISTIR* 6529 (January 3, 2000).

ELECTRONIC:

NIST Biometric Interoperability, Performance and Assurance Working Group (May, 2003) <http://www.nist.gov/bcwg> (May, 10, 2003).

SEE ALSO

APIS (Advance Passenger Information System)
Closed-Circuit Television (CCTV)
Facility Security
Fingerprint Analysis
Forensic Voice and Tape Analysis
IBIS (Interagency Border Inspection System)
IDENT (Automated Biometric Identification System)
INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)
Los Alamos National Laboratory
NAILS (National Automated Immigration Lookout System)
NIST (United States National Institute of Standards and Technology)
PORTPASS (Port Passenger Accelerated Service System)
Retina and Iris Scans
SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)

Bio-Optic Synthetic Systems (BOSS)

In 2002, the Defense Advanced Research Project Agency (DARPA) initiated a program aimed at simplifying complex optical sensors used in military operations by imitating biological visual systems. The goal of the Bio-Optical Synthetic Systems project (BOSS) is to understand and synthesize the components of biological vision systems.

Much of the current technology used for intelligence gathering depends on optical sensors. These sensors are complicated, relying on multiple sets of lenses for focusing on their targets. Biological vision systems, such as the

eye, are extremely compact, yet allow for a wide field of view, a dynamic range of index of refraction and control over spherical aberration. The crystalline structure of the fish eye lens, for example, accomplishes this flexibility in optical properties via an inhomogeneous protein gradient.

The technical challenges for this project include developing materials with a dynamic index of refraction and a variable field of view lens. In particular, the program specifies that the lens must have a field of view ranging from less than one degree to 120 degrees. The program seeks to develop material to improve the index of refraction, which likely requires the use of an inhomogeneous protein gradient. Materials that self-assemble into such hierarchical structure are of key interest. Both public institutions and private corporations have been funded under this initiative.

FURTHER READING:

ELECTRONIC:

Defense Advanced Research Projects Agency, Defense Sciences Office "Bio-Optic Synthetic Systems (BOSS)" <http://www.darpa.mil/dso/thrust/biosci/boss.htm.> (March 25, 2003).

SEE ALSO

Biodetectors
Bio-Engineered Tissue Constructs
Biological and Biomimetic Systems
Biosensor Technologies
Brain-Machine Interfaces
DARPA (Defense Advanced Research Projects Agency)

Biosensor Technologies

The capability for detecting and identifying multiple biological warfare agents quickly and accurately is required to protect both troops on the battlefields and civilians confronted with terrorist attacks. The systems currently available for sensing biological analytes rely on two technologies: reporter molecules that attach to antibodies and give off fluorescent signals and the Polymerase Chain Reaction (PCR) that amplifies suspect DNA. Because two steps are required to identify biological weapons, the procedure is both labor and time intensive. The Defense Advanced Research Projects Agency (DARPA) initiated the Biosensor Technologies Program in 2002 to develop fast, sensitive, automatic technologies for the detection and identification of biological warfare agents. The program focuses on a variety of technologies including surface receptor properties, nucleic acid sequences, identification of molecules found on the breath, and mass spectrometry.

A major thrust of the surface receptor research is to enhance or replace the signal given off by antibodies to biological analytes. One such project has developed short polypeptides (4–5 amino acids long) that can bind to anthrax spores. A separate group has engineered aptamers, short strands of nucleic acid that specifically bind to the DNA of the bacteria that cause anthrax. Another research area involves using ion channels for amplifying the signal of a reporter molecule. This work includes the engineering of an artificial ion channel that is triggered by the binding of an antibody or other small molecules. Such engineered ion channels are sensitive to a single binding event, require no external energy and can greatly amplify the chemical signal. Finally, upconverting phosphors as a replacement for fluorescent reporter molecules are being investigated.

The focus of the nucleic acid sequence technology is the development of a biochip that contains an array of engineered molecules that react with the genome of biological warfare agents. The biochip is embedded in a platform that is portable, automated and allows for direct sampling of the environment. A biochip platform to identify the anthrax bacteria is in the testing stages and additional biochips for identifying other harmful bacteria and viruses are in development.

FURTHER READING:

ELECTRONIC:

Defense Advanced Research Projects Agency: Defense Sciences Office <http://www.darpa.mil/dso/thrust/biosci/biostech.htm> (March 26, 2003).

Biosensor Technologies <http://www.darpa.mil/dso/thrust/biosci/biosensor/index.html> (March 11, 2003).

SEE ALSO

Anthrax
Biodetectors
Biological Input/Output Systems (BIOS)
Biological Warfare, Advanced Diagnostics
DARPA (Defense Advanced Research Projects Agency)

BioShield Project

JULI BERWALD

Although the medical industry has made great strides in the treatment of many naturally occurring diseases, such as cancer and heart disease, over the last few decades, very little has changed in the treatment of many of the diseases that might be used in an terrorist attack. In

particular, the smallpox vaccine has not changed much since the 1960s and the treatments for exposure to radiation have remained the same since the 1970s. The goal of the BioShield project is to focus biomedical research and development on the field of bioterrorism to improve the treatment of bioterrorism threats.

President George W. Bush announced Project BioShield during his State of the Union Address in January of 2003. As approved by Congress, this project commits $6 billion to improve treatment of diseases caused by biological, chemical and radiological weapons. The project is a joint effort between the Department of Homeland Security and the Department of Health and Human Services.

Under the BioShield Project, resources will be made available to buy the most effective drugs and vaccines available for the treatment of anthrax, smallpox, and botulism and, in the future, ebola and plague. This financial commitment is intended to ensure that the private sector produces the vaccines and drugs required to treat bioterrorist threats. The Secretary of Health and Human Services will identify the most critical threats and will collaborate with industry to develop and make available the most effective countermeasures.

The project gives the National Institute of Health funding to expedite research into the most promising new drug treatments. In particular, procedures to speed up the funding process for grant proposals for research into new drug therapies for chemical, biological and radiological diseases will be authorized. Technical experts will be hired more quickly and equipment required for research will be purchased more rapidly. There is hope that some of the most recent research in the fields of genetics, immunology, molecular engineering and proteomics will be useful in developing novel treatments for the diseases caused by bioterrorism. In addition, some of the innovations developed under Project BioShield may become important in the treatment of naturally occurring diseases.

The BioShield project provides the Food and Drug Administration with the authority to make promising drugs widely available in emergency situations.

■ FURTHER READING:

ELECTRONIC:

Defense Advanced Research Projects Agency: Defense Sciences Office <http://www.darpa.mil/dso/thrust/biosci/biostech.htm> (March 26, 2003).

The White House, News & Policies. President Details Project BioShield. February 3, 2003. <http://www.whitehouse.gov/news/releases/2003/02/20030203.html> (April, 3 2003).

SEE ALSO

Anthrax
Biological Warfare
Biological Warfare, Advanced Diagnostics

Bioterrorism

■ BRIAN HOYLE

Bioterrorism is the use of a biological weapon against a civilian or military population by a government, organization, or individual. As with any form of terrorism, its purposes include the undermining of morale, creating chaos, or achieving political goals. Biological weapons use microorganisms and toxins to produce disease and death in humans, livestock, and crops.

Bioterrorism is viewed as a serious threat to national security. For example, disaster scenarios created by United States government agencies predict that the release of a few hundred pounds of the spores of *Bacillus anthracis* (the bacterium that cause the disease called anthrax) upwind of Washington, D.C., could sicken or kill hundreds of thousands to millions of people within twenty-four hours.

Bioterrorism can also be used as a weapon to damage or destroy the economy of the target nation. A report from the Centers for Disease Control and Prevention estimates the costs of dealing with a large-scale anthrax incident is at least $26 billion per 100,000 people. Only a few such incidents could cripple the economy of any nation. Indeed, the few anthrax incidents in the last few months of 2001 cost the United States government hundreds of millions of dollars in treatment, investigation, and other response measures.

Biological, chemical, and nuclear weapons can all be used to achieve similar destructive goals (i.e., massive loss of life). In comparison, biological weapons are inexpensive to make, relative to chemical and nuclear weapons. A sophisticated biological production facility can be set up in a warehouse, or even in a building as small as a house. Biological weapons are relatively easy to transport and resist detection by standard security systems.

In general, chemical weapons act immediately, causing illness in minutes. For example, the release of sarin gas in the Tokyo subway in 1995 by the religious sect Aum Shinrikyo almost immediately killed 12 and hospitalized 5,000 people. In contrast, the illness and death from biological weapons can occur more slowly, with evidence of exposure and illness appearing over time. Thus, a bioterrorist attack may at first be indistinguishable from a natural outbreak of an infectious disease. By the time the deliberate nature of the attack is realized, the health care system may be unable to cope with the large number of victims.

The deliberate production and stockpiling of biological weapons is prohibited by the 1972 Biological Weapons Convention. The United States ceased offensive production of biological weapons in 1969, on orders from then President Richard Nixon. The U.S. stockpiles were destroyed in 1971–1972. This measure has not stopped

University of Nebraska researchers explain laboratory automation equipment available to analyze bioterrorism agents to the Secretary of the Department of Homeland Security, Tom Ridge, second from right. AP/WIDE WORLD PHOTOS.

bioterrorists from acquiring the materials and expertize needed to produce biological weapons.

Genetic engineering can produce a wide variety of bioweapons including bacteria or viruses that produce toxins. More conventional laboratory technologies can also produce bacteria that are resistant to antibiotics.

Examples of the most likely to be used bioterrorist weapons include smallpox (caused by the Variola virus), anthrax (caused by *Bacillus anthracis*), and plague (caused by *Yersinia pestis*).

The last recorded case of smallpox was in Somalia in 1977. As of 2002, only two facilities—one in the United States and one in Russia—are authorized to store the virus. In spite of international prohibitions, security experts suspect that smallpox viruses may be under development as biological weapons in other laboratories of many nations. As recently as 1992, Russia had the ability to launch missiles containing weapons-grade smallpox. A number of terrorist organizations including Al Qaeda have explored the use of biological weapons.

Bioterrorism may ultimately prove to be more destructive than conventional warfare, because of the mobility of the weapons and their ability to spread infection through an entire population. An epidemic can spread a disease far from the point of origin of the illness.

Preparing a strategy to defend against biological warfare is challenging. Traditional identification of microorganisms such as bacteria and viruses relies on assays that detect growth of the microbes. Newer technologies detect microbes based on sequences of genetic material. The genetic technologies can detect microbes in minutes. As of 2002, however, the genetic technologies are not available to any but the most sophisticated field investigative units.

Researchers are also working to counter bioterrorist attacks using several other new technological strategies. For example, robots equipped with sensors or microchip-mechanized insects (with computerized circuitry that can mimic biological processes such as neural networks) are being developed. Bees, beetles, and other insects outfitted with sensors are used to collect real-time information about the presence of toxins or similar threats. These new technologies could be used to examine a suspected biological weapon and spare exposing investigators to potential hazards. The robotics program of the Defense Advanced Research Project (DARPA) works to rapidly identify bio-responses to pathogens, and for designs to effectively and rapidly treat them.

Research is also underway to find genetic similarities between the microbes that could be used by bioterrorists. A vaccine made of a protein that is common to several bacteria could potentially offer protection to the exposure any bacterium in the group, for example.

FURTHER READING:

BOOKS:

Frist, W.H. *When Every Moment Counts: What You Need to Know about Bioterrorism from the Senates only Doctor.* Lanham, MD: Rowman & Littlefield,2002.

Henderson, D. A., and T. V. Inglesby. *Bioterrorism: Guidelines for Medical and Public Health Management.* Chicago: American Medical Association, 2002.

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague," in *Emerging Infections 5* Washington, D.C.: American Society for Microbiology Press, 2001.

PERIODICALS:

Kaufmann, A.F., M.I. Meltzer, and G.P. Schmid. "The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Program Justifiable?" *Emerging Infectious Diseases* no. 3 (1997): 83–94.

SEE ALSO

Anthrax, Terrorist Use as a Biological Weapon
Anthrax Vaccine
Anthrax Weaponization
Antibiotics
Biocontainment Laboratories
Biological Warfare
Biological Warfare, Advanced Diagnostics
Biological and Toxin Weapons Convention
Biological weapons, Genetic Identification
Bioterrorism, Protective Measures
Chemical and Biological Defense Information Analysis Center (CBIAC)
Chemical and Biological Detection Technologies
Chemical and Biological Incident Response Force, United States
DARPA (Defense Advanced Research Projects Agency)
DNA Recognition Instruments
DNA Sequences, Unique
Mail Sanitization
Pathogen Genomic Sequencing
Pathogen Transmission
Pathogens
Polymerase Chain Reaction (PCR)
Salmonella and Salmonella Food Poisoning
Smallpox Vaccine
Spores
Weapons of Mass Destruction
Weapons of Mass Destruction, Detection
World War I

Bioterrorism, Protective Measures

K. LEE LERNER

Bioterrorism is the deliberate use of microorganisms or the poisonous compounds that can be produced by some microbes as weapons. Bioterrorism can be a well-organized government sanctioned weapons development program, or can involve a small group of people dedicated to their particular cause.

In the past, the weapons employed by nations were more easily recognizable and defendable. For example, surveillance allows missile silos to be detected, and counter-strategies put in place to deal with the launch of the missiles. Microorganisms, however, by virtue of their small size can be readily hidden from detection. A vial of anthrax spores—small enough to conceal in a pocket—can be released into the ventilation system of a building.

The ability to protect against the use of biological weapons is becoming recognized as one of the paramount security issues facing nations such as the United States.

The need for protective measures against bioterrorism was dramatically evident in the aftermath of the September 11, 2001 terrorist attacks on the United States, when a lethal form of the anthrax bacterium that could be inhaled was mailed to U.S. government leaders, media representatives, and citizens. The form that readiness and response strategies should take is the subject of much public debate.

A range of protective options exist. These include the mass production and stockpiling of antibiotics (i.e., ciprofloxacin, which is normally effective against the bacterial agent of anthrax) and the resumption of offensive biological weapons programs by countries such as the United States (where offensive research was halted in 1968). However, no single solution will provide protection against the many potential biological weapons. Indeed, an argument has been made that a targeted response (e.g., broadly inoculating the public against the virus causing smallpox) might actually lower overall preparedness by diverting personnel and funding from fundamental research programs that could help spawn a variety of protective measures.

The various protective measures to bioterrorism can be divided into three general categories. These are strategic, tactical, and personal measures.

Strategic deterrence can involve international cooperation. For example, late in 2001, the United States and NATO (North Atlantic Treaty Organization) allies reaffirmed treaty commitments that the use weapons of mass destruction (i.e., biological, chemical, or nuclear weapons) against any member state would represent an attack against all NATO members. As of June 2002, this deterrence was pointed at states—in particular Iraq—that have

programs to develop or use biological weapons, or which provide aid to bioterrorists.

Tactical measures involve the use of devices or weapons to detect or eliminate potential biological weapons. The United States has a variety of tactical non-nuclear options, which include precision-guided conventional thermal fuel-air bombs. In the 1990s military campaigns in the Gulf region, for example, these bombs were used to destroy facilities that were suspected of being factories for the production of biological warfare agents and weaponry.

Terrorist operations are enigmatic and elusive. As a result, these large-scale military responses offer protection against only the largest, identifiable, and targetable enemies. Such responses are inadequate when the hostility is due a small number of people operating in a clandestine way in other countries, or even citizens targeting their own country. For example, according to expert testimony before the Congress, for less than 10,000 U.S. dollars, a laboratory capable of producing spores of the anthrax bacterium could be built in the basement of a typical house. Surveillance of every structure in a country is beyond the scope of established security agencies and, in a democratic country, would severely curtail individual liberties.

Reestablishing offensive weapons programs is a contentious issue. An argument has been made that an offensive program would further the understanding of potential biological agents and weapons delivery mechanisms. However, many scientists and physicians argue instead that an offensive program is unneeded and could possibly be detrimental to the development of effective protective measures, because of the diversion of funding from less visible but vital preventative research. Resumption of an offensive bioweapons programs in the United States would violate the Biological Weapons Convention to which the United States is a signatory.

Rather than a polarized offensive-versus-preventative national policy, scientific bodies in the United States that include the National Institutes of Health and the Centers for Disease Control and Prevention (CDC) advocate a balanced and flexible scientific and medical response to the need to develop protective measures against the variety of disease causing pathogens in the arsenal of the bioterrorist.

Preparedness programs designed to allow a rapid response to bioterrorism also accompany the increased research. One example is the National Pharmaceutical Stockpile Program (NPS). The NPS stockpile of antibiotics, vaccines, and other medical treatment countermeasures is can be rapidly deployed to the site of a domestic attack. For example, in the aftermath of the deliberate release of *Bacillus anthracis* (the bacteria that causes anthrax) during the 2001 terrorist attacks, the United States government and some state agencies were able to quickly provide the antibiotic ciprofloxacin (Cipro) to those potentially exposed to the bacterium.

Following these bioterrorist attacks, increase funding for the NPS was authorized. The additional funds will help train medical personnel in the early identification and treatment of disease caused by the most likely pathogens.

Such steps are commendable, but will not provide comprehensive and effective protection to biological terrorism. Indeed, such protection may not be possible.

Advocates of increased research capabilities argue that laboratory and hospital facilities must be increased and modernized to provide maximum scientific flexibility in the identification and response to biogenic threats. The CDC has already established a bioterrorism response program that includes increased testing and treatment capacity. The plan also envisions an enhanced ability to recognize and respond to the illness patterns that are characteristic of the deliberate release of an infectious agent.

An informed and watchful public is a key element in early detection of biological pathogens. Knowing this, the CDC web site contains a list of potential biological threats. As of July 2002, approximately 36 microbes had been identified (e.g., Ebola virus variants, plague bacterium, etc.) as potential bioterrorist weapons.

Other protective and emergency response measures include the development of the CDC Rapid Response and Advanced Technology laboratory, a Health Alert Network (HAN), National Electronic Data Surveillance System (NEDSS), and Epidemic Information Exchange (Epi-X). These responses are designed to coordinate information exchange to enhance the early detection and identification of biological weapons.

The United States Department of Health and Human Services 1999 Bioterrorism Initiative committed funds to initiate or reinforce some of these protective measures. Following the September 11, 2001 terrorist attacks on the United States, the U.S. Congress more than doubled the previous funding for bioterrorism research. Soon thereafter, the Bioterrorism Preparedness and Response Program (BPRP) was created. The BPRP seeks to increase the number and capacity of laboratories that are capable of identifying pathogens and developing countermeasures to their use.

An essential component of a preventative response including effective therapeutic treatments is basic research into the biology and disease mechanisms of the disease causing microorganisms. In response to terrorist attacks, in February 2002, the U.S. National Institute of Allergy and Infectious Diseases (NIAID) undertook a review of current research efforts. The panel of experts convened for this task hopes to recommend research thrusts that will more effectively anticipate and counter potential terrorist threats. An immediate outcome of the panel's deliberations was an increased emphasis on basic research involving smallpox, anthrax, botulism, plague, tularemia, and viral hemorrhagic fevers.

In addition to medical protective measures, a terrorist biological weapon attack targeted at humans would, at a

minimum, overburden medical infrastructure. Medical personnel and supplies would be in short supply. As well, the costs of responding to attacks would cause economic havoc. Alternatively, a biological weapon that spared humans but targeted domestic animals or crops could cause famine and economic ruin.

On a local level, cities and communities are being encouraged to develop specific response procedures in the event of bioterrorism. Most hospitals are now required to have response plans in place as part of their accreditation requirements.

Another aspect of prevention focuses on the drinking water supply of communities. Many microorganisms or their poisons readily dissolve in water, and so can be spread to a population virtually undetected. As well, water supplies and distribution systems have bee designed for efficiency of water disinfection and deliver, not for security. Because of this, many communities have placed extra security on water supply and treatment facilities. The U.S. Environmental Protection Agency (EPA) has increased monitoring and working with local water suppliers to develop emergency response plans.

It is beyond the scope of this article to discuss specific personal protective measures. Indeed, given the complexities and ever-changing threat, it would not be prudent to offer such specific medical advice. However, a number of general issues and measures can be discussed. For example, military surplus gas masks provide only the illusion of protection. They offer no real protection against biological agents, and should not be bought for that purpose. Personnel stockpiling of antibiotics is unwise. The potency of antibiotics such as Cipro declines with time. Moreover, the inappropriate use of antibiotics actually can lead to the development of bacterial resistance and a consequential lowering of antibiotic effectiveness.

On the other hand, a few days supply of food and water and the identification of rooms in homes and offices that can be temporarily sealed with duct tape to reduce outside air infiltration is a wise precaution.

More specific response plans and protective measure are often based upon existing assessments of the danger posed by specific diseases and the organisms that produce the disease. For example, Anthrax (*Bacillus anthracis*), Botulism (*Clostridium botulinum* toxin), Plague (*Yersinia pestis*, Smallpox (*Variola major*, Tularemia (*Francisella tularensis*, viral hemorrhagic fevers (e.g., Ebola, Marburg), and arenaviruses (e.g., Lassa) are considered high-risk high-priority. These agents do share a common trait of being easily spread from person to person. And, they all can kill many of those who are infected. But, the natures of the diseases they cause are very different. A response that is effective against one microorganism may well be useless against another.

The protective measures that are in place against smallpox and anthrax remain controversial. Vaccines against both diseases are available. However, both vaccines carry the risk of serious side effects. In the absence of a confirmed case of smallpox, the CDC's position is that the risks of resuming general smallpox vaccination outweigh the potential benefits. Vaccine is available for use in a bioterrorist emergency, when the benefits of mass vaccination could well outweigh the risks of harm due to the vaccine. Moreover, vaccines delivered and injected during the incubation period for smallpox (approximately 12 days) convey at least some protection from the ravages of the disease.

Also controversial remains the safety and effectiveness of an anthrax vaccine used primarily by military personnel.

BOOKS:

Henderson, D.A., and T.V. Inglesby. *Bioterrorism: Guidelines for Medical and Public Health Management*.Chicago: American Medical Association, 2002.

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague." *Emerging Infections 5* Washington, D.C.: American Society for Microbiology Press, 2001.

ELECTRONIC:

World Health Organization. "Strengthening Global Preparedness for Defense against Infectious Disease Threats." Statement to the United States Senate Committee on Foreign Relations Hearing on The Threat of Bioterrorism and the Spread of Infectious Diseases. 5 September 2001. <http://www.who.int/emc/pdfs/Senate_hearing.pdf> (24 November 2002).

SEE ALSO

Anthrax, Terrorist Use as a Biological Weapon
Biological Warfare
USAMRIID (United States Army Medical Research Institute of Infectious Diseases
Vaccines

Black Boxes.

SEE *Flight Data Recorders.*

Black Chamber

▮ DAVID TULLOCH

The term "black chamber" has come to represent any code-breaking organization, but was originally applied to groups of code-breakers associated with the French postal service that intercepted, read, copied and decoded diplomatic mail. In the twentieth century, Americans created a black chamber to intercept and decode radio transmissions (telegraphs) rather than postal mail.

In the seventeenth century, talented individuals such as Antoine Rossignol (1600–1682) in France, and John Wallis (1616–1703) in England showed the value of code breakers in affairs of state. Their efforts encouraged European governments in the eighteenth century to recruit further generations of cryptologists, and create formal cryptology organizations that took their collective title from the French *cabinet noir/* ("black chamber"). Usually located within post office buildings, the members of the black chamber would carefully open the sealed mail, make copies of suspect passages, and close the letters with forged wax seals. Then the laborious task of deciphering coded communications would begin.

Most of Europe's black chambers were closed in the mid-nineteenth century by a combination of public opinion and new social philosophies. The reading of other people's mail was seen as an infringement of personal freedom. In England public pressure forced the government to cease its opening of diplomatic mail in 1844. Four years later, the black chambers of Austria and France also ended their work.

America did not have a black chamber until the early twentieth century, and it was concerned with radio transmissions (telegraphs) rather than postal mail. Its fame is mainly due to Herbert Osborne Yardley (1889–1958), who described the inner workings of the covert organization in his book, *The American Black Chamber*. Yardley wrote his controversial text after the closing of the code-breaking organization in 1929. The Hoover government wanted to promote trust in international relations, and as Secretary of State Henry Stimson noted, "Gentlemen do not read each other's mail." However, by 1940, the black chamber had to be reformed (without Yardley) to counter the threat of war. Today black chambers have become electronic monitoring systems, which many governments use to monitor suspicious communications across the world.

FURTHER READING:

BOOKS:

Kahn, David, *The Codebreakers: The Story of Secret Writing.* New York, NY: The Macmillan Company, 1967.

Yardley, Herbert O. *The American Black Chamber.* Indianapolis: Bobbs-Merrill, 1931.

———. *The Chinese Black Chamber,* Boston: Houghton Mifflin, 1983.

SEE ALSO

Codes and ciphers
Cryptology, History
Decryption

Black List.

SEE *McCarthyism.*

Black Ops

"Black ops" is shorthand for "black operations," covert or clandestine activities that cannot be linked to the organization that undertakes them. The term is a highly problematic one, for a number of reasons. First, by definition, many activities conducted by organizations such as the United States Central Intelligence Agency (CIA) are never intended to be linked to the agency itself. Second, a known example of a successful black operation would be a contradiction in terms.

Third, and perhaps most important, is the fact that the term "black ops" itself is much more likely to be used by novices than by members of the intelligence community. A member of the CIA or any such agency would not likely use such a term in describing a true black operation for obvious reasons; agents would be much more likely to disguise the nature of their undertaking with innocuous language. On the other hand, the intriguing sound of the phrase "black ops" makes it highly appealing to conspiracy-theory buffs and others whose interest is more in fantasy than in the often mundane reality of intelligence work. A search of the term "black ops" on the Internet is likely to turn up material from the organizational fringes (some of it tongue-in-cheek), rather than any serious investigation of clandestine activities.

FURTHER READING:

BOOKS:

Kahaner, Larry. *Competitive Intelligence: From Black Ops to Boardrooms: How Businesses Gather, Analyze, and Use Information to Succeed in the Global Marketplace.* New York: Simon & Schuster, 1996.

Nutter, John Jacob. *The CIA's Black Ops: Covert Action, Foreign Policy, and Democracy.* Amherst, NY: Prometheus Books, 2000.

SEE ALSO

Covert Operations

Black Tom Explosion

ADRIENNE WILMOTH LERNER

The Black Tom explosion was the peak act of German sabotage on American soil during the First World War. On July 29, 1916, German agents set fire to a complex of warehouses and ships in the New York harbor that held munitions, fuel, and explosives bound to aid the Allies in

Smoke billowing from the Black Tom explosion, a German sabotage operation on American soil in 1916. ©BETTMANN/CORBIS.

their fight. Though America was technically a neutral nation at the time of the attack, general policies greatly favored the Allies. The attack persuaded many that the United States should join the Allies and intervene in the war in Europe.

German intelligence and sabotage operations. As soon as war broke out in Europe, the United States began manufacturing munitions and sharing the weapons with allied British, French, and Russian forces in Europe. German agents in the United States reported the stockpiling and shipping of weapons, and the German government took action. Because they could only openly attack United States property in limited ways such as the sinking of merchant ships carrying contraband munitions without provoking America to wage war, the German government sent undercover agents to sabotage munitions operations. Numerous fires were set at military supply manufacturing sites. Shipping lines and railroads were also sometimes targets. Over 50 acts of sabotage were carried out on American targets from 1914 to 1918. Of those 50, nearly 30 occurred in the New York area alone. Not only did several factories and warehouses operate in the New York area, but ports in and around New York were the major staging point for shipping supplies to the western front in Europe.

Black Tom pier was located across the harbor from Ellis Island and the Statue of Liberty. The pier partially rested on Black Tom Island, from which it derived its name. The adjacent shore was crowded with warehouses, loading docks, and train tracks. While shipping had always flowed steadily from Black Tom, German agents noted an increase of activity from the site after the outbreak of war. Further investigations revealed that Black Tom was indeed connected to the war effort, and was the major shipping point for most of the fuel reserves bound for Europe. A munitions factory in Manhattan also shipped the detonator fuses it manufactured from Black Tom. A Pennsylvania company used the pier to load dynamite and other explosives onto transports. The combination of materials made Black Tom not only a dangerous place, but also a prime target for sabotage. Destruction of Black Tom would not only stall the shipment of supplies to Europe, but the volatile cargo would ignite and likely cause considerable property damage to the surrounding area.

Planning the attack at Black Tom. In 1914, shortly after the start of war in Europe, the German government sent a new ambassador to Washington. Count Johann Von Bernstorff brought with him a consular staff not of diplomats, but of trained German intelligence operatives. The staff also had an unusually high budget of 150 million dollars. The staff performed regular consular duties, but also led a network of other agents in the Unites States. They designated targets for sabotage, and used their money to buy resources and bribe officials. Soon after the German delegation arrived, the first sabotage fires were reported. In addition to monetary damage, the fires scarred the pre-1920s American psyche. A certain hysteria began regarding the presence of spies and saboteurs on American soil. Rumors of German agents spreading germs, planting bombs, and kidnapping people were plentiful in the public imagination. Even though the threat posed by saboteurs on the public was propagandized to the extreme, the actions of saboteurs were limited in scope until 1916.

German agents, including master spy Franz von Rintelen, worked to increase the damage inflicted by their attacks. Von Rintelen devised an explosive charge called a pencil bomb that was designed to detonate when a ship was already out to sea. German intelligence alerted the German navy of the position and names of ships that were carrying weapons and supplies. Some of these merchant vessels were sunk without warning. After just a few short months, von Rintelen and his operatives caused nearly 100 million dollars worth of damage. British intelligence and police then devised a plan to lure von Rintelen back to Germany via Britain. British intelligence sent the agent a telegram with fake orders from German command to attack a target off the British coastline. Von Rintelen took the bait, was promptly arrested before arriving in Britain, and was extradited back to the United States to stand trial. Sabotage attacks continued to occur. Von Rintelen's most ambitious plan for destruction was carried out in his absence.

The Black Tom explosion. Months before his capture, von Rintelen established a team of agents that would be responsible for the destruction of Black Tom Pier. He hired several agents to perform various tasks from smuggling the charges onto ships to bribing pier workers. It remains unknown who actually lit the first explosive fuse to cause the explosion at Black Tom. Police investigations pointed to a man named Michael Kristoff who was living at a boarding house in Bayonne, New Jersey, and was reported by his land lady to keep odd hours and often return home smelling of fuel or having small soot stains on his hands or clothing. Kristoff, when later questioned by authorities mentioned several other accomplices, but did not specifically mention their various roles in the sabotage.

The exact events of the night of the Black tom explosion largely remain a mystery. Several night watchmen guarded the area around the pier, but two were later discovered to have accepted bribes from German agents to loosen their guard. The cargo itself was largely unprotected, and sat loaded on moored barges and hips in the harbor. An ammunition storage facility and several fuel tanks were located on the adjacent shore. The first fire and explosion most likely began in this area. Guards fled the scene, wary of the materials they knew were in the vicinity. At 2:08 a.m., a thunderous explosion shook the New Jersey harbor, shattered windows, and threw people from their beds across the bay in Manhattan. That explosion began aboard the *Johnson 17,* a ship carrying explosives and fuel that was docked near the pier. Several other explosions were heard shortly after, and continued until dawn. Shrapnel rained down on New York City and the New Jersey harbor area. Immigrants awaiting entry processing on Ellis Island were evacuated from their barracks, and the Statue of Liberty sustained damage from flying debris. When all of the fuel and explosives were spent, the smoke cleared to reveal a swath of devastation several city blocks wide. Black Tom pier and most of its island were gone.

Investigation following the war. Following the war, a special commission convened to assess damages from various incidences of terrorism in the United States. The Mixed Claims Commission consisted of a German, an American, and a neutral representative. The commission reviewed the claims of industries, companies, and governments that lost property to the work of saboteurs during the war. The Black Tom explosion was the largest of such claims. After reviewing evidence supplied by police and intelligence investigations, the panel decided that the explosion was the result of foul play on the part of German terrorists. The commission awarded a settlement amount of 50 million dollars, the largest damage claim awarded for a single incident during the war. The money was to be paid from German reparations payments proscribed in the Treaty of Versailles. The damage award to the plaintiffs, however, was not finally made until 1939.

FURTHER READING:

BOOKS:

Volkman, Ernest. *Espionage: The Greatest Spy Operations of the Twentieth Century.* New York: John Wiley & Sons,1996.

Whitcover, Jules.*Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914–1917.* Chapel Hill, NC: Algonquin Books,1989.

ELECTRONIC:

Vogel, Peter. "Ship Explosions: Black Tom Island, SS *Mary Luckenbach,* SS *Robert Rowan,* USS *Mount Hood"* from *The Last Wave from Port Chicago* 2001. <http://www.portchicago.org/lastwave/chapter8.htm> (December 2, 2003).

SEE ALSO

World War I

Bletchley Park

ADRIENNE WILMOTH LERNER

Bletchley Park was the headquarters of the British Military Intelligence Government Code and Cipher School during World War II. Located fifty miles north of London, on the grounds of the sprawling Victorian mansion for which it was named, Bletchley Park employed 12,000 code breakers and staff. Bletchley Park cryptologists successfully broke the major codes used by the German military and high command, creating the most advanced computing sources of the time with few resources. British cryptologists also aided United States efforts to break Japanese codes. Intelligence information gathered from Bletchley Park is credited with significantly aiding the Allied war effort and saving thousands of lives.

The beginning of Bletchley Park. Although British Military Intelligence employed code breakers during World War I, they failed to establish a permanent cryptology department in the inter-war period. In 1938, on the eve of World War II, British Military Intelligence revived the cryptology department. Drafting cryptographers from all disciplines, and heavily recruiting young men from Oxford and Cambridge, the first cryptology operations were established in London. The group's main task was to correspond with foreign code breakers in allied nations and cull information regarding their cryptology efforts against German codes.

In the summer of 1939, British Intelligence moved the cryptology department to Bletchley Park, officially dubbed Station X because it was the tenth division of the intelligence organization. A cipher school was established on the grounds to train new code breakers. As war was on the horizon, a large number of women were trained for employment at Bletchley Park. At the height of the war, three-quarters of Bletchley Park staff were women. The focus of operations at Station X shifted to active code breaking. By the outbreak of World War II in September of 1939, Bletchley Park cryptologists had already made considerable progress against some German diplomatic codes.

Early code breaking efforts. During the two years of the war, British cryptologists decoded German communications with limited success. Older codes, used for low security messages, were readily identified and broken by the Bletchley Park team. Some newer codes were broken mathematically, but decoding and translating these messages by hand proved an arduous task. By the time messages were fully understood, the information they contained was often outdated. Compounding the problem, these intercepts contained very little useful intelligence information. Since the mid-1930s, the German government had used complex cipher machines to disguise their most important communications.

The first great code breaking triumph at Bletchley Park came on August 30, 1941. A British "Y Station," one of the military listening stations that intercepted German communications, picked up a depth, a repeat transmission that used the same settings on the cipher machine. This intercept was forwarded to Bletchley Park. Cryptologists identified as "fish," the nickname for a message produced by the illusive *Geheimschreiber* cipher machine. Within two months, the Bletchley Park team broke the high-level German code.

To facilitate the processing of "fish" intercepts, Bletchley Park engineers borrowed an idea from plans the Polish intelligence service gave Britain before the war. They constructed a machine that aided the deciphering of intercepts, nicknamed a "bombe" because of the low, roaring noise it made while operating. The "bombe" constructed to decipher *Geheimschreiber* transmissions did help cryptographers to process intercepts more rapidly, but the machine required the exact synchronization of two paper tapes for printing. The tapes often broke, and the machine had to be reset. In addition, the start setting to process each intercept, the original cipher settings used by the Germans to send the message, had to be calculated by British cryptologists by hand. The process was still too complex to yield decoded intercepts ready for immediate translation to be useful to intelligence and military personnel.

Operation Ultra: breaking the German Enigma machine. Most of Germany's high-level military messages were encoded using a cipher machine called Enigma. The complex code used not only a cipher, but also an overlaying encryption to disguise the original text. The series of rotor wheels on the Enigma teleprinter gave the machine an extraordinary number of code combinations. The Germans were so confidant that the machine code was so nearly infinite in possibilities that it could never be broken. However, various intelligence services in neighboring nations had made considerable progress breaking Enigma even before the outbreak of the war. In Britain, efforts to break Enigma were known as Operation Ultra.

In the months preceding the German invasion of Poland in 1939, Polish intelligence passed on to British intelligence information on their efforts to break Enigma. Most helpful was the information Polish spies gathered on how the cipher machine operated, including sketches of the teleprinter and some of its components. With the information, Bletchley Park cryptologists found two key weak links in the Enigma code. Enigma code prohibited that any letter be encrypted as itself, and German standards of communication dictated that the same phrase

The Duke of York, foreground, reads a printout from the Colossus computer during his tour of Bletchley Park, the former British Spy Center, England. ©CORBIS SYGMA.

begin all transmissions. Exploiting these two weaknesses, British cryptologists unraveled the Enigma code mathematically in late 1940.

Even though cryptologists could read portions of Enigma transmissions, they encountered the same delay of accessing intercepted information as they had with other codes. Another bombe was constructed that could process Enigma codes, expediting code breaking. However, cryptologists and engineers at Bletchley Park realized that another mechanical solution was needed to fully exploit German intercepts. To this end, two Bletchley Park engineers invented Colossus, the first electronic, programmable machine in 1943. Colossus not only decoded messages, but also broke through the overlaying cipher, producing a ready to translate copy of the intercept in the original German. With Colossus, Bletchley Park could decipher German communications before the intended recipients. Translated intercepts were immediately passed on to intelligence and military officials, making Bletchley Park central to the Allied war effort.

Security at Bletchley Park. Concerned that the German military and government would change encryption devises if they knew of the operation, operations at Bletchley Park were shrouded in absolute secrecy. Details of Operation Ultra and other specific code breaking missions were fully known by only four people. A special intelligence protocol was established to funnel information into and out of Bletchley Park. No one link in the chain of information knew more than two other people involved in the operation.

In order to guard Bletchley Park secrets in the event of a German invasion or bombing campaign of Britain, Bletchley Park's extensive archives of every decoded intercept and the accompanying original intercept were photographed and catalogued at the Bodleian Library at Oxford University. Code breaking equipment was supposed to be entirely disassembled, put on a nearby train to Liverpool, and then ferried to the United States if Bletchley Park were in danger of falling into enemy hands. The tight security surrounding Bletchley Park was remarkably successful. The operation was one of the few government and military outposts that was not compromised by German spies.

Legacy of Bletchley Park. The work of cryptologists and engineers at Bletchley Park is often credited with shortening the duration of the war in Europe by an estimated two to three years. Bletchley Park intelligence aided military

strategy, the shipment of necessary troops and supplies, and turned the tide of the war in favor of the Allies.

German U-boats controlled the seas until Bletchley Park decoded intercepts provided military leaders and shipping interests with up-to-date fleet positions and mission reports. Ultra intelligence aided the sinking of the German destroyer, *Bismarck*, a great moral victor for the British Navy.

On land, Station X intelligence helped Allied forces plan their invasions of North Africa, Italy, and France. During the D-Day offensive and the subsequent Allied march across France, military field command received daily intelligence updates based on information garnered by Bletchley Park code breaking efforts.

Bletchley Park also intercepted the first dispatches relating to German prisoner of war and concentration camps. Other intercepts decoded by Bletchley Park provided Allied military leaders with the first evidence of the Holocaust.

After the war, the Bletchley Park was abandoned and the staff sworn to secrecy regarding their wartime employment. All of the deciphering equipment, including replica teleprinters, bombes, and even Colossus, were disassembled and archived or simply destroyed. By March of 1946, no trace of Station X operations remained on the grounds of Bletchley Park, with the exception of the hastily constructed outbuildings, known as huts, which housed offices and staff. British Military Intelligence, known after the war as MI-6, did not dissolve the Government Cipher School or cryptology department. The department was moved to MI-6 headquarters in London, and then to Cheltenham in 1952 where its main mission was the decoding of Soviet Cold War-era communications.

Although its contribution to the war effort was highly significant, the exploits of Bletchley Park were not fully known until details regarding Operation Ultra and Station X were finally declassified in 1989. The continued secrecy of Bletchley Park allowed American engineers in 1945 to take credit for the invention of the world's first computer, ENIAC, built two years after Colossus. No member of the Bletchley Park staff betrayed the secrets of Station X until the government opened its files to the public.

FURTHER READING:

BOOKS:

Hinsley, F. H. *British Intelligence in the Second World War.* Cambridge: Cambridge University Press, 1988.

Hinsley, F. H. and Alan Stripp, eds. *Codebreakers: The Inside Story of Bletchley Park.* Oxford: Oxford University Press, 2001.

Smith, Michael. *Station X: Decoding Nazi Secrets.* London: TV Books, 2000.

SEE ALSO

Codes and Ciphers
Codes, Fast and Scalable Scientific Computation
Colossus I
FISH (German Geheimschreiber *Cipher machine*
Operation Magic
OSS (United States Office of Strategic Services
Poland, Intelligence and Security
Ultra, Operation
United Kingdom, Intelligence and security
World War II

Bolivia, Intelligence and Security

Bolivia gained its independence from Spain in 1825. Since then, the nation has weathered nearly 200 political coups and other incidences of political upheaval. Throughout the last century, power has shifted between large landowners and military interests. However, political reforms in the 1980s brought the first democratized government to power. The nation still deals with periodic unrest, but continuing reform policies and an expanding intelligence and security community have helped to stabilize the Bolivian government.

Bolivia's main civilian intelligence branch collects and processes both domestic and foreign intelligence. The Ministry of the Interior oversees government intelligence services, including the Special Security Group and the Multipurpose Intervention Brigade (BIP). Both agencies have garnered criticism from Bolivian citizens and journalists for conducting political espionage operations in recent years.

Illegal drug trafficking remains one of Bolivia's main political and social issues. In cooperation with international anti-crime and anti-trafficking efforts, Bolivia established the Special Anti-narcotics Force (FELCN). The FELCN maintains intelligence personnel and surveillance equipment to identify and track drug smuggling rings. The agency also has elite action units that infiltrate trafficking networks and made arrests. The FELCN also works closely with The Bolivian National Police.

Bolivia's intelligence community has a full-time anti-terrorism department, the Special Elite Anti-terrorism Force (FEAE). This unit has been operational in Bolivia long before the recent international focus on global terrorism. FEAE focuses on collecting intelligence regarding threats to Bolivian national interests and government personnel, mostly from paramilitary groups in Latin America and from drug cartels.

Bolivia is a member of the United Nations (UN) and several pan-Latin American security organizations.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. "Bolivia" CIA World Factbook <http://www.cia.gov/cia/publications/factbook/geos/bl.html> (April 8, 2003).

Bomb Damage, Forensic Assessment

■ JUDSON KNIGHT

Just as fires and explosions are closely related phenomena in physical and chemical terms, bomb-damage assessment is an aspect of forensic science closely related to arson investigation. In both cases, authorities analyze a crime scene for telltale signs of the nature of the materials that facilitated the conflagration. In the United States, the two agencies most concerned with bomb-damage assessment at the federal level are the Bureau of Alcohol, Tobacco, and Firearms (ATF), and the Explosives Unit of the Federal Bureau of Investigation (FBI).

Both fires and explosions involve a physical change in materials, such as the conversion of solid or liquid into gas, as well as the conversion of small quantities of matter into energy. Additionally, these processes involve a chemical change or reaction, that is, a rearrangement of atoms. Both processes must take place in the presence of oxygen, which is among the most reactive of the chemical elements, meaning that it is highly likely to bond with atoms of other elements.

During the process of oxidation, an element bonding with oxygen loses electrons, while the oxygen gains electrons, a process chemically known as reduction. The world is full of oxidation-reduction reactions, some of which include the rusting or corrosion of metals, the metabolism of food and other biological processes, and combustion. The last of these is commonly known as the process by which materials catch fire, and explosion is simply a fast form of combustion. In the combustion process, chemical bonds are broken quickly, releasing energy that is experienced in the form of heat. In the case of explosion, these bonds are broken even more quickly, producing even more heat and more kinetic energy, which propels objects outward from the center of the blast with greater impact.

Investigating a crime scene. The investigator of a scene where a bombing has taken place must be schooled both in basic physics and chemistry, but also forensic science, or the application of scientific techniques for the purpose of solving crimes. One of the first matters of interest to the investigator, obviously, is the nature of the explosive itself. At the low end of the spectrum are unsophisticated devices such as pipe bombs, which are usually little more than metal pipe containing black powder from shotgun shells.

Much more complex are explosives using TNT (trinitoluene) or nitroglycerin. The latter is found in dynamite, which combines sodium nitrate, nitroglycerin, and inert compounds. One notorious variety of explosive is ammonium nitrate, used in the 1993 World Trade Center bombing and the 1995 Oklahoma City bombing. Combined with fuel oil, it is known as ANFO, a foul-smelling—and lethal—sludge.

One difference between lower-level explosives and their more sophisticated cousins is the fact that the latter requires a detonator or blasting cap, a device to make it active. Investigators will, therefore, seek not only the telltale physical and chemical residue that will lead to a determination of the type of bomb used, but also for evidence of detonators and other components such as tapes, wires, timers, switches, and batteries.

Agencies and bombings. ATF agents investigating the first World Trade Center bombing, which killed six people, found a great deal of chemical evidence in the aftermath, ranging from the acrid, acidic smell of the air to specific types of molecular residue. There was also physical evidence that identified the perpetrators' van as the site where the blast originated: among the items noted were "feathering," or the fact of being stretched by the blast; "bluing," exposure to welding-torch-like heat; and "dimpling," whereby the metal close to the blast liquefied and shot out, colliding with nearby objects and leaving tiny craters on their surfaces.

In addition to the ATF, the FBI operates a laboratory to which other law-enforcement agencies submit materials for investigation. At the international level, bomb damage assessment may be performed by security services of various nations, or even by international teams, which may include civilians. Such was the case in the investigation of the scene in Bali, Indonesia, where Islamist terrorists detonated a bomb that killed several hundred people in October 2002.

■ FURTHER READING:

BOOKS:

Bolz, Frank, et al. *The Counterterrorism Handbook: Tactics, Procedures, and Techniques.* Boca Raton, FL: CRC Press, 2002.

ELECTRONIC:

BBC News. Q&A: Bali Forensic Challenge. <http://news.bbc.co.uk/2/hi/asia-pacific/2327687.stm> (January 16, 2003).

Bureau of Alcohol, Tobacco, and Firearms. Arson and Explosives Programs. <http://www.atf.treas.gov/explarson/index.htm> (January 16, 2003).

An Australian forensic team collects evidence at the bombing site of a nightclub in Kuta, Bali, that killed nearly 200 people. Suspects arrested for the bombing claimed to be members of the Jemaah Islamiyah regional network, an ally of Osama bin Laden's Al Qaeda. AP/WIDE WORLD PHOTOS.

FBI Laboratory Explosives Unit. <http://www.fbi.gov/hq/lab/org/eu.htm> (January 16, 2003).

SEE ALSO

Bomb Detection Devices
Forensic Science

Bomb Detection Devices

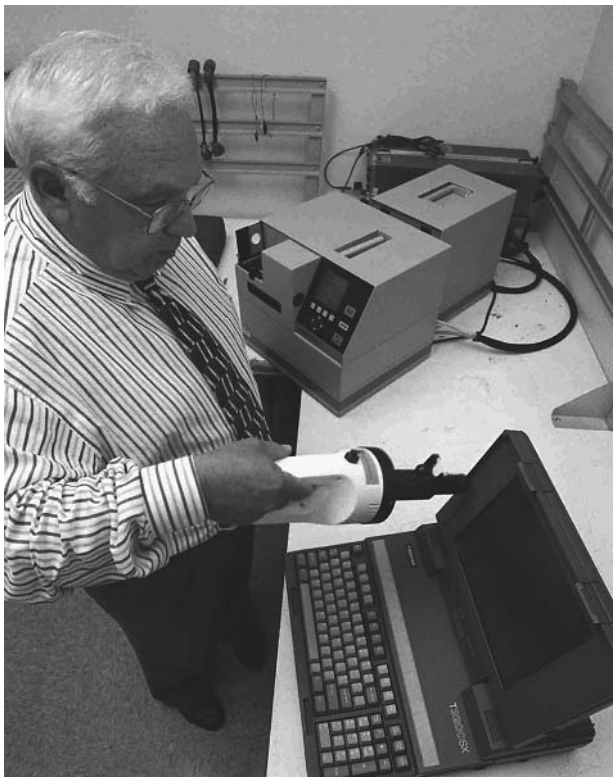
BRIAN HOYLE

When detonated in strategic, population-dense, or confined spaces, bombs are especially destructive. For example, a bomb planted by political terrorists in a suitcase was responsible for the explosion of Pan Am Flight 103 over Lockerbie, Scotland, on December 21, 1988, that claimed 270 lives. Given the devastation that bombs can cause, and the risk they pose to national security, the detection of bombs is a important priority in airports and elsewhere.

Despite the fact that x-ray examination may not detect some bombs, the technique is still a mainstay in bomb detection. For example, x rays are the best way to reveal the presence in luggage of suspicious shapes. Plastic explosives can be molded to resemble common objects. Also, explosives are not metallic, and so will escape metal detection. A well-trained operator is a key part of this bomb detection strategy. A newer version of the x-ray examination places a reflector on the opposite side of an object from the x-ray beam. As the rays are scattered back, they are analyzed by a sophisticated computer program, which can reveal differences in the outgoing and incoming beams that were caused by passage of the beams through suspicious material.

Another version of the x-ray dual energy technology sends two x-ray beams through the object at the same time. One of the beams distinguishes organic material (i.e., food, leather objects, paper) and displays them as red. The other beam distinguishes inorganic objects (i.e., metal clips, umbrella, metal pens) as green or blue. The color difference helps the operator quickly scan packages and baggage for object that are suspicious by their shape or chemistry. A similar method, which uses radio waves instead of x rays, is called quadrupole resonance technology.

Another optical device is computer tomography, a technique that has been adapted from the CAT scan x-ray technology used in the medical operating room. In



A dust sample is taken from a laptop computer and the particles analyzed for explosives residue by a Barringer explosives detection device. AP/WIDE WORLD PHOTOS.

tomography, an object is scanned and then a computer analyzes the x-ray image. If areas of the package have not been adequately revealed, the x-ray source can be rotated so as to produce a detailed view of the specific area. In this way packages and baggage can be examined in great detail.

Some bomb components can leave a scent. Until a few decades ago, specially trained dogs were a mainstay of bomb detection squads. Specially trained dogs are still used today to check out packages or locations that are difficult to examine using a machine. A dog's nose is actually a bit more sensitive than the sensitivity of detection machinery that is currently available. However, a dog and handler costs approximately $50,000 a year, whereas a piece of detection equipment represents a one-time cost of $20,000 to $40,000. Thus, machines are becoming more prevalent.

One such technology utilizes gas chromatography and a property called chemiluminescence. In gas chromatography, chemicals of different composition can be separated from each other based on their differing speeds in a stream of gas (selection of the gas can determine the rate of movement of different compounds). A compound in the gas, which will then glow, will recognize an isolated compound that has a certain chemical group in its structure. The glowing (chemiluminescence) registers on an optical detector, revealing the presence of the explosive chemical.

Devices known as sniffers detect vapor given off by certain explosives. Chemicals such as nitroglycerin are readily detected. But, a sniffer can miss explosives such as plastic explosives that do not readily vaporize. Thus, a sniffer should be used only as part of a bomb detection regimen that involves other detection techniques.

Another device detects chemicals present in bombs by concentrating the air collected from a target location. The air is drawn through a filter, where explosive chemicals collect, due to their tendency to be heavier than the air molecules around them. The filter is analyzed using ion mobility spectrometry

The spectrometric technique is very sensitive. Less than a nanogram (10_9 of a gram) of explosives residue can be detected. To put this into perspective, a fingerprint on a luggage handle left by someone had been handling explosives will typically contain 100,000 times more of the residue.

FURTHER READING:

BOOKS:

Green, Michael. *Bomb Detection Squads.* Mankato, MN: Capstone Press, 1998.

Shubert, Hiltmar, Andre Kuznetsov, and Audrey Kuznetsov. *Detection of Explosives and Landmines.* Hingham, MA: Kluwer Academic Publishers, 2002.

Yinon, Jehuda. *Forensic and Environmental Detection of Explosives.* New York: John Wiley & Sons, 1999.

ELECTRONIC:

Sandia National Laboratories. "Miniaturization of chemical preconcentrators brings better bomb-detecting and drug-sniffing devices." Sandia Lab News. August 13, 1999. <http://www.sandia.gov/LabNews/LN08–13-99/sniffer_story.html>(21 January 2003).

SEE ALSO

Explosive Coal
Gas Chromatograph-Mass Spectrometer
Isotopic Analysis
Metal Detectors
Remote Sensing

Bombe

ADRIENNE WILMOTH LERNER

A bombe was a mechanical device used for the rapid decryption and transcription of complex ciphers. Developed during World War II, the multiple bombes employed by British and United States military intelligence code breakers aided the allied war effort by providing access to German and Japanese military secrets. The most famous bombe, employed by British code breakers at Bletchley

Joe Desch, shown in 1943, headed a top-secret program at the National Cash Register Co. in Dayton, Ohio, to develop a high-speed deciphering machine called a Bombe, used to crack the Nazi submarine code. AP/WIDE WORLD PHOTOS.

Park against the German Enigma cipher, could break messages 72 times faster than the first Pentium computer.

The bombe derived its name from the loud, rhythmic, and somewhat ominous ticking noise it made while computing code permutations. The machine itself was highly complex, requiring skill in mathematical code breaking and engineering to construct. Throughout World War II, the form of the bombe changed many times. Each improvement added to the machine's ultimate effectiveness and efficiency.

Enigma and the development of the bombe. Most of Germany's high-level military messages were encoded using a cipher machine called Enigma. The complex code used not only a cipher, but also an overlaying encryption to disguise the original text. The series of rotor wheels on the Enigma teleprinter gave the machine an extraordinary number of code combinations. The Germans were confidant that the machine code was perfectly random, and therefore mathematically unbreakable. However, both Polish and Swedish intelligence made significant progress breaking Enigma even before the outbreak of World War II.

In the months preceding the German invasion of Poland in 1939, Polish intelligence gave British intelligence information on their efforts to break Enigma. Most helpful was the information Polish spies gathered on how the cipher machine operated, including sketches of the teleprinter and some of its components. The Poles also included blueprints for a code-breaking device that they had not yet been able to construct, the first bombe decoder. At the time the Poles broke Enigma using longhand mathematics, the Enigma machine had only three rotors. On the eve of war, the Germans replaced most of the three rotor machines with new a new five rotor model, making Enigma more difficult to break, and sending British engineers back to the drawing board to redesign the bombe.

Before the mechanical device could be designed and constructed, however, Bletchley Park cryptologists had to break the new version mathematically. With the information provided by Polish intelligence, Bletchley Park cryptologists found two key weak links in the Enigma code. Enigma code prohibited that any letter be encrypted as itself, and German standards of diplomatic communication dictated that the same phrase begin many transmissions. Exploiting these two weaknesses, British cryptologists broke Enigma in 1940. Within a year, they had broken two other major German codes, including the perplexing Lorenz cipher used by Hitler's High Command. Bletchley Park engineers then set out to adapt original bombe designs to operate against the new codes.

British engineer Alan Turing designed and constructed the first successful bombe. The Turing Bombe, or "Tabs," as it became known, operated against the German Enigma code, but could be adapted to decipher other codes. The Turing Bombe was the main device used against Enigma, but its complex operation required the work of several operators. During the course of the war, women were the predominant operators of Bletchley Park bombes, decoding and translating intercepts for intelligence service use. Even with the operation of several bombes, Enigma intercept information could not be used in "real time" but military field command or forward intelligence units. A series of improvements aided computational time, including a diagonal switchboard and "machine gun" voltage regulator, which were added to eliminate processing errors that stopped the bombe's computation. A teleprinter was added to the device to allow for simultaneous transcription of messages into the original German, ready for translation.

British intelligence shared some of their cryptanalytic work with United States forces, even before the U.S. entered the war in 1941. However, after the bombing of Pearl Harbor, President Roosevelt acknowledged that the cryptanalytic efforts of military intelligence needed additional aid. Some Bletchley Park personnel went to America to train new code breakers, most of whom were members of the Women Accepted for Voluntary Emergency Service Corps (WAVES). WAVES assembled and trained to operate various bombes, eventually producing 121 bombes for used against seven different Japanese and German codes. After the Germans began sharing Enigma code secrets and teleprinter construction secrets with the Japanese in 1942, U.S. intelligence became more able to decipher

Japanese codes and could adapt Enigma bombe designs to fit Japanese Red and Purple codes.

How a bombe worked: The mechanics of code breaking. The Enigma teleprinter functioned by replacing plain text letters with random letters, chosen by the settings of a series of rotors individual to each letter and space in a plain text message. The Enigma machine had a possible 15 million, million (15×10^{12}) combinations, but within each rotor set, the combinations were far fewer. Repeated phrases, called "cribs," such as common greetings or the name and ranks of officers, gave cryptographers a clue about the mathematical cycle of the rotors and how they replaced plain text letters. Once a series of these cycles was mathematically determined, the logic equation could be used to painstakingly decipher intercepts. The bombe worked on the concept that these cycles, and the equations representing them, could be replaced with electrical circuits.

The Turing Bombe replicated the rotors of a German Enigma machine, replacing the center reflecting rotor with a standard rotor that could be handset. The rotors were connected by a set of 26 parallel wires. The wire selected by the rotor positions determined the passage of voltage to the plug board. The machine then searched for various combinations of loops and live wires, assigning each a value on the plaintext/ cipher text rows of a diagonal board. A teleprinter decoded the messages on to synchronized paper tapes.

Legacy of bombes. By the end of the war, the bombe was still being used to decode enemy intercepts in the United States. British code breakers and engineers at Bletchley Park, however, invented a new machine, Colossus, that decoded messages more rapidly and with greater accuracy than the bombes. Colossus was the world's first programmable computer, capable of decoding and transcribing messages without the cumbersome synchronization of paper tapes. The advent of punch-card computer processing ended the era of the code breaking bombe.

After the end of the war, British intelligence dismantled its operations as Bletchley Park. The numerous bombes, and Colossus, were disassembled or destroyed. The entire code breaking operation remained secret until the late-1980s, but after the news of Bletchley Park operations was broken to the public, historical preservationists sought to restore Bletchley Park and its code breaking apparati. The British Computer Society's Computer Conservation Society embarked on an ambitious endeavor to reconstruct Colossus and the Turning bombe in 1999.

FURTHER READING:

BOOKS:

Hinsley, F. H. *British Intelligence in the Second World War.* Cambridge: Cambridge University Press, 1988.

Hinsley, F. H. and Alan Stripp, eds. *Codebreakers: The Inside Story of Bletchley Park.* Oxford: Oxford University Press, 2001.

Stinson, Douglas. *Cryptography: Theory and Practice*, second edition. Chapman and Hall, 2002.

SEE ALSO

Codes and Ciphers
Codes, Fast and Scalable Scientific Computation
Colossus I
FISH (German Geheimschreiber *Cipher Machine)*
Operation Magic
OSS (United States Office of Strategic Services)
Poland, Intelligence and Security
Purple Machine
Ultra, Operation
United Kingdom, Intelligence and Security
World War II, United States Breaking of Japanese Naval Codes

Border Crossing and Inspection.

SEE *IBIS (Interagency Border Inspection System).*

Bosnia and Herzegovina, Intelligence and Security

Following World War I, the nations in the Balkan region were unified into a single state, known after 1929 as Yugoslavia. Tensions between the region's ethnic populations remained high, but the establishment of a dictatorship under Marshal Tito kept Yugoslavia united after World War II. After Tito's death, authoritarianism continued to dominate the Yugoslavian regime. The Yugoslavian intelligence community was dominated by secret police forces and government-backed political espionage. Modeled after intelligence and security forces in the Soviet Union, Yugoslav intelligence focused on protecting the ruling regime under the direct control of the Communist Central Committee.

In the early 1990s, Yugoslavia broke apart following the fall of the Soviet Union. In 1991 and 1992, the various ethnic states in the Balkan region declared their independence. Border disputes and ethnic tensions flared in the region, sparking intense warfare. The most intense conflict erupted in Bosnia and Herzegovina. The state was deeply divided. Bosniak Muslims, seeking autonomy, fought Serbian-backed forces. As the conflict escalated, the international community became concerned with the region's endemic warfare. By the time United Nations and NATO forces intervened in the region, ethnic cleansing—genocide—plagued Bosnia and Herzegovina.

International intervention helped end genocide and warfare in the region, but civil war left the national infrastructure of Bosnia and Herzegovina devastated. In 1998, the Bosnian government began an ambitious program to rebuild the nation's intelligence and security forces. As of 2003, NATO-led Stabilization Forces (SFOR) continue to operate in Bosnia and Herzegovina, preserving peace in the region and aiding in the formation of new national security forces.

Bosnia and Herzegovina's main civilian intelligence service is the Agency for Investigation and Documentation (AID). The AID investigates current and past criminal activities, with a focus on ferreting out perpetrators of genocide and other war crimes. The investigative force also conducts domestic intelligence operations, including political and communications surveillance of military forces. The State Security Agency and the Civil Police work closely with the AID to assess and neutralize threats to national security, and protect the nation's citizens.

Although Bosnia and Herzegovina's military is greatly limited in their actions under the terms of current, regional cease-fire agreement, some military-based intelligence services continue to operate. The main objective of military intelligence services is to obtain foreign intelligence information, especially that which relates to the military strength of its neighboring states, Croatia and Serbia. Government-backed espionage against dissident and rival ethnic groups was circumscribed by international peacekeeping forces to deter renewed hostilities in the region.

The government also maintains a mixed civilian-military Anti-terrorist Brigade. Little is known about the daily operations of this secret police force.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. "Bosnia and Herzegovina" CIA World Factbook <http://www.cia.gov/cia/publications/factbook/geos/bk.html> (April 8, 2003).

SEE ALSO

Croatia, Intelligence and Security
Serbia, Intelligence and Security
United Nations Security Council

Botulinum Toxin

BRIAN HOYLE

Botulinum toxin is among the most poisonous substances known. The toxin, which can be ingested or inhaled, and which disrupts transmission of nerve impulses to muscles, is naturally produced by the bacterium *Clostridium botulinum*. Certain strains of *C. baratii* and *C. butyricum* can also be capable of producing the toxin.

Botulinum toxin has become well known in recent years for two reasons. First, the toxin has become a weapon in the arsenal of terrorists. Contamination of food is one route for infection with the toxin. The toxin can also be released into the air, which was attempted on at least three occasions between 1990 and 1995 by the Japanese cult Aum Shinrikyo. The government of Iraq admitted to United Nations inspectors following the 1991 Persian Gulf War that tens of thousands of liters of botulism toxin had been produced and loaded into weapons. The toxin was the most numerous of all the biological weapons then developed by Iraq.

Paradoxically, the other reason for the toxin's fame is the use of the toxin as a cosmetic enhancement (i.e., "botox").

There are at least seven structurally different versions of botulinum toxin. The type designated as type A is responsible for some food-borne outbreaks in the United States and elsewhere. Improperly canned foods are a particular threat.

Clostridium botulinum is a spore-forming bacterium. Like the well-known anthrax bacillus, the spores of *Clostridium botulinum* can persist in the environment for many years and, when conditions become more favorable (i.e., in a wound, food, and the lungs) the spore can germinate and free the toxin. Dried preparations of the spores can thus represent a terrorist weapon.

The use of botulinum toxin as a weapon began in the 1930s, with experiments conducted by the Japanese on prisoners during the occupation of Manchuria. In World War II, plans were made to vaccinate Allied troops participating in the D-day invasion of Normandy, because of concerns that Germany had weaponized the toxin. Even the United States maintained an active biological weapons program, including the use of botulism toxin, into the late 1960s.

Botulism toxin acts by preventing the transmission of nerve signals between the nerves that connect with muscle cells. Progressive functional deterioration of the affected muscles occurs. Symptoms of botulism intoxication include dizziness, blurred or double vision, nausea, vomiting, diarrhea, and weakness of muscles in various areas of the body. The muscle failure can be so severe as to lead to coma and respiratory arrest. Even in those who survive exposure to the toxin, complete recovery can take months.

FURTHER READING:

BOOKS:

Tucker, J.B., (ed.). *Toxic Terror: Assessing the Terrorist Use of Chemical and Biological Weapons.* Cambridge: MIT Press, 2000.

PERIODICALS:

Byrne, M.P., and L.A. Smith. "Development of Vaccines for Prevention of Botulism." *Biochimie* no. 82 (2000): 955–966.

Kahn, A.S., S. Morse, and S. Lillibridge. "Public-health Prepardness for Biological Terrorism in the USA." *Lancet* no. 356 (2000): 1179–1182.

Montecucco, C. (ed.). "Clostridial Neurotoxins: The Molecular Pathogenesis of Tetanus and Botulism." *Current Topics in Microbiology and Immunology* no. 195 (1995): 1–278.

Lacy, D.B., W. Tepp, A.C. Cohen, et al. "Crystal Structure of Botulinum Neurotoxin Type A and Implications for Toxicity." *Nature Structural Biology* no. 5 (1998): 898–902.

ELECTRONIC:

Centers for Disease Control and Prevention. "Botulism." Public Health Emergency Preparedness and Response. February 7, 2003. <http://www.bt.cdc.gov/agent/botulism/index.asp>(April 15, 2003).

Johns Hopkins University. "Botulinum Toxin." Center for Civilian Biodefense Strategies. 2002. <http://www.hopkins-biodefense.org/pages/agents/agentbotox.html>(April 15, 2003).

SEE ALSO

Biological Warfare
Microbiology: Applications to Espionage, Intelligence and Security
USAMRIID (United States Army Medical Research Institute of Infectious Diseases)

Botulism.

SEE *Bioterrorism.*

Brain-Machine Interfaces

JULI BERWALD

A brain-machine interface is the linkage of the brain to a mechanical device exterior to the body in such a manner that the device is controlled by natural signals from the brain. An important goal for developing such technology is to aid people who are paralyzed or otherwise physically impared. The military has interest in brain-machine interfaces as a means of controlling robotics from a distance with extreme accuracy and precision.

One of the major technological hurdles in the development of brain-machine interfaces is the understanding of neural patterns required to accomplish tasks. One company headed by American scientist Phillip Kennedy has made great advances in this area. Kennedy has developed a very small neurotropic device that is implanted into the motor cortex of the brain of severely paralyzed people. This device transmits electronic signals from the person's brain to electronic equipment that then translates the signals to a computer. People with the implant learn to control a mouse on the computer and to type text using electronic signals in their brain.

The extension of this technology is the understanding of the neural patterns required to control complex motor tasks. In 2000, scientists at Duke University implanted an array of 96 electrodes into the brain of an owl monkey. The electrical signals measured on each of the electrodes were collected when the monkey performed certain tasks, including reaching for food. These signals were then analyzed and mathematical algorithms were developed that allowed scientists to predict the trajectory of the monkey's hand from the neural signals. The scientists then programmed a robotic arm to move in three dimensions according to the monkey's brain signals. They eventually transmitted these signals over the Internet to a laboratory at MIT, where another robotic arm 600 miles away was controlled by the monkey's neural signals.

The Defense Advanced Research Projects Agency (DARPA) is extremely interested in brain-machine interfaces for controlling robotics and interpreting sensory information. In 2001, they authorized funding for the Brain-Machine Interfaces program. The goals of this program are to create new technologies that enhance human performance through non-invasive integration of neural signals into external devices. This includes understanding the neural codes required to complete complex motor tasks, building a feedback loop from an external device back to the brain, and fabricating new materials required to capture neural commands. In addition, biomimetic systems that integrate nueral signals are of interest.

Other defense related projects investigate neural networks and optics. Scientists at the U.S. Army Aviation and Missile Command (Weapons Sciences Directorate) headquartered at the Redstone Arsenal, Alabama are working intently on projects designed to integrate optic "flow" and automatic target recognition systems. These projects utilize mathematical techniques improving image factorization (e.g., image decomposition). For example, neural network based optics using specific algorithms can translate optic flow into four separate image planes that represent various motion parameters. In addition to targeting, neural network based optics may be used to navigate autonomous vehicles and other robotics.

FURTHER READING:

ELECTRONIC:

Defense Advanced Research Projects Agency: Defense Sciences Office, "Brain Machine Interfaces" <http://www.darpa.mil/dso/thrust/biosci/brainmi.htm> (March 26, 2003).

Neural Signals <http://www.neuralsignals.com> (March 26, 2003).

Science Daily: "Monkeys Control A Robot Arm Via Brain Signals" <http://www.sciencedaily.com/releases/2000/11/001116080512.htm> (November 16, 2000).

SEE ALSO

Biological and Biomimetic Systems
DARPA (Defense Advanced Research Projects Agency)

Brain Wave Scanners

The term *brain wave scanners,* in the context of law enforcement, encompasses an array of research studies and technological developments undertaken with the aim of using electronic equipment to determine the truth or falsity of an individual's statements. While such a concept may sound farfetched at first glance, it is based not on subjective phenomena, but on apparently measurable brain states. Using magnetic resonance imaging (MRI) and related equipment, it is possible to measure a subject's brain for increased activity that may indicate the telling of a lie.

The concept of a brain wave scanner is not unlike that of a polygraph, but whereas a polygraph measures fluctuations in heart rate and breathing, a scanner measures brain responses to stimuli. It could be more effective, because a "good liar" may experience little excitement in the circulatory system; however, even such an individual would be required to expend extra energy on the thought necessary to tell a lie, and it is this energy that a brain wave scanner may be able to measure.

It is often said that the truth is much easier to remember than a lie, and the activity measured by brain wave scanners offers a concrete illustration of this. When one is asked a question to which one knows the true answer, that answer comes first to mind automatically. Even if the individual has already prepared and rehearsed a lie, it is still necessary to think past the true answer and access the lie. This extra activity is easily measured on a brain scan.

Testing and Possible Applications

In a 2001 University of Pennsylvania experiment using MRI, 18 subjects were given objects to hide in their pockets, then shown a series of pictures and asked to deny that the object depicted was in their pockets. Included was a picture of the object they had pocketed, meaning that the subject was lying when saying that the object was not in his or her pocket. At that juncture, the MRI recorded an increase of activity in the anterior cinglate, a portion of the brain associated with inhibition of responses and monitoring of errors, as well as the right superior frontal gyrus, which is involved in the process of paying attention to particular stimuli.

After the September 11, 2001, terrorist attacks, a number of government agencies began to take a new look at brain scanning technology as a means of security screening. In 2002, officials of the National Aeronautics and Space Administration reportedly informed airline officials that they were developing brain-monitoring technology for use in screening airline passengers. Such activity, along with an increase of interest in brain-wave scanning by the Federal Bureau of Investigation, has raised concerns among civil-liberties groups, which view brain-wave scanning as a particularly objectionable invasion of privacy in the service of public security.

■ FURTHER READING:

PERIODICALS:

Feder, Barnaby J. "Truth and Justice, By the Blip of a Brainwave." *New York Times.* (October 9, 2001): F3.

Vedantam, Shankar. "The Polygraph Test Meets Its Match." *Washington Post.* (November 12, 2001): A2.

Wright, Karen. "Go Ahead, Try to Lie." *Discover.* 22, no. 7 (July 2001): 21–22.

Young, Emma. "Brain Scans Can Reveal Liars." *New Scientist.* (November 12, 2001).

SEE ALSO

Brain-Machine Interfaces
Electromagnetic Pulse
Polygraphs

Brazil, Intelligence and Security

Brazil gained its independence from Portugal in 1822, seizing upon a period of European unrest to establish its own government. Since that time, the government of Brazil has been traditionally unstable, with large-scale landowners, the military, and democratic forces vying for political power.

A military coup took control of the nation for much of the late twentieth century, but civilians regained control of the government in 1985. Under military rule, political dissidents were taken into custody and sometimes tortured. The government used the intelligence services to conduct surveillance of citizens and infiltrate political organizations. The regime also imposed strict censorship. In 1989, Brazil had its first free elections in three decades. Seeking to distance the new government from the legacy of its predecessors, sweeping reforms were made to

demilitarize the national intelligence and security agencies. While Brazil's government has continued to weather scandal and presidential overthrow, the reformed intelligence community established in the early 1990s remains largely intact.

While the armed forces still maintain limited special intelligence units, most of Brazil's intelligence community is civilian. The Brazilian Intelligence Agency (ABIN) was created in 1995 to replace the Strategic Affairs Secretariat (SAE). The civilian government's first attempt at a reformed intelligence agency, the SAE supervised the Brazilian intelligence community from 1990–1994. Amid concerns that military interests dominated the agency, despite efforts to demilitarize its operations, the agency was dissolved and replaced with ABIN.

The Brazilian Intelligence agency is the main intelligence and security force in Brazil. Responsible for both internal and external intelligence, the agency coordinates operations between various operational branches and national law enforcement services. Charged with the protection of Brazilian interests both at home and abroad, ABIN collects and analyzes information from a variety of sources. The agency utilizes human, signals, and remote intelligence. The largest operational branch of ABIN is its counterintelligence unit. ABIN's counterintelligence division focuses on the protection of economic interests from sabotage, terrorism, and corporate espionage. The unit also conducts political surveillance of the military and coordinates efforts with law enforcement to ensure border security.

Today, Brazil has the sixth-largest population in the world. Its two largest cities, Sao Paulo and Rio de Janeiro, have respective populations of 19 and 10 million people. The most populous nation in South America, Brazil is one of the regions leading economies. In 2000, Brazilian intelligence began a series of operations targeting illegal business practices, including money laundering, trafficking of illegal drugs, and corporate espionage.

SEE ALSO

Counter-Intelligence
Economic Espionage
Economic Intelligence

Brilliant Pebbles.

SEE *Strategic Defense Initiative and National Missile Defense.*

British Secret Intelligence Service.

SEE *MI6 (British Secret Intelligence Service).*

British Security Service.

SEE *MI5 (British Security Service).*

British Terrorism Act

In July, 2000, the British Parliament passed the Terrorism Act, a lengthy piece of legislation that criminalized a number of activities associated with groups tied to terrorism. The act initially prescribed 14 groups, most of whom were involved in Northern Ireland's sectarian conflict. In March, 2001, Parliament passed an amendment to the act, listing 21 other organizations, of which most had a Middle Eastern base.

The British Terrorism Act is an example of the fact that, and while the United Kingdom and the United States have much in common politically, the British government reserves the right to exert far greater authority over freedom of speech than Washington. Whereas the Terrorism Act makes it illegal to possess certain written materials, in America, books on bomb-making and subversion are legal.

The Terrorism Act reformed or repealed earlier measures, including the Prevention of Terrorism Act of 1989, the Northern Ireland (Emergency Provisions) Act of 1996, and the Criminal Justice (Terrorism and Conspiracy) Act of 1998. It defined terrorism, listed proscribed organizations, established government powers against proscribed groups, provided for offenses relating to fund-raising for terrorists, gave the police authority to investigate terrorist groups, and criminalized a number of offenses, including the possession of information for terrorist purposes.

Within two weeks of the September, 2001 terrorist attacks in the United States, British authorities arrested four men under the British Terrorism Act. Among them was Sulayman Balal Zainulabidin, a 43-year-old cook. Another, Loifti Raissi, was wanted in Arizona on misdemeanor charges relating to his application for a pilot's license, but was thought to have been involved in training four of the terrorists involved in the September 11 attacks.

FURTHER READING:

PERIODICALS:

Jackman, Tom. "Terror Suspect Allowed to Seek Foreign Aid." *Washington Post.* (July 18, 2002): B2.

Milbank, Dana, and T. R. Reid. "New Global Threat Revives Old Alliance." *Washington Post.* (October 16, 2001): A10.

ELECTRONIC:

London Man Charged Under British Terrorism Act. Cable News Network. <http://www.cnn.com/2001/WORLD/europe/UK/10/04/inv.britain.arrest/> (April 7, 2003).

Terrorism Act 2000. Her Majesty's Stationery Office. <http://www.hmso.gov.uk/acts/acts2000/20000011.htm> (April 7, 2003).

SEE ALSO

MI6 (British Secret Intelligence Service)
Official Secrets Act, United Kingdom
September 11 Terrorist Attacks on the United States
United Kingdom, Counter-Terrorism Policy
United Kingdom, Intelligence and Security

Brookhaven National Laboratory

K. LEE LERNER

Founded in 1947, Brookhaven National Laboratory is operated for the U.S. Department of Energy by Brookhaven Science Associates, a non-profit research company.

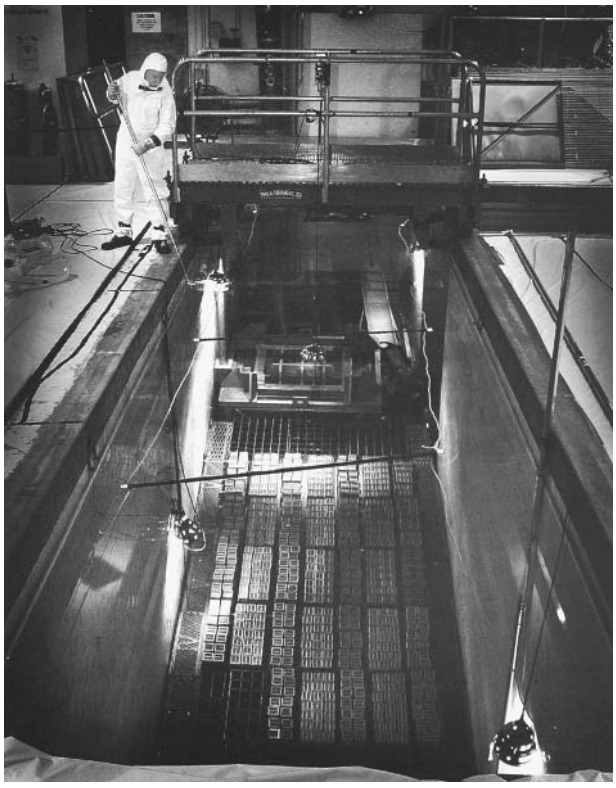
At Brookhaven, a staff of approximately 3,000 scientists, engineers, and technical support staff work alongside an additional 4,000 scientists and engineers who annually visit the facilities located on Long Island, New York.

Although research at Brookhaven impacts both basic science and national security related science issues, following the September 11, 2001, terrorist attacks on the United States, Brookhaven established an interdisciplinary working group to tackle specific issues related to counter-terrorism. The focus of the group is to oversee the development of technologies devoted to prediction, detection, and preemption, of terrorism.

An important component of Brookhaven projects is the development of sensors useful in detecting nuclear, chemical, and biological agents. For example, highly sensitive chemical sensors can detect explosives, and radiation detectors are useful in detecting contact with nuclear materials. Highly sensitive detectors are capable of measuring trace amounts in concentrations so small that the sensors can provide evidence of prior contact with suspect materials—even if the materials are no longer physically present.

Facilities at Brookhaven include a thermal neutron imaging camera that can detect radiation source emanation at distances up to approximately 200 feet. In addition, Brookhaven sensor systems utilize a number of physical properties—from laserscattering patterns to microwave probes—to interrogate unknown materials.

Biotechnology research at Brookhaven includes the development of vaccines to combat the deleterious effects of a broad spectrum of biological weapons and chemical nerve gas agents. Antidote treatment research includes the development of topical creams that contain enzymes capable of degrading nerve agents.



A Brookhaven National Laboratory employee works at a 68,000-gallon pool housing spent fuel rods in 1997, thought to be the source of a leak of radioactive materials that contaminated the groundwater source for Long Island's drinking water aquafer. AP/WIDE WORLD PHOTOS.

To facilitate rescue of individuals in debris of collapsed buildings, Brookhaven engineers designed devices to help remove debris and to image debris fields. Magnetic imaging equipment can locate damaged structural elements (e.g., iron girders) and allow rescue personnel to evaluate structural integrity and identify possible areas of survival.

Brookhaven scientists and engineers developed the Mini-Raman Lidar System (MRLS) that is capable of detecting trace amounts of dangerous chemicals (including illegal narcotics and other drugs). Laser scattering devices can also detect distinct chemical profiles or "fingerprints." MRLS allows investigators to detect those chemical associated with the processing of nuclear fuels. Because MRLS is highly sensitive, inspectors can examine questionable objects from safer distances. In many cases, MRLS can accurately detect trace molecules at distances ranging from three to ten feet. Given the proper environmental controls, MRLS can detect trace molecules at far greater distances.

Another recent national security related project at Brookhaven National Laoratory involved the development

of the Large-Volume Radiation Detector that uses compressed xenon as part of a portable, battery powered, room-temperature spectrometer unit. The spectrometer is very sensitive and offers high discrimination and resolution at levels that allow investigators the ability to distinguish between isotopes used in medical products and those associated with prohibited nuclear activities. Investigators are hopeful that the success of the small scale detector will allow construction of larger units using similar technology that are capable of rapidly examining large cargo loads (e.g., bulk cargoes at truck terminals, ports, etc.) at safer "standoff" distances.

Other research facilities include a relativistic heavy ion collider, alternating gradient synchrotron, synchrotron light source, tandem Van de Graaff accelerators, high-field MRI, positron emission tomograpahy (PET) facilities, transmission electron (TEM) and scanning (SEM) electron microscopes, a laser electron accelerator facility (LEAF), and other accelerator test facilities including 60-inch and 40-inch cyclotrons.

FURTHER READING:

ELECTRONIC:

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <http://www.dhs.gov/dhspublic/display?theme=27&content=374> (March 23, 2003).

Brookhaven National Laboratory. March 26, 2003. <http://www.bnl.gov/world/> (April 2, 2003).

SEE ALSO

Argonne National Laboratory
DOE (United States Department of Energy)
Environmental Measurements Laboratory
Lawrence Berkeley National Laboratory
Lawrence Livermore National Laboratory (LLNL)
Los Alamos National Laboratory
NNSA (United States National Nuclear Security Administration)
Oak Ridge National Laboratory (ORNL)
Pacific Northwest National Laboratory
Plum Island Animal Disease Center
Sandia National Laboratories

Bubonic Plague

BRIAN HOYLE

A concern of health and defense officials is the possible deliberate introduction of plague—or the exploitation of plague—as a terrorist weapon. Plague causing microorganisms are highly lethal, highly transmissible, and relatively easy to develop as terrorist weapons.

Bubonic plague is transmitted via fleas infected with *Yersinia pestis*. Pneumonic plague results from plague bacterium investing lung tissue. Pneumonic plague exhibits an airborne form of transmission. Infection occurs from breathing aerosolized bacteria. Untreated pneumonic plague is highly lethal.

Bubonic plague is a disease that is typically passed from rodents to other animals and humans via the bite of a flea. The flea acquires the bacterium that causes the disease as it lives on the skin of the rodent. Humans can also acquire the disease by direct contact with infected tissue.

The bacterium *Pasteurella pestis* is also known as *Yersinia pestis*, after one of its co-discoverers, Alexandre Yersin.

Prior to 1970, both United States and Soviet biological weapons programs developed techniques that enabled weapons developers to aerosolize plague particles.

Bubonic plague is named because of the symptoms. The bacterial infection produces a painful swelling of the lymph nodes. These are called buboes. Often the first swelling is evident in the groin. During the Middle Ages, a pandemic of bubonic plague was referred to as the Black Death, because of the blackening of the skin due to the dried blood that accumulated under the skin's surface.

The bubonic plague has been a significant cause of misery and death throughout recorded history. The Black Death is only one of many epidemics of plague that extended back to the beginning of recorded history. The first recorded outbreak of bubonic plague was in 542–543. This plague destroyed the attempts of the Roman emperor of the day to re-establish a Roman empire in Europe. This is only one example of how bubonic plague has changed the course of history.

The plague of London in 1665 killed over 17,000 people (almost twenty percent of the city's population). This outbreak was quelled by a huge fire that destroyed most of the city.

The disease remains present to this day. In North America, the last large epidemic occurred in Los Angeles in 1925. With the advent of the antibiotic era, bubonic plague has been controlled in the developed world. However, sporadic cases (e.g., 10 to 15 cases each year) still occur in the western United States. In less developed countries (e.g., in Africa, Bolivia, Peru, Ecuador, Brazil) thousands of cases are reported each year.

The infrequency of bubonic plague outbreaks does not mean the disease disappears altogether. Rather, the disease normally exists in what is called an enzootic state. That is, a few individuals of a certain community (e.g., rodents) harbor the disease. Sometimes, however, environmental conditions cause the disease to spread through

the carrier population, causing loss of life. As the rodent populations dies, the fleas that live on them need to find other food sources. This is when the interaction with humans and non-rodent animals can occur. Between outbreaks, *Yersinia pestis* infects rodents without causing much illness. Thus, the rodents become a reservoir of the infection.

Symptoms of infection in humans begin within days after contamination with the plague bacterium. The bacteria enter the bloodstream and travel to various organs (e.g., kidney, liver, spleen, lungs) as well as to the brain. Symptoms include shivering, nausea with vomiting, headache, intolerance to light, and a whitish-appearing tongue. Buboes then appear, followed by rupture of blood vessels. The released blood can coagulate and turn black.

If the infection is untreated, the death rate in humans approaches 75%. Prompt treatment most often leads to full recovery and a life-long immunity from further infection. Prevention is possible, since a vaccine is available. Unfortunately, the vaccine is protective for only a few months. Use of the vaccine is usually reserved for those who will be at high risk for acquiring the bacterial infection (e.g., soldiers, travelers to an outbreak region). Antibiotics such as tetracycline or sulfonamide are used more commonly as a precaution for those who might be exposed to the bacterium. Such use of antibiotics should be stopped once the risk of infection is gone, to avoid the development of resistance in other bacteria resident in the body.

The most effective way to prevent bubonic plague is the maintenance of adequate sanitary conditions. This acts to control the rodent population, especially in urban centers.

In 1970, a World Health Organization study concluded that deliberate dissemination of 110 lbs (50 kg) of aerosolized Y pestis over a city with a population of approximately 5 million people could potentially result in 150,000 cases of pneumonic plague. Half of these cases would require advanced medical care and approximately 20% would be expected to perish.

FURTHER READING:

BOOKS:

Campbell, G. L., and D. T. Dennis. "Plague and other Yersinia infections." In: D. L. Kasper, et al; eds. *Harrison's Principles of Internal Medicine,* 14th ed. New York: McGraw Hill, 1998.

Dennis, D. T., N. Gratz, J. D. Poland, and E. Tikhomirov. *Plague Manual: Epidemiology, Distribution, Surveillance and Control.* Geneva: World Health Organization, 1999.

Frist, W. H. *When Every Moment Counts: What You Need to Know about Bioterrorism from the Senates Only Doctor.* Lanham, MD: Rowman & Littlefield, 2002.

Henderson, D.A., and T.V. Inglesby. *Bioterrorism: Guidelines for Medical and Public Health Management.* Chicago: American Medical Association, 2002.

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague." *Emerging Infections 5.* Washington, D.C.: American Society for Microbiology Press, 2001.

PERIODICALS:

Kaufmann, A. F., M. I. Meltzer, and G. P. Schmid. "The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Program Justifiable?" *Emerging Infectious Diseases* no. 3 (1997): 83–94.

SEE ALSO

Antibiotics
Biocontainment Laboratories
Biological and Toxin Weapons Convention
Biological Warfare
Biological Weapons, Genetic Identification
Bioterrorism, Protective Measures
Chemical and Biological Defense Information Analysis Center (CBIAC)
Chemical and Biological Detection Technologies
Pathogen Transmission
Pathogens
Weapons of Mass Destruction

Bugs (Microphones) and Bug Detectors

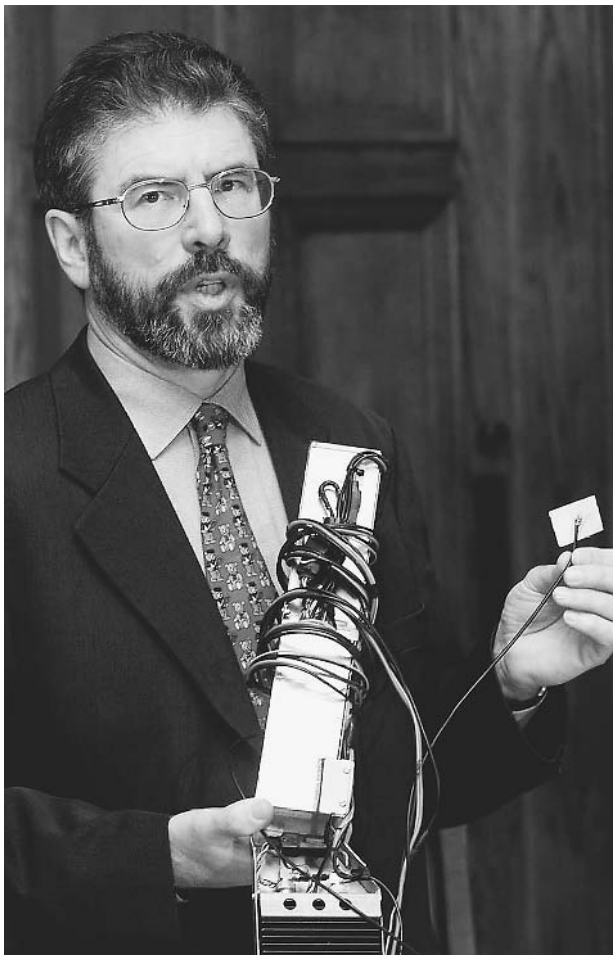
BRIAN HOYLE

A key part of intelligence gathering and surveillance is the installation of listening devices. The classic Cold War image of Soviet espionage agents secretly planting "bugs" in an office of the United States embassy is an accurate historical picture of the use of these listening devices. Police forces and private investigators also use bugging devices (with legal approval).

The use of listening devices is often a race to acquire information before the devices are discovered and removed. For example, rooms where top-secret intelligence activity occurs are frequently examined, or "swept", for bugs.

A typical electronic bug consists of a microphone and a radio transmitter. The microphone receives sound waves and either vibrates a thin membrane called a diaphragm (a dynamic microphone) or a thin metal ribbon suspended in a magnetic field (a ribbon microphone). Vibration of the diaphragm produces an electrical signal. Vibration of the metal ribbon produces a voltage change, which can be converted to an electrical signal.

The electric signals are then beamed out of the transmitter portion of the bug to a receiver. The conversation



Sinn Fein President Gerry Adams dsiplays an electronic tracking and listening device, found in a car used by Sinn Fein leaders, during a press conference in Belfast, Northern Ireland in 1999. AP/WIDE WORLD PHOTOS.

transmitted by the bug to the receiver can be recorded or listened to directly. Other types of bugs exist. For example, radio frequencies passing through the electrical wiring of a building can be intercepted. Bugs can also intercept the electrical transmissions from portable phones, wireless computers linked to a network, and even from a computer monitor.

The designation of secret listening devices as bugs is entirely suitable, given their small size. Modern bugs can be concealed in pens, calculators, and even buttons (although the latter need to be replaced frequently, as their power supply is so small).

The miniaturization of electronics has made it possible to pack more devices into the small package. For example, video equipment can be contained in a bug, enabling sight as well as sound surveillance.

Up to the 1980s, bugs operated using very high frequency, or VHF, radio waves. However, the development of mobile communications technology, particularly digital telephones, paved the way for the development of bugs that operate using ultrahigh frequency wavelength or microwaves. This has made the detection of bugs more difficult than simply detecting the output of radio waves. Some modern bugging devices can also disguise the output signal or vary the frequency of the signal, which can thwart detection.

Some bugs contain voice-activated recorders that are capable of storing up to 12 hours of conversation. The information can then be rapidly sent to a receiver in a "burst" transmission. Because detection of the bug is geared toward the frequencies emitted during transmission, the detection of these bugs is difficult. Counter systems are designed to try and activate the bug and then detect it. The transmission range of bugs has improved from mere yards to miles. Some bugs can even transmit to satellites, making monitoring from thousands of miles away feasible.

Another surveillance option is the use of a microphone. Conventional microphones operate electronically; the electrical signals representing the converted sound waves are passed through a wire to a receiving device located elsewhere. Microphones that operate using magnetic fields also exist.

Shotgun microphones equipped with a parabolic reflector can record conversation outside at a distance. Electronic filters screen out extraneous background noise in order to enhance the sensitivity of the microphone.

Laser microphones bounce a laser beam off of an object that is near the conversation. The object must be something that resonates, or is able to move as pressure waves created by noise in the room encounter it. As the object vibrates back and forth due to the sound waves from the conversation in the room, the distance traveled by the laser beam will become slightly shorter and longer. These length differences can be measured over time, and the pattern of the vibrations translated into the text of the conversation.

Microphones are extremely hard to detect, especially when used in a room where other electrical appliances (i.e., computers, telephones) are operating.

Bugs are detected by virtue of the frequencies they emit. Essentially a bug detector is a receiver. When brought near an operating bug, the detector will collect and amplify the bug's transmission. Bug detectors are now portable enough to be carried in a "sweep" of a room.

Bugs and microphones have moved from the arena of political espionage to the boardrooms of corporate offices and police surveillance operations. Recognizing the prevalence of electronic eavesdropping devices and their threat to privacy, the United States Congress passed the Electronic Communication Privacy Act in 1986, which made bugging illegal. Nonetheless, the use of eavesdropping devices and detectors is widespread in the intelligence

and business communities. One estimate places the annual sales of such devices in the United States alone at $888 million.

FURTHER READING:

BOOKS:

Shannon, Michel L. *Bug Book: Everything You Ever Wanted To Know About Electronic Eavesdropping…But Were Afraid To Ask.* Boulder, CO: Paladin Press, 2000.

Shannon, Michel L. *Don't Bug Me: The Latest High-Tech Spy Methods.* Boulder, CO: Paladin Press, 2002.

SEE ALSO

Codes and Ciphers
Computer Hackers
Internet Surveillance

Burn Box.

SEE *Document Destruction.*

Bush Administration (1989–1993), United States National Security Policy

CARYN E. NEUMANN

The administration of President George H. W. Bush confronted the most fundamental changes in the national security environment since the onset of the Cold War in the 1940s. The collapse of the Soviet Union and the disintegration of the Soviet empire removed the threat of communism that had long determined the direction of security efforts. To respond to this changed environment, Bush reduced the size of the military, shifted resources to the war on drugs, and pursued a new world order that included access to the oil-rich Persian Gulf states. This last goal made imperative the removal of Iraqi forces from Kuwait after it was invaded by Iraq, and resulted in the U.S. coalition-led Persian Gulf War with Iraq.

Bush, a former director of the Central Intelligence Agency, entered the White House after serving as vice president to Ronald Reagan. His approval of Reagan's security policies meant that he would largely continue them as president. The appointment of General Brent Scowcroft, National Security Adviser during the Ford administration, brought deep experience to the National Security Council (NSC) leadership. James Baker headed the State Department. The Department of State and the NSC worked harmoniously, with the jealous guarding of territory that had marked earlier administrations notably absent from this administration.

Reagan had issued a 1986 directive that characterized illegal drugs as a national security threat. The Bush administration expanded this initiative in 1989 with National Security Directive (NSD) 18. This two-part NSD designated the Department of Defense as the lead agency for the detection and monitoring of the aerial and maritime transit of illegal drugs into the country. While there are few specifics in the document, implementation of the directive almost certainly included increased use of intelligence resources, specifically more extensive use of U.S. reconnaissance satellites to locate coca-growing laboratories, communication intercepts to identify drug-smuggling planes entering the country, and other efforts to help monitor the communications of major drug cartel leaders. The second part of the NSD, named the "Andean Initiative", called for foreign aid for Columbia, Bolivia, and Peru with most of the assistance coming in the form of military equipment, such as helicopters, patrol boats and ammunition. The NSD also included such intelligence aid as radars, electronic sensors, secure communications equipment, and computers to store and retrieve information about drug traffickers.

Along with freeing resources for the war on drugs, the end of the Cold War also brought a renewed emphasis on arms control. The collapse of the Soviet system had left a considerable amount of military hardware in Europe and Bush saw arms control as a way of reducing the risks associated with this weaponry. The Conventional Forces Europe (CFE) agreement in 1990 covered the area from the Atlantic Ocean to the Urals. The North Atlantic Treaty Organization (NATO) forces and the recently Soviet-aligned divisions of the Warsaw Treaty Organization (WTO) were limited to 20,000 tanks; 30,000 armored combat vehicles; 20,000 artillery pieces; 2,000 helicopters; and 6,800 combat aircraft. These figures meant marginal cuts for NATO countries, but substantial cuts for WTO states. The result was parity in conventional military forces. CFE served as a major symbol of the end of the Cold War by speeding the demilitarization of Europe.

The dependency of the United States upon oil made access to the Persian Gulf a vital matter of national security. In NSD 26, Bush ordered federal agencies to expand political and economic ties with the Saddam Hussein regime of Iraq to ensure the continued friendliness of the dictator. This 1989 directive led to U.S. government loan guarantees that enabled Iraq to purchase vital foodstuffs on credit and divert hard currency reserves to finance a massive arms buildup. In 1990, Iraq used these arms to support an invasion of Kuwait. The resulting Persian Gulf War succeeded in freeing Kuwait from Iraq's grasp, but U.S. national security interests were damaged in the long term by allowing Hussein to remain in power.

FURTHER READING:

BOOKS:

Williams, Phil and Dilys M. Hill, eds. *The Bush Presidency: Triumphs and Adversities.* New York: St. Martin's Press, 1994.

ELECTRONIC:

Digital National Security Archive. "Presidential Directives on National Security from Truman to Clinton." <http://nsarchive.chadwyck.com/pdessayx.htm> (April 25, 2003).

SEE ALSO

Cold War (1972–1989): The Collapse of the Soviet Union
National Security Strategy, United States
NATO (North Atlantic Treaty Organization)
NSC (National Security Council)
Persian Gulf War

Bush Administration (2001–), United States National Security Policy

CARYN E. NEUMANN

George W. Bush, transformed the national security system of the United States to combat the threat of global terrorism. After the terrorist attacks of September 11, 2001, Bush faced the likelihood of a repeat attack with the knowledge that terrorism could not be effectively addressed through traditional defensive strategies. Accordingly, the administration developed a homeland security

Former U.S. CIA Director Robert Gates, left, visits with former Russian President Boris Yeltsin, second from left, at the Kremlin during the first trip to Moscow by the head of the U.S. intelligence agency in 1992. Also shown are Victor Barannikov, right, former Minister of Security, and Yvgeny Primakov, second from right, former head of the Russian Foreign Intelligence Service, the successor to the KGB. AP/WIDE WORLD PHOTOS.

President Bush meets with his National Security Council in the White House situation room in October, 2001. Clockwise, from center are: White House Chief of Staff Andrew Card, Vice president Dick Cheney, President Bush, Secretary of State Colin Powell, Defense Secretary Donald Rumsfeld, and National Security Advisor Condoleeza Rice. AP/WIDE WORLD PHOTOS.

system and advanced a new doctrine that took into account the shadowy nature of terrorism. With this theory of pre-emption, Bush argued that the U.S. possessed the right and the moral responsibility to launch preventive strikes against states that posed a danger to national security even when that danger was not imminent. This doctrine led to the U.S. led attack upon Iraq, Operation Iraqi Freedom, in 2003.

Bush, a past governor of Texas, took office with little experience in foreign affairs. Nine months into his presidency, the terrorist attacks of September 11, 2001, revealed shortcomings in national security. Simply, the major institutions of American national security were designed during the Cold War to meet the requirements of that era and failed to adequately protect the U.S. from the twenty-first century threat of global terrorism. To meet the challenge of retooling the security system, Bush relied upon Donald Rumsfeld as Secretary of Defense, Colin Powell as Secretary of State, and Condoleezza Rice as National Security Advisor.

In order to address terrorism, the Bush administration changed the way that security threats were identified and monitored. Designed with the aim of collecting information about the massive and immobile Soviet bloc, the intelligence community now had to follow a far more complex and elusive set of targets. The administration strengthened intelligence warning and analysis to provide integrated threat assessments for national and homeland security. Through such new creations as the Terrorist Threat Integration Center and the use of such older networks as Interpol, the U.S. disrupted terrorist networks, removed key leaders, and arrested more than 3,000 terrorists around the world. The new Department of Homeland Security intensified security at borders and ports of entry through measures that included posting more than 50,000 federal screeners in airports.

Afghanistan had provided a safe base for al-Qaeda terrorists to plot against the U.S. and this country became the first target of an anti-terrorism strike. The 2001 war in Afghanistan aimed to capture al-Qaeda leader Osama bin Laden, remove a government that had permitted the growth of terrorism, and establish a democratic system. While the government quickly collapsed and the terrorist support network appears to be shattered, bin Laden, as of June, 2003, has not been captured. Significant numbers of U.S. military forces remain in the country to continue the search for terrorists and to serve as peacekeepers.

In the months after the Afghanistan attack, the Bush administration honed a doctrine of pre-emption that justified military aggression as the prevention of evildoing. Bush sought to persuade other nations to adopt this doctrine as part of an effort to protect the U.S. and its allies from attack by strengthening alliances to defeat global terrorism. The refusal of many other countries to cooperate for reasons that included nationalism and anger at perceived American arrogance has meant that some of these alliances have not formed. The 2003 war upon Iraq became an Anglo-American project to prevent Saddam Hussein from employing weapons of mass destruction and supporting terrorism.

Under Bush, the United States possesses the strongest military that the world has ever known. The global arms race is over, with no nation able to match the U.S. in naval, air, missile, or tank strength and only China offering a larger ground force. The ability of a large military to ensure national security, however, is not certain. The historic hostility of Arabs to Western intervention may complicate efforts to stabilize the Middle East and establish a model of democracy in Iraq and Afghanistan. With the perspective of history, therefore, the accomplishments of the Bush administration can be fully evaluated.

FURTHER READING:

ELECTRONIC:

White House. "National Security." <http://www.whitehouse.gov/response/index.html> (April 27, 2003).

SEE ALSO

Domestic Intelligence
Enduring Freedom, Operation
Homeland Security, United States Department
Interpol (International Criminal Police Organization)
Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)
Iraqi Freedom, Operation (2003 War Against Iraq)
Terrorist Threat Integration Center
United States, Counter-terrorism Policy
World Trade Center, 2001 Terrorist Attack

C

Cambodian Freedom Fighters (CFF)

Cambodian Freedom Fighters (CFF) also operates as, or is known as, the Cholana Kangtoap Serei Cheat Kampouchea.

CFF emerged in November, 1998, in the wake of political violence that saw many influential Cambodian leaders flee and the Cambodian People's Party assume power. With an avowed aim of overthrowing the government, the group is led by a Cambodian-American, a former member of the opposition Sam Rainsy Party, and its membership includes Cambodian-Americans based in Thailand and the United States and former soldiers from the separatist Khmer Rouge, Royal Cambodian Armed Forces, and various political factions. The CFF has on at least one occasion attacked government facilities and planned other bombing attacks. In late November, 2000, the CFF staged an attack on several government installations, during which at least eight persons died and more than a dozen were wounded, including civilians. The group's leaders claimed responsibility for the attack. Following a trial of 32 CFF members arrested for the attack, five received life sentences, 25 received lesser jail terms, and two were acquitted. In April, 1999, five other members of the CFF were arrested for plotting to blow up a fuel depot outside Phnom Penh with antitank weapons.

CFF's exact strength is unknown, but totals probably never has exceeded 100 armed fighters. CFF operates in Northeastern Cambodia near the Thai border. Its U.S. based leadership collects funds from the Cambodian-American community.

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual Reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Cambridge University Spy Ring

ADRIENNE WILMOTH LERNER

The Cambridge spy ring was a group of British young men recruited as Soviet spies in the 1930s. The group was known in Britain as the Cambridge spy ring, after the University where the men attended classes and were recruited for espionage. In the Soviet Union, the group was known as the "magnificent five." The Cambridge spy ring infiltrated the highest level of the British government, including MI-5, MI-6, the Foreign Office, and the War Ministry. During their career, the group betrayed some of

Kim Philby (right) shown here following the shelling of his vehicle during the Spanish Civil War, was a member of the Communist Party while at Cambridge University, where he recruited and led a ring of spies for the Soviet Union. ©BETTMANN/CORBIS.

Britain's most guarded secrets to the Soviet Union. The group was led by master-spy, Harold "Kim" Philby.

Soviet agents planned to expand their espionage network in Britain as early as 1928. Though several spies operated successfully in Britain at the time the Cambridge ring was founded, Soviet intelligence officials realized that it was necessary to recruit people who had access to the upper echelons of British society, who could land prestigious civil service jobs, to infiltrate the highest levels of British government. To that end, Soviet agents began recruiting young men at Oxford University and Cambridge University into service. They looked for students who held genuine communist or socialist political sympathies, and who possessed the necessary social pedigree to obtain the confidence of high level peers. From Cambridge, Soviet agents persuaded Kim Philby, Guy Burgess, Donald Maclean, Anthony Blunt, and John Carincross into service for the Soviet Union.

Kim Philby. After graduating Cambridge, Kim Philby (1912–1988) failed to land a position in the Foreign Service. He worked briefly at the *London Times*. Philby proved his worth to Soviet intelligence during this time by smuggling agents and communist supporters out of fascist Austria. He then traveled to Spain as a war correspondent, covering the Spanish Civil War. When World War II began, Philby returned to Britain, finally securing a job with British Intelligence.

From 1944 to 1946, Philby served as director of anti-Soviet counterintelligence for British Intelligence. The position guaranteed his access to top-level British military, intelligence, and government secrets, including World War II battle plans and Cold War agreements between Britain and the United States to thwart the spread of communism is Europe.

In 1949, Philby was stationed in Washington, D.C. as part of an Anglo-American intelligence cooperative operation. For three years, Philby had access to CIA and FBI files. More damaging, he received briefings of Venona Project intercepts, providing him with the ability to inform Moscow of United States efforts to break Soviet communications codes. The Venona intercepts also allowed Philby to monitor American knowledge of Soviet spy networks within

the United States, and report defections to Soviet authorities. After returning to London in 1951, Philby continued his career as a mole (double agent) for over a decade.

Guy Burgess. Guy Burgess (1910–1963) worked as a radio correspondent for the BBC from 1936 through 1944. During World War II, Burgess was also employed by British intelligence agency, MI5. Burgess was somewhat successful in transmitting messages to Soviet agents via radio broadcasts and smuggled several key documents to Moscow. Burgess stole some of the most sensitive information in the career of the Cambridge spy ring. While working for MI-5 in London, he smuggled copies of documents relating to nuclear weapons development. He also informed the Soviet government of United States and British plants to create the North Atlantic Treaty Organization (NATO), a European-American military alliance system.

In 1950, Kim Philby requested that Burgess be assigned to the Washington, D.C., bureau of the British Foreign Office. Burgess worked as Philby's assistant until he came under the suspicion of British intelligence. Philby then sent Burgess back to London, presumably to avoid suspicion upon himself.

Donald Maclean. The third member of the Cambridge spy ring, Donald Maclean (1913–1983), worked closely with Burgess. After graduating from Cambridge, Maclean worked in diplomatic service. In 1950, he became head of the Foreign Office's American Department.

While working at the British Embassy in Washington, D.C., Maclean was the main source of information regarding United States and British communications, advising Moscow on Anglo-American policy. In 1951, Maclean was tapped to be the British representative on the American-British-Canadian council on the sharing of atomic secrets. With Burgess, Maclean used his position to funnel highly classified atomic secrets to Soviet military intelligence. The two men did not steal technical information about the atomic bomb, but did provide Moscow with accurate assessments of the American atomic arsenal, production capabilities, and nuclear resources.

The Defections of Maclean, Burgess, and Philby. In 1949, Robert Lamphere, an FBI counterintelligence agent working with the Venona project, discovered that someone was sending telegraph messages from the British Embassy in Washington, D.C. to Moscow. The sender, under the codename "Homer" was later identified as Maclean. Philby, while working in Washington, learned of the FBI investigation of Maclean. Philby then devised a plan to warn Maclean of his impending exposure, while protecting himself and the rest the Cambridge spies.

Philby and Burgess agreed that Burgess would endeavor to be recalled by the Foreign Office to London, where he could arrange to meet with, and warn Maclean without arousing suspicion. Since Burgess had lived in the Philby family home while assigned to his Washington, D.C. post, Philby cautioned Burgess not to attempt to defect to the Soviet Union with Maclean should he decide to escape. Burgess agreed to escort Maclean to safety, but to return to Britain to avoid drawing attention to other members of the Cambridge ring.

Days before he was scheduled to be questioned by British and American intelligence officials, Maclean, with Burgess, escaped to France. Once on the continent, they made their way to Moscow via a network of KGB safe houses. Soviet authorities insisted that Burgess defect with Maclean. Burgess lived in Russia until his death in 1963, though he reportedly did not attempt to further participate in the Soviet government. Maclean learned Russian and spent his remaining years working as an economic analyst and advisor on Western policy.

When British intelligence learned of Burgess and Maclean's defection, and acknowledged their roles in Soviet espionage operations, Philby was immediately placed under suspicion as a possible Soviet mole. In 1955, he deftly weathered MI-5 and MI-6 interrogation. After being released from his job at MI-6, he later was permitted to return to the civil service. Philby continued to act as a mole for Soviet intelligence for several more years, though he had limited access to top-secret materials.

In 1963, under renewed suspicion of espionage, Philby took a position as Foreign Office correspondent in Beirut, Lebanon. Later that year, a Soviet intelligence agent defected to the West. While being interrogated by Australian and British intelligence in Sydney, the defector named Philby as one of the Soviet's greatest human intelligence assets. Philby quickly defected to the Soviet Union, where he spent the rest of his life. He worked with the KGB, training spies for operation in the West. Cambridge spy ring member Anthony Blunt aided Philby's final escape.

Anthony Blunt. Though not the most active spy in the Cambridge ring, Anthony Blunt (1907–1983) aided Soviet agents' recruitment efforts at Cambridge. Blunt supplied the names of possible moles, and regularly attended communist political meetings in search of young recruits.

Blunt received degrees in history and art history from Cambridge. At the outbreak of World War II, Blunt went to work for British Intelligence. Blunt lacked the high-level security clearances possessed by other Cambridge spy ring members, however he was successful in smuggling photographs of documents regarding British troop locations and counterintelligence reports to his KGB contact, Yuri Modin. Blunt also provided information to Soviet military intelligence regarding British code breaking efforts against the Germans. After the war, he cultivated a reputation as a leading national academic. Socially, he often refused to comment on national and international political matters, leading colleagues to believe he had grown disillusioned and possessed little interest in the subject.

Though Blunt did conduct espionage for the Soviets after World War II, a majority of his operations was conducted during wartime. He was the first member of the Cambridge spy ring to retire from service, returning to his career as an art historian and museum curator, and the only member to remain in Britain.

In 1964, an American, Michael Straight, who had attended Cambridge with Blunt told FBI and MI-5 agents that Blunt had tried to recruit him to spy for the Soviet Union. After being exposed as a member of the Cambridge spy ring, Blunt provided MI-5 and MI-6 with some information regarding his past operations and associates, most of whom had by 1964 died or defected to Russia and were out of reach of British prosecutors. In exchange, Blunt was not tried for his offenses. He continued his career in art history, managing the Courtauld Collection until his retirement. His career as a spy for the Soviet Union was exposed to the public by the government officials under Prime Minister Margaret Thatcher in 1979. He was stripped of his knighthood and academic honors. By the time of his exposure, the public was already well acquainted with the stories of agents Maclean, Burgess, and Philby. Blunt was then presumed to be the final member of the infamous Cambridge spy ring.

John Carincross. In 1990, a fifth member of the Cambridge ring was publicly identified. John Carincross (1913–1995) worked with Maclean in the Foreign Office before being transferred to the offices of the Treasury in 1940. Through his connections with British intelligence and the Treasury, Carincross obtained a significant amount of information about the British Cipher School and code-breaking program at Bletchley Park. Heeding Carincross's warnings, Soviet intelligence changed their diplomatic, military, and intelligence codes before the end of World War II. Bletchley Park cryptologists thus, had to begin anew with efforts to break the Soviet code.

Carincross also leaked information about British and American nuclear programs. Analysts estimate that the Soviet Union was able to develop nuclear weapons three years faster, and millions of dollars cheaper, with the aid of intelligence from moles such as the Cambridge spies.

Similar to Blunt, when Carincross was exposed, he provided information about Soviet espionage networks to British intelligence. While the ultimate usefulness of such information remains the subject of debate, he was nonetheless granted some level of immunity from prosecution. When his career as a Soviet spy was made public, he left England for France.

The legacy of the Cambridge University spy ring. The actual damage to British and American national security caused by the activities of the Cambridge spy ring may never be fully assessed. Even with the declassification of reports and archives in the former Soviet Union, a comprehensive account of secrets stolen by the ring remains illusive. The Cambridge spies did have a profound short-term influence on British and American intelligence operations. Both nations stepped up counterespionage efforts to root out similar moles in government agencies. Competitive tensions between MI-5 and MI-6 in Britain, and the CIA and FBI in the United States, were greatly exacerbated after Kim Philby's defection. The agencies blamed each other for not conducting adequate background checks on British personnel sent to work on joint Anglo-American intelligence operations, and for not discovering the Soviet spy network in time to prevent the loss of substantial information. The incident humbled both the British and American intelligence communities, and even fostered mistrust between the two nations. For a decade, Britain and American intelligence forces shared only limited information.

Relations between the British and American intelligence communities gradually became more supportive, eventually returning to the cooperative status enjoyed in the early Cold War years. When the Cold War ended with the fall of the Soviet Union, the extent to which rival nations infiltrated each other's governments with spy networks was made apparent. Declassification of documents relating to Cold War espionage proved the Cambridge spy ring was far from alone in its operations.

The Cambridge ring gained its notoriety not only from its exploits of espionage, but also because of it seemingly unlikely cast of characters—upper class, well-schooled, British citizens who fit well into the "old boys" network that dominated the British civil service. Their social credibility helped them gain access to the nation's top secrets. Further complicating the legacy of the spy ring was the effectiveness with which the group operated. Philby, Burgess, Blunt, Maclean, and Carincross spent years building reputations as loyal British citizens and staunch anti-communists before beginning active espionage during World War II. With the exception of one payment made to Kim Philby when his family was in dire financial need, none of the Cambridge spies demanded compensation for their services to Soviet intelligence. The group thus seemed ideologically loyal to communism, as opposed to performing espionage for personal gain.

Regardless of motive or the ultimate success of their operations, the Cambridge spies are some of the most infamous figures of British intelligence. Subsequent incidences of British citizens in the employ of Soviet intelligence stealing sensitive information from high-level officials further embarrassed British intelligence. In 1963, the Profumo Affair exploded to public attention when intelligence agents and journalists learned that the mistress of a British cabinet minister was a Soviet informant. The "Sex for Secrets" scandal helped bring down the administration of Prime Minister Harold Macmillan. Ironically, Macmillan, while serving as Foreign Secretary, cleared Kim Philby of wrong-doing eight years before his ultimate defection.

Labeled traitors in Britain and America, the "magnificent five" enjoyed fame in the Soviet Union. When Kim

Philby died there in 1988, he was buried in Moscow with full state honors.

FURTHER READING:

BOOKS:

Boyle, Andrew. *The Climate of Treason: Five Who Spied for Russia.* London: Hutchinson, 1979.

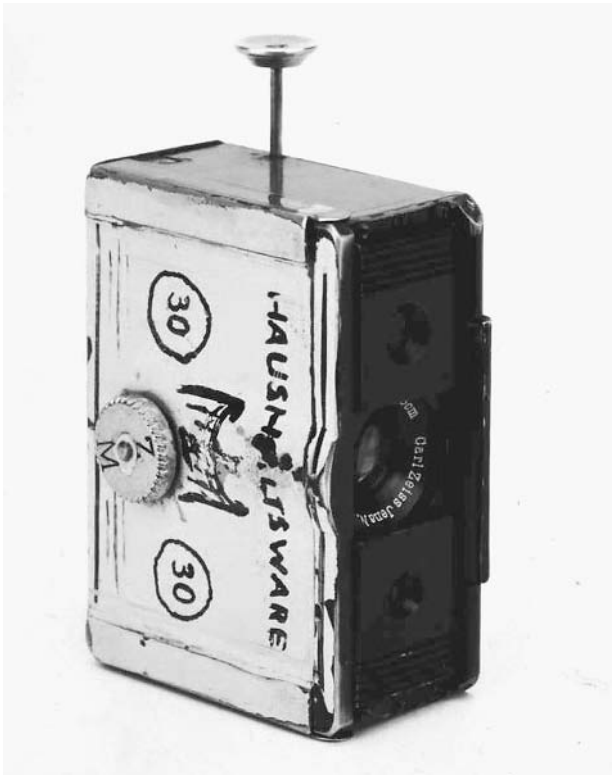
Brown, Anthony Cave. *Treason in the Blood.* Boston: Houghton Mifflin, 1994.

PERIODICALS:

Teagarden, Ernest M. "The Cambridge Five: The End of the Cold War Brings Forth Some Views from the Other Side." *American Intelligence Journal* 18, no. 1/2 (1998): 63–68.

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*
MI5 (British Security Service)
MI6 (British Secret Intelligence Service)
OSS (United States Office of Strategic Services)
Soviet Union (USSR), Intelligence and Security
Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom



A circa 1938 top secret spy camera made to resemble a contemporary German matchbox. AP/WIDE WORLD PHOTOS.

Cameras

JUDSON KNIGHT

Cameras have a number of applications in the world of security and espionage. Cameras can be used for conducting surveillance, for instance, an activity that may require neither proximity to the subject nor even a human operator. More intriguing and wide-ranging, however, are the uses of the camera in up-close work by intelligence operatives. Such situations require human ingenuity, not only for designing effective photographic equipment, but also for concealing the camera and its operations. Intelligence personnel have used cameras to photograph individuals and their activities, as well as buildings and installations. A significant subcategory of espionage photography involves the copying of documents, often with special cameras, although sometimes with ordinary equipment.

Background

A camera functions by focusing light through a lens onto a surface coated with light-sensitive chemicals. The concept of the camera dates back to the Renaissance idea of the camera obscura, a small, dark chamber into which light was permitted only through pinholes. During the early nineteenth century, inventors perfected the camera obscura to make the prototype of the modern camera, but early photography was a cumbersome affair characterized by large, boxy cameras and slow exposures. It is for this reason that most photographs from the American Civil War—the first conflict chronicled in depth by photojournalists—tend to be stills rather than action shots.

Only in the twentieth century was it possible to build cameras useful for work in espionage. Particularly after World War II, the number of possible camera types suited either to speed, concealment, range, or photographic resolution proliferated along with the many uses to which espionage and security organizations applied them. Today, the principal uses for cameras in the security and espionage context are copying documents, capturing activities of individuals at a close range, or conducting surveillance on large groups over large areas from a distance.

The last of these activities, while certainly a significant part of espionage and security operations, typically lacks the tactile qualities popularly associated with the use of cameras by spies. Surveillance aircraft such as the U–2 and SR–71 Blackbird, as well as satellites of the KH or "keyhole" series, carried sophisticated cameras for long-range photography of missile installations, weapons factories, and other facilities. In such a situation, the human

operator of the camera plays a lesser role than the technology behind its operation, and that of the craft that keeps it aloft many thousands of feet or miles above Earth's surface.

Surveillance cameras in daily life. Similarly, with close-range surveillance and security cameras that operate automatically, the human operator is of little significance. Still, there is a great deal of immediacy and intimate contact between camera and subject—especially because the unwitting subject seldom knows the degree to which he or she is under surveillance. In modern times, Americans have become accustomed to ordinary security cameras in stores and other businesses, particularly those whose contents have high monetary value. According to the Security Industry Association, by 2003, there were some two-million closed-circuit television systems in operation, most of them operated by private businesses for security purposes, in the United States. CCS International, a security company, estimated that the average person in Manhattan was photographed 73 to 75 times a day. Often this happened when the individual was not aware of the surveillance, even when the camera itself was in plain view. That camera might well be a dummy, with the real camera photographing an individual's activities from another angle.

Although civil libertarians protested this proliferation of security cameras, they are unlikely to disappear any time soon. J. P. Freeman, a firm that performs marketing research for the security industry, estimated in 2002 that the market for digital video surveillance equipment was growing at the rate of fifteen percent per year, particularly noticeable gains during the early twenty-first century recession. Additionally, in the heightened climate of awareness that followed the terrorist attacks of September 11, 2001, Americans were less likely than ever to react to potential violations of privacy.

In communist Eastern Europe. If surveillance cameras are ubiquitous in a democratic nation such as the United States, they are pervasive in closed societies—assuming that the nation possesses the financial means to watch its citizens with electronic eyes. Certainly this was true in East Germany, by far the most prosperous nation in the history of communism, where per-capita incomes in the 1980s ran higher than those of non-communist Greece. The East German Stasi (short for das Ministerium für Staatssicherheit or Ministry of State Security) frequently monitored patrons of public lodgings through the use of a Czech-made surveillance camera with a German T1–340 lens. Made to fit into a special cylinder built into the hotel wall, the camera could be operated using a remote shutter release. This piece of equipment, used to spy on hotel patrons, was a variety of the German robot camera developed prior to World War II.

Surveillance Cameras in Espionage

First used by the Nazis in 1934, the robot could snap multiple exposures without requiring manual winding. Originally used by the German air force to rapidly photograph the destruction of targets, it later became a favorite of Nazi intelligence services. The designs of the Nazi era culminated in the Star 50, which could snap 50 exposures in rapid succession. After the war, intelligence agents on either side of the Iron Curtain used robot cameras.

Made to be concealed and, if necessary, operated from a remote location, the robot was ideal for surveillance. Specific varieties of Star 50 were designed to be hidden in handbags, while the robot Star II was flat enough to fit in a special belt concealed by a trench coat. A false coat button covered the camera lens, and the manufacturers provided an entire matching set of buttons so that the user could replace those already on the trench coat if they did not match the false one. The robot Star II could also fit neatly into a briefcase.

The Soviet KGB developed their own variation on the robot, the F21, in 1948. Small—about the size of a hotel soap bar—and quiet, the F21 was ideal for concealment. At various times, Soviet designers adapted the F21 to hide it in belt buckles, jackets, umbrellas, and even camera cases. In the latter instance, the spy, posing as a tourist, would carry the camera case open and slung around the neck. The visible camera was a dummy; mounted on the side of the case was an F21 that took pictures at a 90-degree angle to the lens of the dummy camera.

Some other significant surveillance models in the history of Cold War espionage include the British Mark 3 automatic camera. Developed in the 1950s and still in use during the 1990s, the Mark 3 had a chamber so large it could hold enough film for 250 35mm exposures. Sometimes intelligence operatives needed moving pictures rather than stills, and for this, KGB relied on a movie version of the F21, developed in the 1960s. The camera was made to be hidden in a coat, using the false button technique applied with the robot camera.

Copy cameras. To copy documents, intelligence services required special cameras. An ordinary camera could theoretically be used, but would have difficulty in obtaining readable images. A much better option is to use a camera and accessories specially made for that purpose. A camera made specifically for copying documents has a high degree of photographic resolution, and is constructed in such a way as to be operated with a remote shutter release in order to avoid shaking the camera. Usually, the equipment would also include a stand of some kind that would both keep the camera steady and hold it fixed in place some distance from the documents being copied. Finally, because copying by an intelligence agent would most likely be a clandestine activity, it would be necessary to house all this equipment in a package that could easily be concealed.

One camera that fit the bill handsomely was built for the StB, the intelligence service of communist Czechoslovakia. Made to fit into an unobtrusive-looking wooden box, the kit included a Meopta copy camera, lights, a power plug, and a four-legged stand. The camera sat atop the stand, pointed downward. By pressing a button on a shutter release cable, the operator could photograph documents, which were illuminated by light bulbs fitted into housings at the base of the stand.

Both American and Soviet intelligence services used kits that resembled miniature copier machines. The American model was made to fit into an attaché case, while the Soviets' Yelka C–64 copy camera had the appearance of a thick book and, therefore, was unlikely to raise immediate suspicions.

Particularly ingenious was the Soviet rollover camera, disguised as a notebook. The undercover agent would regularly carry a real notebook to work, and use it often. Then, when it came time to make copies of documents, the agent would bring the rollover camera notebook, which was identical in appearance to the real notebook. In order to photograph a document, the agent would run the spine of the notebook carefully back and forth across the documents to be copied. Inside the spine were wheels that activated the camera, which was hidden, along with a battery-powered light source, inside the notebook.

Working without a copy camera. Perhaps the greatest resourcefulness of all was required for those situations in which the agent had no special equipment other than an ordinary camera. Victor Ostrovsky, of Israel's Mossad, developed a method for copying that used only a standard camera with a shutter release, a few thick books, and a couple of lamps. The document would be taped to the front a book, which would be set standing on end, facing the camera. The latter would be placed atop one or more books lying flat, and fixed in place with an ordinary adhesive, such as chewing gum. On either side, desk lamps would provide concentrated lighting.

Another setup could be used when the agent needed to copy large amounts of documents, but could use only a camera and standard office equipment. Books would be stacked in two towers of equal height—perhaps 18 inches or so—with enough space between them to lay a document flat. Bridging the tops of the "towers" would be two parallel rulers, spaced almost the width of an ordinary 35mm camera. The camera would be taped to the rulers, and lamps placed on either side of the document. Then, documents could be run through one after the other, and a high volume of information recorded in a short time.

FURTHER READING:

Babington-Smith, Constance. *Evidence in Camera: The Story of Photographic Intelligence in World War II.* Newton Abbott, England: David and Charles, 1974.

Melton, H. Keith. *The Ultimate Spy Book.* New York: DK Publishing, 1996.

Murphy, Dean E. "As Security Cameras Sprout, Someone's Always Watching." *New York Times* (September 29, 2002).

Siljander, Raymond P. *Applied Surveillance Photography.* Springfield, IL: Thomas, 1975.

SEE ALSO

Cameras, Miniature
Photo Alteration
Photographic Resolution
Privacy: Legal and Ethical Issues

Cameras, Miniature

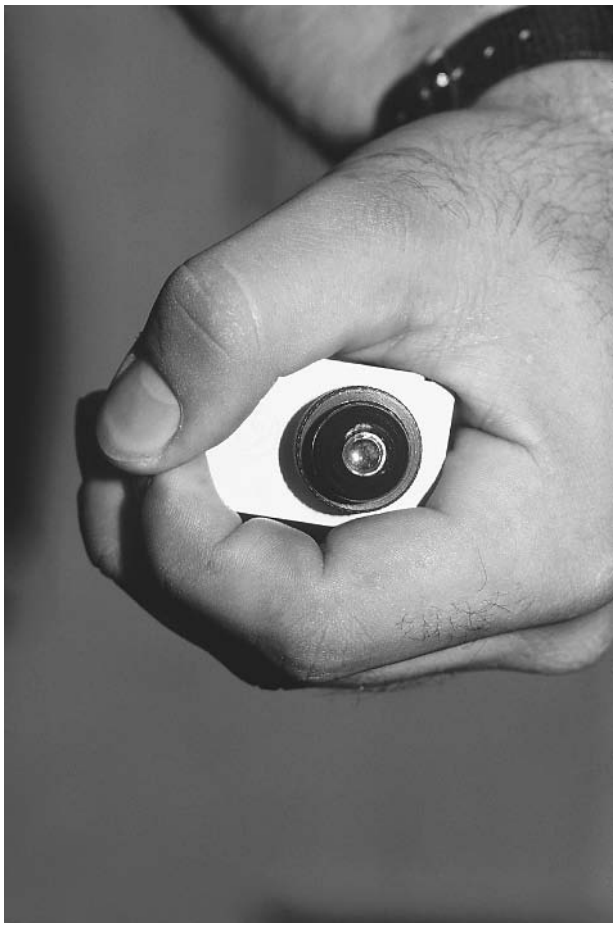
JUDSON KNIGHT

Intelligence operatives frequently have a need for cameras that can be concealed, and while small size is not the only means to protect a camera from detection, it is certainly a significant one. Hence the value of small cameras such as the Minox, which could easily fit into the palm of a person's hand, as well as extremely small models no bigger than a thumb. During the years of World War II and the early Cold War, an age when cigarette-smoking was common, many spy cameras were designed to look like lighters, matchboxes, or cigarette packs. Some were made to photograph documents, others to photograph persons and buildings, while a special variety of cameras was applied to the copying of miniaturized photographic images via microdots.

Concealment and Miniature Cameras

Concealment is often a concern for intelligence operatives using cameras. Sometimes a camera larger than miniature can still be concealed—even when in plain view. For example, the lens cap may be in place, so that observers would not think the camera was even taking pictures, but in reality the operator could be shooting exposures through inconspicuous holes in the lens cap, using a concealed shutter release. Or the apparent lens of the camera might be a dummy, and the real lens could be off to the side, at a 90-degree angle to the apparent lens.

The Soviet Tokya 58-M, while not miniature, was smaller than a pack of cigarettes, and made to be concealed behind the user's necktie. The agent would wear it strapped to his body, with the lens concealed behind a special tie pin. In order to ward off suspicion, the agent would make it a point to be seen often wearing an identical tie pin; then, when it was necessary to discreetly snap photographs, he could put the camera into place. The camera itself snapped pictures in almost complete silence, such that the sounds of a dinner party or a busy office



An Israeli miniature video camera of the 1980s. ©JEFFREY L. ROTMAN/CORBIS.

would be enough to conceal what little noise it made while operating.

Despite the variety of techniques for concealing cameras that are of ordinary size or very nearly so, in some instances it is preferable for an intelligence operative to carry a miniature camera. Some of these are small, and some very small: therefore it is common to speak of "miniature" and "subminiature" cameras. The distinction is a subjective one, however, and in both cases, the camera in question is so small that it must be constructed using principles somewhat different from those of a typical consumer camera.

Design and Optics of Miniature Cameras

A miniature spy camera is almost completely lacking in the "frills" that one might expect from a camera built for ordinary use. Because of the size (and the need, in many cases, to prevent the camera from looking like a camera), there is almost never any viewfinder. The user must therefore be highly experienced at photography, so as to know when an image is in focus without being able to actually see how it looks through the lens.

It is unlikely that a miniature camera, particularly those of the pre-digital cold-war era, would use color film, since this would simply constitute another frill and hence a complication in obtaining clear images. The film itself was usually smaller than 35mm: sizes ranging from 16mm all the way down to 9.5mm or smaller are typical of miniature and subminiature cameras.

Lenses and light. Virtually all cameras have at least one glass lens, and one with a zoom or telephoto lens typically has three: front and rear convex lenses, with a concave one in between. Though zoom lenses clearly have an application in the world of espionage, miniature and subminiature cameras are usually for photographing images at close range. Typically they would have only a single lens, perhaps with a coating to reduce reflections or glare.

An unusual example of miniature camera optics was the Soviet pinhole camera from the 1980s. One of the Soviet strengths in technology was the use of extremely simple, sometimes almost primitive, design to create extremely functional equipment that often outperformed its more complex and temperamental Western counterparts. Such was the case with the tiny camera, which was actually based on principles pioneered in the nineteenth century.

In place of lenses, a pinhole camera uses tiny apertures, or openings, so small that they are known as pinholes. The value of a lens lies in its ability to focus and thus photograph distant objects or ones close by, depending on the settings. By contrast, the value of a pinhole camera is precisely the fact that it does not have lenses, and therefore can produce images of distant and nearby images equally well.

Neither the faraway nor the closeup images produced by a pinhole camera have a very high degree of photographic resolution, and a photograph taken using this nineteenth-century technology will probably look like an old daguerreotype. But where clarity of image is not as important as versatility, quietness, and simplicity of design, a camera such as the Soviet model—so small it could be worn unobtrusively on a key chain—would be ideal.

The Minox camera. One of the great triumphs of miniature and ultraminiature design, applied for espionage work on both sides during the Cold War, was the Minox subminiature camera. Originally produced in 1938, it was the first significant and widely used miniature camera of the twentieth century. Small and flat, it could easily be concealed in the hand, yet for its size, it was exceptional in both its speed and the quality of the pictures it produced.

The designer of the Minox was Walter Zapp, a Latvian engineer who set out, not to make a tool of espionage, but rather to produce a camera that could be easily portable yet capable of producing photographs both quickly and

accurately. A Baltic German living in the Latvian capital of Riga, Zapp began producing his camera just before the Soviets annexed his country as an outgrowth of the 1939 non-aggression pact with the Nazis. Because of his German heritage, Zapp opted to move to his homeland, but it appears that the Nazis did not make use of his design. Therefore seven years elapsed between the production of the Riga Minox in 1938 and the founding of the Minox GmbH company in Germany. The latter produced more than 1 million cameras in its first half-century, and a 90-year-old Zapp was on hand for the company's 50th anniversary in 1995.

Uses for espionage. In the meantime, the Soviets, having appropriated Minox technology after capturing Riga, began producing their own miniature cameras. Among the Soviet spies associated with the Minox was John A. Walker, Jr., who used one given to him by his KGB handlers for photographing sensitive U.S. Navy and National Security Agency documents. After his arrest, Walker demonstrated for authorities how he used a Minox, along with a measuring chain to ensure that the camera was held a proper and uniform distance from the documents.

Western intelligence also recognized the value of the Minox, and its operatives continued to use them into the 1990s. Popular among both civilians and intelligence operatives was Model B, produced from 1958 to 1972, which was the first Minox with its own built-in light meter. It required no batteries, and therefore could be kept in hiding for many months until it was needed. As time passed, the resolution quality of Minox film improved dramatically, along with the enlargers used to make prints from the minuscule negatives produced by the camera. There were also improvements in the technology of developing film: thanks to a developing tank, it became possible to produce pictures without a darkroom, even in broad daylight.

Other Notable Miniature Cameras

Today miniature and subminiature cameras are available for sale to civilian consumers via the Internet, but once these were virtually the sole province of intelligence services working on either side of the Iron Curtain. Today's designs for consumers—a jealous spouse, or an employer suspicious of employee malfeasance—are typically based on these old cold-war models.

As for the photographic technology utilized by today's espionage services, that information is unavailable to the general public. However, it is a safe guess that the technological gap between the equipment used by intelligence services and that used by amateur photographers is at least as great as it was in the middle of the twentieth century.

Wristwatch cameras. An example of a civilian product with a design related to that of a camera used in espionage is the Tessina, still produced and sold by Concava SA of Switzerland. Unlike most tiny cameras, the Tessina, which is made to fit on a watchband, uses 35mm film, though this is loaded into special cassettes to make frames that measure just 14 x 21 mm. The Tessina was reportedly designed by Rudolph Steineck, whose Steineck ABC wristwatch camera is a classic of compactness in the service of espionage.

First produced in 1948, the Steineck ABC resembled a wristwatch, though it was not disguised behind a watch face. In fact, nothing about the Steineck looked like a watch except the size and the fact that it was attached to a watchband. Yet it bore such a close resemblance to a watch from a distance that it seldom attracted attention as a camera. The Steineck was capable of producing eight exposures, each about 6mm across, on a film disk that measured 25mm (some sources say 24) across.

Cameras disguised as smoking paraphernalia. One variety of Tessina used in the realm of espionage was a 35mm model, the smallest motor-driven camera of its kind in the world, which was designed to fit inside a cigarette pack. The shutter could be pressed from outside the pack, with very small holes on the exterior letting in just enough light to take pictures. The Tessina could shoot up to 10 exposures before it required manual winding.

Ingenious as this Tessina model was, it simply fit inside a cigarette pack. By contrast, the Soviet Kiev 30 16mm model was actually designed to resemble a metal cigarette case, complete with dummy cigarettes. By moving one of the cigarettes, the user advanced the film and snapped pictures through a lens at the side of the pack.

During World War II, Eastman Kodak designed for the Office of Strategic Services a 16mm camera that was as small as a matchbox, and could be disguised as one simply by affixing a matchbox label. The lens opening was on the side, in a small hole on the striking surface, and the shutter release was at the end.

An early example of postwar Japanese technology was the Echo 8 cigarette lighter camera, which first appeared in 1951. It was even more authentic than the Soviet cigarette case or the American matchbox, because the lighter actually worked. In order to photograph the subject, the user simply flipped the top, revealing a viewing port and other equipment for a camera. It was a simple task to light a cigarette while snapping a picture from the side of the lighter. The "8" in its name referred to the 8mm film, made by slicing 16mm film down the middle.

Microdot cameras. Microdots were a specialized application for which certain cameras were used during the Cold War. This was particularly the case during the 1950s and 1960s, though microdots—tiny photographic images that require magnifying to be viewed—have been a fixture of intelligence work since the mid-nineteenth century. Microdots were ideal for passing messages between East and West

Berlin, for instance, a situation in which it was virtually impossible for agents to cross sides and pass documents without attracting attention. Instead, they could simply send mail containing microdots, which were so small that they would, in most instances, evade detection.

The East Germans designed a microdot camera about the size of the end joint on an average man's thumb. It could produce microdots smaller than a typical letter or character in a book. East German designers also created an ingenious microdot viewer that could be concealed in a fountain pen. Additionally, German intelligence services of both the Nazi and communist eras were known for their microdot concealment devices, which included a man's ring used in World War II (with the microdot hidden in a secret chamber atop the ring), as well as a postwar coin designed with a secret chamber.

FURTHER READING:

BOOKS:

Babington-Smith, Constance. *Evidence in Camera: The Story of Photographic Intelligence in World War II.* Newton Abbott, England: David and Charles, 1974.

Melton, H. Keith. *The Ultimate Spy Book.* New York: DK Publishing, 1996.

Pritchard, Michael, and Douglas St. Denny. *Spy Camera: A Century of Detective and Subminiature Cameras.* London: Classic Collection, 1993.

SEE ALSO

Photographic Resolution

Canada, Counter-Terrorism Policy

BRIAN HOYLE

Canada's measures to respond to or prevent terrorist activities have their origin in the October Crisis of 1970. At that time, a minister in the government of the Canadian province of Quebec and the British trade commissioner were kidnapped by members of a radical organization who advocated the separation of Quebec from Canada. The minister, Pierre Laporte, was killed by his captors.

One response of the federal government was to invoke an act of Parliament that temporarily revoked many democratic freedoms of Canadians in the interest of national security. As well, the Royal Canadian Mounted Police (RCMP) began a campaign of investigation and infiltration of the separatist organization and other perceived domestic terrorist organizations.

This counter-terrorism function shifted to the Canadian Security Intelligence Agency (CSIS) upon its establishment in 1984.

In the 1980s and 1990s, terrorism in Canada involved religious extremists (mainly Islamic groups), political activities surrounding the separation of states in India, Sri Lanka, Ireland, and the Middle East, and the activities of groups opposed to abortion, animal rights, and globalization. CSIS and other law enforcement agencies in the country assumed responsibility for the investigation of such incidents and prevention of further domestic violence. A full-scale government counter-terrorism policy did not yet exist.

The September 2001 terrorist attacks on the World Trade Center and the Pentagon in the United States prompted Canada to formulate policies to address the possibilities of terrorist movement through Canada to the U.S. and the presence of terrorist bases of operation in Canada. As well, Canadian officials were concerned that Canada might itself become a target of terrorism.

Canadian counter-terrorism policy involves several federal government departments and agencies. CSIS has assumed a prominent role in its capacity as an intelligence-gathering agency and as an advisor concerning possible national security threats. In the 1990s, some 80% of CSIS resources were devoted to counter-intelligence with only 20% dedicated to counter-terrorism. As of 2002, this ratio is reversed. Public safety has become the priority of CSIS.

The Threat Assessement Unit in the Counter-terrorism Branch of CSIS collects and evaluates information about domestic and international terrorism. This information is passed on to other government departments to initiate specific action (i.e., tightening of Canada-United States cross-border security by the departments of Citizenship and Immigration, and Transport). Information is also gathered prior to major international events to be hosted by Canada, which could become the target of terrorist activity.

CSIS, in combination with Citizenship and Immigration Canada, has tightened the screening of citizenship and refugee applicants, and has streamlined the review process for applicants in order to speed up approval or deportation. The rights of an applicant to appeal have been limited if their claim is rejected on their grounds of national security. Prior association with a recognized terrorist organization is a legal reason for refusal of entry to Canada and immediate deportation.

The United States-Canada border is the longest undefended national border in the world. Movement of terrorists across the border, particularly from Canada into the U.S., has not been difficult. As of late 2002, the Canadian government has taken steps to increase border security, searches of vehicles, and is developing joint strategies of border security with the United States.

Canada was one of the first countries to implement Resolution 1373 (2001) of the United Nations Security

Council, which required states to take action to prevent and suppress terrorism.

On October 2, 2001, the government of Canada implemented Resolution 1373. On October 15, 2001, the Antiterrorism Act was tabled in Parliament. The act (Bill C-36), which was passed in December 2001, amended the Criminal Code to restrict the ability of terrorists to finance their activities from Canada, restricted known terrorists from owing property in Canada, and increased the surveillance powers of the RCMP and CSIS. As well, stricter controls were put in place concerning the purchase and ownership of firearms.

Another piece of legislation, Bill C-42, proposes to amend the Immigration Act to allow the Minister of Immigration to approve the destination of anyone being deported. This would help ensure that the deportee did not escape to a jurisdiction that is sympathetic to their cause. The bill would also strengthen the search and seizure powers of customs agents at border crossings.

Objections to Bill C-42 concerning its infringement on civil liberties prompted its withdrawal and reformulation. New legislation called the Public Safety Act was introduced in April 2002. Among the recommendations is the coordination of federal and provincial government databases, to make a variety of information more widely accessible.

FURTHER READING:

ELECTRONIC:

Canadian Security Intelligence Service. "Counter-Terrorism: Backgrounder Series No. 8." Government of Canada. August 8, 2002. <http://www.csis-scrs.gc.ca/eng/backgrnd/back8_e.html> (26 November 2002).

Department of Foreign Affairs and International Trade. "Report of the Government of Canada to the Counter-Terrorism Committee of the United Nations Security Council on Measures Taken to Implement Resolution 1373 (2001)." Government of Canada. July 13, 2002. <http://www.dfait-maeci.gc.ca/anti-terrorism/resolution1373-en.asp.> (26 November 2002).

SEE ALSO

Airline Security
Canada, Intelligence and Security
Information Security

Canada, Intelligence and Security

BRIAN HOYLE

As of July 1984, Canadian security and intelligence operations have been the responsibility of the Canadian Security Intelligence Service (CSIS). The Canadian Security Intelligence Service Act legislated the formation of CSIS as a replacement for the Security Service, which was part of the Royal Canadian Mounted Police (RCMP).

In 1984, Canada was one of only a few western democratic nations to have a legislated security and intelligence force, with mandated boundaries to the scope of its operations and a monitoring process to ensure that the agency operates as intended. The Federal Bureau of Investigation in the United States is another example of a security and intelligence gathering agency with a conceived purpose and mandate.

Up until the mid-1970s, the task of defining what was to be considered a security risk to Canada and monitoring security developments was the responsibility of the RCMP. The force's Security Service performed security and intelligence gathering functions for the country. At that time, the perceived threat from other nations or organizations was ill defined, and no government security policy was in force. The operations of the Security Service had evolved over time and were the sole responsibility of the RCMP. Decisions regarding the targets of intelligence gathering were the domain of the Security Service. As a result, the government and the citizens of Canada had little knowledge of the measures being taken by the RCMP in the areas of national security and intelligence gathering.

Canadian security agency history. The roots of Canada's intelligence and security agencies date back almost 150 years, to the Royal Canadian Mounted Police Act of 1864. At that time, Canada had not formally become a country. A number of police forces operated in various regions of what, three years later, would become Canada. In 1864, Sir John A. MacDonald—the prominent political figure of the day and the man who would become Canada's first Prime Minister—assigned certain responsibilities to what was then called the Dominion Police Force. Security related duties included safeguarding the federal government's parliament building and collecting information concerning perceived security threats to Canada (i.e., at that time, the government was wary that the Fenians—a group of Irish nationalists who advocated for the political separation of Ireland from England—were planning to invade Canada from the United States).

The intelligence and security role of the Dominion Police Force increased in scope in 1920, when the Dominion Police joined with another force called the Royal North West Mounted Police (who operated in the western region of the country) to form the RCMP.

Having assumed the role as the country's intelligence and security agency, the RCMPs role and focus shifted over time in response to national priorities. For example, by the time of World War I, the RCMP was actively responding to labor unrest, which was perceived as being anarchist and of Communist origin, and so was viewed as a national security threat.

In 1920, the RCMP's security role was officially sanctioned with the formation of the Criminal Investigation

Branch. By the early 1940s, the focus of the Criminal Investigation Branch shifted yet again. Then, in the climate of escalating tensions between the former Soviet Union and the democracies of the western world, the existence of Soviet espionage networks in Canada became known. In 1946, largely in response to these tensions, an official branch of the RCMP dedicated to security and intelligence gathering was created and termed the Special Branch.

From the Special Branch, to the Security Service, to CSIS. Over the intervening decades, the relatively free hand that the RCMP exercised in national security created an atmosphere conducive to excessive and inappropriate behavior. For example, by the 1960s the RCMP was conducting surveillance campaigns on university campuses across Canada, having been convinced that campuses were fostering social unrest. Entertainment personalities and the even the country's tax payer-funded national radio and television system, the Canadian Broadcasting Corporation, were targeted for the same reason. Indeed, by the late 1960s the RCMP had investigated over 800,000 Canadians for evidence of Communist connections. Additionally, during the 1960s and 1970s, the Special Branch had adopted illegal methods—including theft, break-ins and property damage—to obtain information and foster dissension among groups considered to be security threats.

Recognizing the need for reform of the security framework in the country, the federal government of the day undertook an exhaustive analysis of the RCMP's security framework (in Canada these analyses are termed Royal Commissions). The Report of the Royal Commission on Security was released in 1969. The report recommended that national security should part of a civilian agency and part of the mandate of the country's federal police force.

The government responded in 1970 by forming the Security Service, which, while still part of the RCMP, was "civilian in nature", according to then Prime Minister Pierre Elliot Trudeau. For example, the Director General of the service was a civilian. In reality, however, the bulk of the Security Service was composed of RCMP officers and little changed in the intelligence and security operations community.

In October 1970, a minister in the government of the province of Quebec and the British trade commissioner to Canada were kidnapped by members of a group advocating separation of Quebec from Canada. The minister, Pierre Laporte, was murdered. In the aftermath of these events, the lack of information concerning the radical separatist movement became apparent, as did the illegal nature of some of the Security Service's intelligence gathering activities. The federal government was galvanized into revamping the Security Service. Another examination of national security was commissioned. The MacDonald report, which was released in 1981, echoed the earlier Royal Commission report in calling for a civilian security agency.

In May 1983, the Canadian government introduced Bill C-157, legislation that would create CSIS. This bill proved controversial, with many challenges arising concerning the possible infringement on civil liberties. After revision, Bill C-9 was proclaimed law in July and August, 1984. The responsibility for Canadian security measures and intelligence gathering passed from the RCMP's Security Service to CSIS.

The Mandate of CSIS. The legislation that created CSIS mandated the agency to function as a clearinghouse for security information. In other words, CSIS investigates perceived security threats to Canada and, if warranted, collects, analyzes, and compiles information on the security threats. The agency is able to provide advance warning to various government departments and agencies of individuals or activities that are suspected of being national security threats. The agency's powers end there. CSIS does not have any law enforcement responsibilities. If a department requires further information, CSIS can have an ongoing role in the process.

The legislation that spawned CSIS also mandated the types of security threats that the agency could respond to. Potential security threats take four forms. The first is espionage or sabotage that is actively directed against Canada or either threatens the country's own intelligence gathering efforts or other national interests. An example of such a threat is the gathering of economic, military, or scientific information by a group or government in a way that is illegal or unauthorized.

The second category of security threat involves activities originating in another country that threatens Canadians or the country's interests. An example would be the pressuring of an ethnic community by a foreign organization or government seeking the community member's participation in a terrorist conflict in the home country.

In the third category, security threats originate from within the country. Hostage taking (e.g., the separatist kidnappings of 1970), bomb threats or bombings, and politically motivated violence could threaten the security of Canadians. Also in this category is the use of Canada as a haven for terrorist activities in other countries. The alleged existence of Al-Qaeda terrorist cells in Canada is a current example of a security threat that CSIS is mandated to explore.

Finally, subversive threats to various levels of government in Canada and the country's judicial and economic system are potential security threats.

Regulation of security and intelligence in Canada. CSIS is subject to regular review and monitoring of its procedures and activities. The act that spawned CSIS also created the office of the inspector general and the Security Intelligence Review Committee (SIRC). The inspector general monitors CSIS operations and reports on whether these operations are legal or appropriate to the deputy solicitor

general (the second most powerful law enforcement officer in the country) and the SIRC. The SIRC is composed of five people who are selected following consultations with the prime minister and the leaders of all the qualified opposition parties in the House of Commons. The SIRC also conducts a review of CSIS activities and operations each year and reports its finding to the ministers of defense and foreign affairs, and to Parliament. By reporting to Parliament, the fullest public disclosure of the SIRC reports are ensured.

A caveat to the full and open disclosure of information, however, is the denial of cabinet documents to both the inspector general and the SIRC. Thus, some information about CSIS operations is kept secret.

The covert nature of some of Canada's intelligence and security network has been contentious from the establishment of CSIS. Much of the debate surrounding the formation of CSIS centered on its mandate. The idea that the country's security force would have full authorization to deal with "subversion" and "foreign influenced activities" struck some critics as too broad and hazy a frame of reference. Civil libertarians, in particular, argued that the lack of precision in the mandate could allow CSIS to legally infringe on the civil right of Canadians.

The regulatory and monitoring processes seek to minimize these civil rights issues. In response to a legal challenge, the Federal Court of Appeal ruled in 1987 that the Canadian Security Intelligence Act does not violate the Canadian Charter of Rights and Freedoms.

The powers of CSIS. The security and intelligence functions of CSIS apply only within the borders of Canada. Foreign intelligence, including offensive operations in other countries, is not part of the mandate of CSIS.

The federal government guides the powers that CSIS wields. Thus, the direction of the agency can change. This has occurred as the global tensions between the Eastern Europe and the West have declined, and as terrorists operations have escalated. CSIS is now concerned primarily with preserving the national security from disruption from within the country than from beyond Canada's borders. Operationally, the solicitor general, a member of the governing party who is the overseer of CSIS, provides government direction.

Intelligence information is gathered from a wide variety of sources, both public and privileged. Public sources include newspapers, trade journals, periodicals, academic journals, radio and television broadcasts in Canada and abroad, and via official government documents. Privileged sources include the interception of telecommunications.

The information that is collected is analyzed by the field staff who collect it and by personnel at CSIS headquarters. The information can be combined with other information to provide a national picture of the significance of the suspected security threat. The final step is the release of the analysis to the concerned government departments.

One of the main analysis reports is known as a threat assessment. Different departments use the threat assessment to determine responses. For example, the RCMP can use a threat assessment to gauge the degree of security provided to a visiting dignitaries and to prominent Canadians traveling abroad. As another example, the Department of Foreign Affairs and International Trade will use a threat assessment report to provide the proper security to Canadian business and governmental missions in foreign countries. Transport Canada also uses the assessment to issue warnings to the general public about travel.

As of late 2003, the primary role of CSIS is the safety of Canadians from security threats. This includes terrorist activity. As such, much of the information that CSIS collects on terrorist activities is shared with security and enforcement agencies in other countries including the United States.

■ FURTHER READING:

BOOKS:

Cleroux, Richard. *Official Secrets: The Story behind the Canadian Security Intelligence Service.*Toronto: McGraw-Hill Ryerson,1990.

Hewitt, Steven. *Spying 101: The RCMP's Secret Activities at Canadian Universities.*Toronto: University of Toronto Press,2002.

Starnes, John. *Closely Guarded: A Life in Canadian Security and Intelligence.*Toronto: University of Toronto Press,2001.

PERIODICALS:

Farson, S.A. "Is Canadian Intelligence Being Re-Invented?" *Canadian Foreign Policy* no. 6 (1999): 49–83.

ELECTRONIC:

Canadian Security Intelligence Service. "A Historical Perspective on CSIS." Government of Canada. November 01, 2001. <http://www.csis-scrs.gc.ca/eng/backgrnd/back5_e.html> (06 December 2002).

Library of Parliament. "The Canadian Security Intelligence Service." Parliamentary Research Branch. January 24, 2000. <http://www.parl.gc.ca/information/library/PRBpubs/8427-e.htm> (06 December 2002).

Canine Substance Detection

■ JUDYTH SASSOON

Canine substance detection involves the use of specially trained dogs, commonly golden or Labrador retrievers, for the detection of illegal substances. Dogs of this kind are now being used in various different situations, such as

John Long and his bomb-sniffing dog Coby check luggage as they go through a drill at Lackland Air Force base in San Antonio, Texas, in February 2002. AP/WIDE WORLD PHOTOS.

workplaces, airports and schools, to detect weapons, contraband, narcotic drugs, abused medication, alcohol, firearms and explosives. The necessity for this is due, in part, to the increasing incidents of drug abuse and violence among young people and employees, along with a growing need for increased security in schools and workplaces. Many schools and employers in the United States are now engaging "sniffer dogs" to improve safety and assist in the prevention of drug abuse. Supporters of this policy argue that the presence of these dogs, even if they do not immediately turn up illegal substances, provides a powerful deterrent. There are also, however, a number of school principals and employers who are concerned about this method because they anticipate that the seizure of illegal substances would reflect badly on their institutions and companies. Nevertheless, the reality is that today narcotic drugs, alcohol, and weapons are discovered in schools and in addition account for an astonishing 70 percent of injuries at work.

Dogs trained to detect the scent of illegal substances are useful as they can utilize their acute sense of smell to penetrate many hiding places which are inaccessible to other detection methods. A dog has about 200 million sensitive cells in its nose, compared to about five million or so in a human being, and therefore, a dog's olfactory system is around 40 times more sensitive than that of a human. A dog's sense of smell is made even keener by an organ in the roof of the mouth that is not found in the human olfactory system and this enables it to "taste" a smell, amplifying a weak smell into a stronger one. This sensitivity to, for example, the odor of butyric acid emitted in sweat, enables a dog to locate an object, such as a ball, belonging to its owner from several similar objects thrown by a number of different people. It also enables tracking dogs such as bloodhounds to pursue and keep pace with a fugitive for up to 100 miles. Dogs also have the ability to distinguish individual odors when other strong smells are also present. They can be trained to detect the odors of heroin, marijuana and cocaine hidden in suitcases even in the presence of strong smelling perfumes. Drug traffickers are constantly attempting to find more sophisticated ways of smuggling illegal drugs and the scenting abilities of sniffer dogs often provide the only means of locating well-hidden narcotics. Canine drug detectors have proved so

successful that they are now employed in many airports and also at bus stations, border crossings, and ports. The dogs are trained both to detect the drugs and then to alert authorities, either by pawing at the surface near the location of the smell or by sitting down next to the source. This behaviour usually provides the authorities with a valid cause to search luggage or vehicles.

Trained detection canines were introduced into American public schools in Texas in the 1980s. The concept soon became popular and widely used as a tool for increased safety and as a drug deterrent on campuses. Thus, drug and narcotic detection are today an important aspect of school security. Also, because of the increasing danger of violence in schools, weapons and contraband detection also plays a role in the promotion of school safety. Depending upon the school or business, a program of regular canine visits is developed to detect illegal substances or weapons. Typically, everyone is informed about the pending visit of a sniffer dog and in most cases, the dogs are allowed to meet the students and employees beforehand. Subsequently, the dogs are brought in with a handler on a random, unannounced basis and perform "spot checks" on designated areas.

Some dogs are specially trained to detect the acidic smell of nitroglycerin and the sulphur in gunpowder for work with explosives detection. Fire investigators use arson dogs to help in criminal investigations. These canines locate minute traces of gas or other flammable liquids in situations where arson is suspected. Arson dogs are trained in such a way that they can accurately detect traces of arson about the size of a thousandth of a drop, which is much more efficient than any commonly used electronic detection device.

In 2002, it was reported that scientists at Russia's DS Likhachev Scientific Research Institute for Cultural Heritage and Environmental Protection successfully bred a new kind of highly efficient sniffer dog. The new breed is a cross between a wild jackal and a Russian husky. The breeding program was started in 1975, and in 2002, the institute successfully produced hybrids that were a quarter jackal and three-quarters husky. These hybrids were bred to combine the very sensitive nose of the wild, scavenging jackal with the more benign temperament of the husky. The jackal has a sense of smell that is even keener than that of its domestic counterpart. It was reported that many dog species are losing their naturally sharp sense of smell through domestication. Huskies are used as the domesticated breed in this program because they have a better developed sense of smell than all other dog breeds. This is because they are adapted to severe conditions of arctic cold where many substances become non-volatile and exist in only a highly diluted form. This crossing of highly sensitive canines has produced a breed that is now being used by authorities at Russian airports. By 2003, some twenty-five of the dogs were employed at Sheremetyevo Airport, Moscow and ten more were working at the forensic criminology examination department nearby. Their handlers reported that, aside from their sharp sense of smell, the jackal hybrids were also highly courageous and expert at crawling into the tightest corners, especially during the inspection of aircraft.

FURTHER READING:

BOOKS:

Tonry, Michael *Malign Neglect: Race, Crime, and Punishment in America.* Oxford University Press, 1996.

PERIODICALS:

Charles Mesloh, Ross Wolf and Stephen Holmes. "A Pilot Study of the Confounding Effects of 'Jute' on Law Enforcement Canine Training." *Journal of the Academy of Canine Behavioral Theory* 1 (2002): 2–9.

ELECTRONIC:

United States Department of Agriculture. "The AQI Program at Airports." <http://www.aphis.usda.gov/oa/pubs/detdog1.html> (February 20, 2003).

SEE ALSO

Airline Security
Drug Control Policy, United States Office of National

CAPS (Computer Assisted Passenger Screening System).

SEE *IBIS (Interagency Border Inspection System).*

Carnivore Program.

SEE *Internet Surveillance.*

Carter Adminstration (1977–1981), United States National Security Policy

CARYN E. NEUMANN

While President Jimmy Carter notably became the first president to label access to Middle Eastern oil as a vital security interest, his single term in office is widely viewed with skepticism in terms of national security. Carter's micro-management and concomitant power struggles within the administration did little to arrest the sharp decline in American power and influence that occurred in the 1970s.

United States President Jimmy Carter, left center, and Soviet President Leonid Brezhnev, right center, shake hands amidst applause in the Vienna Imperial Hofburg Palace after signing the SALT II treaty, June 8, 1979. AP/WIDE WORLD PHOTOS.

In the 1976 presidential election, the Democrats chose Carter, a one-term governor of Georgia as their standard bearer specifically because he could capitalize on the post-Watergate cynicism about politicians. A graduate of the United States Naval Academy, a born-again Baptist, and a peanut farmer, the folksy Carter spent the campaign stressing both his honesty and his lack of inexperience in the byways of Washington politics. He promised to use his engineering education and his experience as an officer on a nuclear submarine to be a hands-on manager who would establish systemization in government. In office, Carter's strong concern with the minutiae of administrative procedure left him less able to assume the chief leadership role among top levels of government.

Carter sought to avoid the extreme centralization of power that had characterized the Nixon administration's security policy. He expected to serve as a policy initiator and manager who would make decisions from the range of views presented to him by his senior advisors. He saw Secretary of State Cyrus Vance as the principal advisor for foreign policy, while the National Security Council would play a less active and assertive role than in previous administrations. In practice, the Carter administration had two secretaries of state. National Security Advisor Zbigniew Brzezinski, a man accustomed to aggressive debate, proved particularly adept at gaining the president's confidence. He also became an outspoken advocate of the administration's security policy. Vance publicly competed with Brzezinski for the position of chief presidential advisor, a situation that left some congressional members confused about the chain of authority. Vance ultimately resigned in 1980 in protest over the failed rescue attempt of the American hostages held by Iran. His replacement, Edmund S. Muskie, had too brief a term to make a significant impact.

While suffering from management strategy weaknesses, the Carter administration may have been troubled from the start by growing problems facing the United States. Dwindling resources had led to a severe energy crisis that worsened when renewed violence struck the Middle East. This situation prompted Carter to issue a new foreign policy declaration that marked energy as a matter of national security. The Carter Doctrine stated that the United States would employ force if necessary to protect its continued access to the oil fields of the Middle East. The administration also pushed for the development of synthetic fuels, but Congress only partially funded this request.

Like Nixon and Ford before him, Carter attempted to reduce tensions with the Soviet Union. The controversial Strategic Arms Limitation Treaty (SALT II) was similar to SALT I in that it did not do much to slow down the nuclear

Despite President Jimmy Carter's (shown here with his advisors) efforts to resolve the Iranian hostage crisis, 52 Americans were held at the American embassy in Teheran, Iran for 444 days. January 20, 1981. ©BETTMANN/CORBIS.

arms race. The agreement placed a ceiling of 2,250 bombers and missiles on each side and set limits on the number of warheads and new weapons systems. In order to ensure that the Soviets did not gain an advantage in the number and destructive power of land-based missiles, Carter proposed the MX missile system. The system proposed to befuddle the Soviets and prevent them from successfully launching an attack by moving the MX missiles around a vast maze of underground tunnels connected by a railroad. While the Senate debated the merits of SALT and the MX, the Soviets invaded Afghanistan. Carter immediately shelved the treaty.

Carter's presidency would be further weakened when the Iranian hostage crisis in 1979 exposed the inability of the U.S. to control world affairs. Carter appealed to the United Nations for help but the head of Iran, Ayatollah Ruhollah Khomeini, ignored the U.N.'s requests. Carter then froze Iranian assets and imposed a trade embargo. Americans clamored for a military response, which Carter eventually provided by sending commandos to Iran in 1980. The raid was aborted by helicopter failures that left eight soldiers dead. The crisis finally ended after 444 days when Carter released Iranian assets to ransom the 53 hostages.

FURTHER READING:

BOOKS:

Carroll, Peter N. *It Seemed like Nothing Happened: America in the 1970s.* New Brunswick: Rutgers University Press, 1990.

Crabb, Cecil V. and Kevin V. Mulcahy. *American National Security: A Presidential Perspective.* Pacific Grove, CA: Brooks/Cole, 1991.

SEE ALSO

ADFGX Cipher
Cold War (1972–1989): The Collapse of the Soviet Union
Eisenhower Administration (1953–1961), United States National Security Policy

Middle East, Modern U.S. Security Policy and Interventions
National Security Advisor, United States
Nixon Administration (1969–1974), United States National Security Policy

Case Officer.

SEE *Intelligence Officer.*

CDC (United States Centers for Disease Control and Prevention)

▮ BRIAN HOYLE

CDC is an acronym for Centers for Disease Control and Prevention. The center, which is headquartered in Atlanta, Georgia, is one of the predominant public health institutions in the United States and in the world. The CDC serves United States national security by monitoring the incidence of infectious disease in the U.S. (and around the world), and through the development and implementation of disease control procedures. As part of this mandate, the CDC is one of the few facilities in North America that houses a biological laboratory capable of handling very infectious and lethally-dangerous microorganisms such as the Ebola virus and *Bacillus anthracis*, the bacterium that causes anthrax.

The CDC is the pre-eminent institution in the United States dedicated to the prevention of disease, and is a global leader in public health. In addition to the Atlanta headquarters, the CDC has facilities in San Juan, Puerto Rico, and in eight other locations in the continental United States. The U.S. locations are Anchorage (Alaska), Cincinnati (Ohio), Fort Collins (Colorado), Morgantown (West Virginia), Pittsburgh (Pennsylvania), Research Triangle Park (North Carolina), Spokane (Washington), and Washington D.C.

Approximately 8,500 people work at the CDC in 170 occupations pertaining to public health research, administration, monitoring, and education. CDC personnel are also seconded to other international health agencies such as the World Health Organization and to state and local health agencies in response to disease outbreaks.

The CDC is organized into 11 national centers that are concerned with health care and disease prevention. The national centers study:

- Birth Defects and Developmental Disabilities,
- Chronic Disease Prevention and Health Promotion,
- Environmental Health (that includes the Office of Genomics and Disease Prevention),
- Health Statistics
- HIV (Human Immunodeficiency Virus), STD (Sexually Transmitted Disease), and TB (Tuberculosis) Prevention,
- Infectious Diseases,
- Injury Prevention and Control,
- Immunization Program,
- Occupational Safety and Health,
- Epidemiology Program, and,
- Public Health Practice Program.

At the beginning of 2003, the CDC enters its 57th year of existence. The institution was established on July 1, 1946 in Atlanta. At that time the acronym CDC stood for Communicable Disease Center. The CDC replaced another center known as the Malaria Control in War Areas. The former institution had been established as part of the Public Health Service to rid the southern United States of malaria during the years of World War II. As well, the center had assumed the responsibility for keeping the region free of murine typus fever. The establishment of the Communicable Disease Center continued these functions while expanding to include all diseases that could be transmitted from person to person.

The institute's founding director was Dr. Joseph M. Mountin. In its early days, the center was small and research and surveillance programs were still geared towards insect-transmitted diseases such as malaria. After an aggressive campaign of expansion by Mountin, however, which was intended to entrench CDC's position and value to the country, the center became the national agency for epidemiology (the study of the origin and spread of diseases).

The Korean War in the 1950s solidified the center's value as an epidemiological resource. The Epidemiological Intelligence Service (EIS) was created during that time, with the mandate to protect U.S. citizens from diseases that originated in other regions of the world. The EIS remains an important part of today's CDC, especially because of the recognition, in the 1950s, that biological warfare was an emerging threat to national security.

Two other events in the 1950s besides the Korean conflict increased the national importance of the CDC, and served to ensure that the funding of the center continued. First, a national campaign to inoculate children with the recently approved Salk polio vaccine led to a spate of poliomyelitis cases. A Polio Surveillance Unit was established at CDC. The unit quickly determined that a contaminated batch of the vaccine has been the problem. Their findings allowed the contaminated units of vaccine to be withdrawn from use, and the inoculation program continued with confidence. In retrospect, the continuation of the vaccination campaign has been invaluable, since it was pivotal in the eradication of polio, and since it instilled the confidence in vaccines in general that helped ensure the

In one of the biggest steps taken towards modernizing defenses against smallpox, the Centers for Disease Control (CDC) dedicated one of its two maximum containment laboratories to smallpox-only research in 2002. A senior researcher is shown through a glass viewer entering the Biosafety-Level-4-Lab wearing a biohazard protective suit. AP/WIDE WORLD PHOTOS.

success of other vaccination campaigns. These outcomes also solidified the CDC's reputation as a disease-monitoring center of excellence. The other event was a large influenza outbreak in the U.S. Once again, a surveillance campaign on the type of virus that was involved and its pattern of spread helped future efforts to develop effective vaccines and inoculation programs.

During the 1950s and 1960s, the CDC grew through the assumption of responsibility for programs that had been previously handled by other government departments and agencies. Examples include the centers of venereal disease, tuberculosis, and immunization.

Beginning in the 1960s, CDC assumed an increasingly important role in the public awareness of infectious diseases. One important example occurred in 1961 when the institution took over the publication of the *Mortality and Morbidity Weekly Report* (MMWR). The MMWR publishes information on the number of deaths and cases of infectious disease from every state in the country each week. The availability of such detailed information has allowed the progression of some emerging diseases such as AIDS to be charted.

By the late 1960s, the CDC had become much more than a center for the study and action against communicable diseases. These activities had moved CDC far beyond its original mandate as a communicable disease center. In recognition of the center's changed role, its name was changed in 1970 to the Center for Disease Control. Further expansion led to a slight name change in 1981, to the Centers for Disease Control. Finally, as further expansion took the CDC into disease prevention, in 1992 the organization became the Centers for Disease Control and Prevention. Even so, for the sake of continuity the acronym CDC has been retained.

These and other efforts have contributed to national security through the preservation of public health. In more recent times, accomplishments of significance have included participation in the development of a smallpox vaccine and inoculation program, and the identification of the agents of several diseases including Legionnaire's disease, toxic shock syndrome, hantavirus pulmonary syndrome, and Acquired Immunodeficiency Syndrome.

In 1978, biosafety level 4 containment laboratory was opened in the CDC Atlanta headquarters. Then as now, this is one of only a handful of level 4 labs in North America. Other similar facilities are present in San Antonio, Texas, at the U.S. Army Medical Research Institute of Infectious Disease (USAMRIID) in Fort Detrick, Maryland, and in Winnipeg, Manitoba, Canada. It is only at these facilities that highly infectious and lethal viruses and bacteria can be safely studied and treatments devised. At CDC, for example, the Special Pathogens Branch studies the Ebola, Marburg, and Hantaviruses.

In the present day, CDC provides a great deal of information concerning naturally occurring infectious diseases and, particularly since in the aftermath of the September 11, 2001 terrorist attacks on the U.S., information on bioterrorist threats such as anthrax. The research and disease surveillance expertise at CDC is being harnessed, along with other national laboratories and intelligence gathering organizations, to strengthen the United States from bioterrorist attacks.

FURTHER READING:

PERIODICALS:

Epidemiology Program Office, CDC. "CDC's 50th Anniversary: History of CDC." *Morbidity and Mortality Weekly Report* no. 45 (1996): 525–30.

ELECTRONIC:

Centers for Disease Control and Prevention. "About CDC." November 2, 2002. <http://www.cdc.gov/aboutcdc.htm> (28 December 2002).

Centers for Disease Control and Prevention. "CDC Timeline." <http://www.cdc.gov/od/oc/media/timeprnt.htm> (28 December 2002).

SEE ALSO

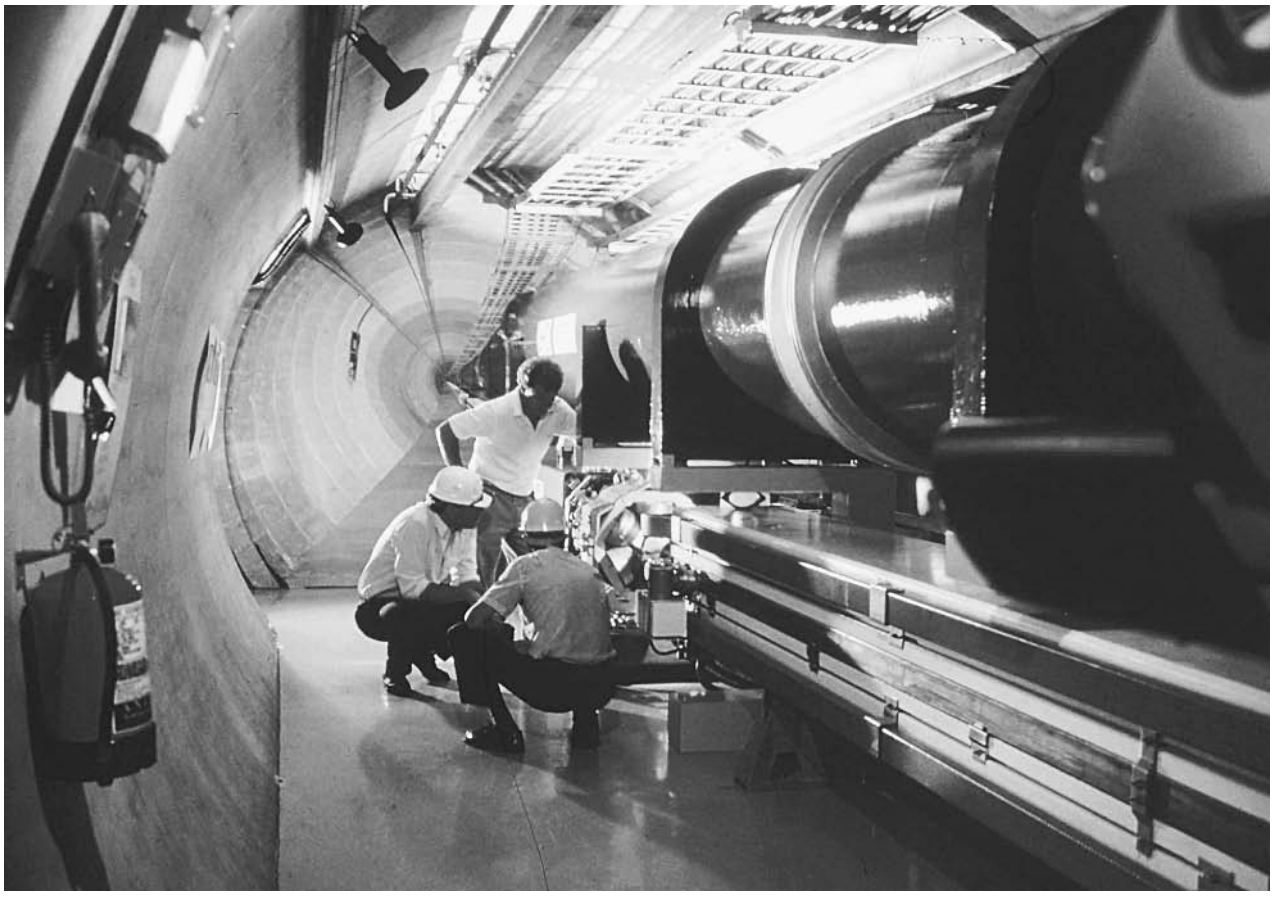
Biocontainment Laboratories
NNSA (United States National Nuclear Security Administration)
Public Health Service (PHS), United States

CERN

LARRY GILMAN

CERN, located along the French-Swiss border near the Swiss capital Geneva, is the world's largest particle-physics laboratory. (The acronym stands for Conseil Européenne pour la Recherche Nucléaire, French for CERN's original name, the European Council for Nuclear Research; since October 1954, despite retention of the old acronym, CERN's name has actually been *Organisation* Européenne pour la Recherche Nucléaire.) CERN was founded in 1954 and today is supported by a consortium of 20 European nations and by a number of "observer states," including Japan and the U.S. Besides being responsible for many fundamental discoveries in particle physics, primarily through the use of particle accelerators, CERN is the birthplace of the World Wide Web.

CERN is a non-military organization; Article II.1 of the multinational convention establishing the laboratory states that it "shall have no concern with work for military requirements and the results of its experimental and theoretical work shall be published or otherwise made generally available." However, CERN is unavoidably relevant to



Mock-up of the CERN Large Hadron Collidor or LHC atom-smasher under construction in a 27-kilometer tunnel near Geneva. ©AFP/CORBIS.

military affairs via the relevance of all physics to military affairs. The proposal in 1949 to form a regional European physics laboratory (i.e., CERN) was directly inspired by the explosion by the Soviet Union, in that year, of its first atomic bomb; furthermore, while CERN was being founded during the early 1950s, the building of particle accelerators in the United States was funded primarily by the military, which hoped to produce particle-beam weapons and to manufacture polonium for radiological warfare (i.e., the use of radioactive dust as a weapon). Both scientists and politicians involved in the founding of CERN were, therefore, aware that military applications of research in particle physics, though not predictable, might eventually occur. Furthermore, the advanced scientific equipment and techniques that would be developed at CERN and the large pool of expertise it would create and sustain were seen as basic military European assets. Likewise, the U.S. Navy's Office of Naval Research financed research in fundamental physics in U.S. universities in the postwar years on the ground that even "untargeted" research—science for science's sake—could, on average, ultimately be counted on to bear military fruit.

Nevertheless, CERN is as non-military, non-secretive, and international as an institution could well be. The construction of a nuclear reactor at CERN was ruled out from the beginning precisely because of the obviously military applications of such technology. CERN has therefore focused on the use of particle accelerators for research, avoiding the production or use of militarily significant amounts of fissionable materials and leaving the military implications (if any) of its discoveries to be worked out by national and commercial laboratories. To further distinguish it from a weapons-research laboratory, CERN does not classify any of its results, but, in accordance with its founding convention, makes them openly available to all inquirers.

Design work for CERN's first facilities proceeded in Geneva, Switzerland during 1953 and 1954 while the final international agreements were being worked out by CERN's original 11 member states. Construction contracts were awarded in October 1954, and CERN's first accelerator, a 600 MeV proton synchro-cyclotron, began operation in 1957. Confirmation of pion decay was one of the first experimental results, beginning a long line of important physics results made at CERN.

Not all of CERN's contributions have been in the realm of physics; in 1990, CERN computer scientists Tim Berners-Lee and Robert Cailliau proposed a network of

"hypertexts" (texts, images, and other information objects linked by computer addresses routinely hidden from the user) that would run on computers connected through the Internet, which was already used for file transfers, e-mail, and other purposes. They proposed that this network be called the World-Wide Web, a name which has stuck.

Approximately 6500 physicists from 80 countries work at CERN, which operates a number of particle accelerators and detectors. CERN's largest tool is a circular particle accelerator 16.7 miles (27 km) in circumference, located some 320 feet (100 m) underground. CERN can achieve higher particle energies than any other facility in the world, making it a key facility for ongoing advances in particle physics.

FURTHER READING:

BOOKS:

Hermann, Armin, et al. *History of CERN.* Amsterdam: North-Holland Physics Publishing, 1987.

ELECTRONIC:

"The CERN Archive." February 12, 2002. <http://library.cern.ch/archives/index.html> (March 11, 2003).

Chain Reaction.

SEE *Nuclear Reactors.*

Chatter.

SEE *Electronic Communication Intercepts, Legal Issues.*

Chechen-Russian Conflict

JUDSON KNIGHT

During the 1990s, westerners became aware of a seemingly incongruous conflict between the Russian Federation and Chechnya, a small breakaway republic along its southern border. In fact, Chechens had resisted Russian rule, sometimes actively and sometimes passively, for over two centuries. To both sides, as well as to outside observers, the success of the Russian response to the secessionist movement served as a litmus test for the Kremlin's ability to maintain sovereignty over Russian territories in the post-Cold War era.

Background (1791–1991)

Located along the northern flank of the Greater Caucasus mountain range, Chechnya is about the size of Massachusetts, with a much smaller population: about 1,165,000 people at the end of the twentieth century. To the east and southeast is Dagestan, which, like Chechnya, was an outlying minority region of the Russian Empire in the eighteenth and nineteenth centuries, and an "autonomous republic" in the Soviet Union and later the Russian Federation. For decades, Moscow administered Chechnya as a unit with Ingushetia, which lies to the west. By contrast, Georgia, to the south, has enjoyed full independence since the breakup of the Soviet Union at the end of 1991.

Ethnic Chechens, as well as the Ingush minority in Chechnya, are Muslim, and their shared religion has long been a rallying point for resistance against Russian rule. In 1791, their Sheikh Mansur, a national hero and symbol of Chechen resistance, lost a key battle to the Russians, yet Russia did not truly secure control for several more decades. In the 1830s, Muslim leader Shamil prosecuted a campaign of guerrilla warfare against the Russians, and when the latter were diverted by the Crimean War in the 1850s, it seemed that the Chechens might successfully break away. As soon as Russia turned its attention to the Chechen problem, however, it crushed Shamil's revolt.

In 1917, the new Bolshevik government created a joint Chechen and Ingush entity that would eventually be given the name "Chechen Ingush Autonomous Region." During World War II, Soviet dictator Josef Stalin used alleged Nazi sympathies on the part of the local populace as a pretext for a mass deportation in 1944. Thousands of Chechens and Ingush died in transit, or as a result of deliberate Soviet actions. Only in 1957 were they allowed to return to their homeland, where they remained an obscure fringe element of the Soviet empire until that empire began to crumble.

The first Chechen war (1991–96). In August 1991, Chechen politician and former Soviet air force general Dzhozkhar Dudayev led a coup against the local Moscow-appointed government. Elected president on October 27, he declared independence on November 1. In 1992, Chechen-Ingushetia split in two, with Dudayev still leading the Chechen portion, and in 1993, he dissolved Chechnya's parliament.

Over the course of 1994, Moscow attempted to foment a coup by backing anti-Dudayev groups within Chechnya. When these efforts failed to yield fruit, President Boris Yeltsin in November ordered the Chechens to peaceably accept Russian sovereignty or face armed intervention. When the Chechens did not surrender the reins of

government, Russia invaded with a force of 40,000 men on December 11, 1994.

In a situation that recalled the Soviet debacle in Afghanistan that had begun almost exactly 15 years earlier, the Russians found themselves thwarted in their hopes for easy victory. Pushed back from the capital city of Grozny, they only managed to take it in March 1995, at a heavy military and civilian cost. In April, Yeltsin ordered a unilateral ceasefire, but sporadic fighting continued throughout the spring. Only in June did peace talks begin.

January 1996 saw a Russian incursion in neighboring Dagestan, where rebels had seized control of a hospital. Meanwhile, fighting went on as before in Chechnya, and though Yeltsin on March 31, called for a limited withdrawal, this did nothing to abate hostilities. Anti-Russian sentiment in Chechnya flared when a rocket attack killed Dudayev on April 21, and on August 6, rebel forces gained control of Grozny. Then, on August 31, newly instated Russian security chief Alexander Lebed signed a pact with the rebels, declaring the war concluded and putting off the question of Chechen independence.

The second Chechen war (1997–99). In 1997, Aslan Maskhadov, leader of one of the anti-Dudayev forces, was elected president of Chechnya. That May, Maskhadov and Yeltsin signed a peace treaty, but still failed to address the question of Chechnya's future status. Resentment of Russian rule continued, and with it sporadic armed resistance.

August 1999 saw more incursions into Dagestan, this time on the part of Chechen rebels, who seized control of several towns. Meanwhile, Russia, which had sponsored terrorist movements worldwide during the Soviet years, for now became the target of terrorism as Chechen separatists set off a wave of bombings in Russia proper. Chechen separatists destroyed four apartment buildings in Moscow, and by the end of September, more than 300 people had died in terrorist incidents across the country.

Although the Kremlin had opposed the U.S. and allied European bombing of Yugoslavia under the aegis of NATO (North Atlantic Treaty Organization) earlier in 1999, in September, the Russians in Grozny emulated the NATO strategy of strategic air offensives. At month's end, however, it became clear that bombing alone would not be enough, and as midnight approached on September 30, several thousand Russian soldiers, with the support of some 1,000 armored vehicles, advanced into northern Chechnya.

At the end of October came an announcement from Russia's defense minister, Igor Sergeyev, that Russian troops would remain in Chechnya "for a long time and seriously." This marked a reversal of Moscow's claim, made at the beginning of the offensive, that it was acting only to stop Chechen incursions into Dagestan. Meanwhile, the Russians had set up a government under the leadership of a pro-Russian parliament whose members had been living in Moscow since 1996.

Chechnya since 1999. By the end of the 1990s, it was estimated that some 100,000 people had died, and more than 400,000 were rendered homeless, by the wars in Chechnya. In 2002, actions by Chechen troops and terrorists against the Russians continued, with suicide bombings, the downing of a Russian helicopter, and—most dramatically—the storming of a Moscow concert hall in late October. The Russian government responded to the terrorists by gassing the building, rescuing most of the hostages, while killing some hostages along with the perpetrators.

On November 3, 2002, Sergei Ivanov, who had replaced Sergeyev as defense minister, announced that Russia would intensify military operations in Chechnya. Military activity continued, but in early 2003, Russia signaled a new strategy. It declared six months' amnesty for all who had fought on either side in the Chechen conflict since 1993, offering all combatants—including convicts and those under investigation, though not persons accused of major crimes such as murder—immunity from prosecution or prison time.

The Russian and Chechen governments held a referendum in April, 2003, that saw large voter acceptance for a new Russian-backed constitution. Critics in Chechnya, however, charged that the referendum and constitution were simply a means toward providing an illusion of self-rule. Internationally, leaders of human rights groups, as well as some Western officials, described the election as an attempt by the Kremlin to avoid negotiation with guerrilla forces.

■ FURTHER READING:

BOOKS:

Gall, Carlotta, and Thomas De Waal. *Chechnya: Calamity in the Caucasus.* New York: New York University Press, 1998.

Knezys, Stasys, and Romanas Sedlickas. *The War in Chechnya.* College Station: Texas A&M University Press, 1999.

Lieven, Anatol. *Chechnya: Tombstone of Russian Power.* New Haven, CT: Yale University Press, 1998.

Politkovskaia, Anna. *A Dirty War: A Russian Reporter in Chechnya.* London: Harvill, 2001.

ELECTRONIC:

Chechnya News. <http://www.chechnyanews.com/> (April 30, 2003).

Pravda. <http://english.pravda.ru/> (April 30, 2003).

Russian Informational Centre. Ministry for Press, Television, Radio Broadcasting and Mass Communications of the Russian Federation. <http://www.infocentre.ru/eng_user/> (April 30, 2003).

SEE ALSO

Cold War (1972–1989): The Collapse of the Soviet Union

Kosovo, NATO Intervention
Russia, Intelligence and Security

Chemical and Biological Defense Information Analysis Center (CBIAC)

JUDSON KNIGHT

The Chemical and Biological Defense Information Analysis Center (CBIAC) is a civilian-operated institution that contracts with the United States Department of Defense (DOD) to provide information on chemical and biological warfare technology. Headquartered in Maryland, it has satellites throughout the United States. CBIAC is a full-service DOD information analysis center operated by Battelle Memorial Institute, and supported by a number of other technology and information entities in the private sector.

CBIAC's mission is to generate, acquire, process, analyze, and disseminate information on chemical and biological (CB) science and technology. It operates under contract to the Secretary of Defense, and is managed by the Defense Technical Information Center under the information analysis center (IAC) program. The information it produces is intended to support commanders, warfighters, and reservists; the CB defense research, development, and acquisition community; and various federal, state, and local departments and agencies in need of current CB information.

CBIAC operations. The Defense Department established CBIAC in 1986, and placed Battelle Memorial Institute in charge of its operations. Founded in Columbus, Ohio, in 1929, Battelle is an information and technology company involved in a wide array of disciplines. Among the most notable examples of its achievements are the office copier machine, bar code symbol, and compact disc, all of which are the direct or indirect result of Battelle research and development.

Working with Battelle specialists at CBIAC headquarters in Aberdeen Proving Ground, Maryland, are representatives of Horne Engineering Services, Innovative Emergency Management, MTS Technologies, QuickSilver Analytics, and SciTech. Together they assist DOD and other government agencies, as well as approved contractors, with the use of CB information for integrated solutions. In addition to its headquarters, CBIAC maintains satellite operations in Arlington and Stafford, Virginia; Natick, Massachusetts; Saint Robert, Missouri; San Antonio, Texas; and Dugway Proving Ground, Utah.

Activities of CBIAC. In accordance with its responsibilities to the DOD, CBIAC identifies and acquires CB data and information from media sources; processes, stores, and retrieves CB data and information; identifies, develops, and applies tools and techniques for the analysis, interpretation, and application of such data and information; and prepares reports, tables, and other forms of focused information for military field personnel, managers, planners, scientists, and engineers.

Among the areas of interest for CBIAC are analysis of manufacturing processes for nuclear, biological, and chemical (NBC) systems; identification of chemicals and the physical and chemical properties of chemical warfare/chemical and biological defense (CW/CBD) materials; combat effectiveness; counter-proliferation, international technology proliferation, and arms control; counter-terrorism; decontamination; demilitarization, conversion of CB materials and equipment for defense purposes, and technology transfer for dual use; individual and collective protection and domestic preparedness; environmental effects of CB materials; force protection; and many others.

CBIAC attempts to anticipate the requirements for CB information, and seeks to work with emerging CB defense organizations. Its products range from handbooks and training kits to computerized databases, interactive software, and CD ROMS. Additionally, it offers inquiry and referral services whereby it provides answers and information relevant to specific CB needs. CBIAC also maintains an extensive library, containing some 108,000 citations of CB information, as well as 41,000 holdings.

FURTHER READING:

BOOKS:

Drell, Sidney D., et al. *The New Terror: Facing the Threat of Biological and Chemical Weapons.* Stanford, CA: Hoover Institution Press, 1999.

Joseph, Robert G., and John F. Reichart. *Deterrence and Defense in a Nuclear, Biological, and Chemical Environment.* Washington, D.C.: Center for Counterproliferation Research, National Defense University, 1999.

ELECTRONIC:

Battelle Memorial Institute. Defense Systems—CBIAC. <http://www.battelle.org/army/cbiac.stm> (January 17, 2003).

Chemical and Biological Information Analysis Center. <http://www.cbiac.apgea.army.mil/> (January 17, 2003).

SEE ALSO

Biochemical Assassination Weapons
Biological Warfare
Chemical Warfare

A technician collects a sample from a laptop computer that will be analyzed by the Sabre 2000 trace detection instrument, which can detect traces of explosives, drugs, or chemical weapons. AP/WIDE WORLD PHOTOS.

Chemical and Biological Detection Technologies

BRIAN HOYLE

The ability to detect the components of chemical and biological weapons is an important part of a national security strategy. For example, the inability to rapidly detect letters for the presence of anthrax spores provided a route for the targeting of infectious microorganisms in the United States in 2001. The portability of chemical and biological weapons has made them attractive to individuals or groups with political, religious, or other grievances. This has spurred development of more sophisticated, accurate and rapid detection technologies.

The conventional x-ray technology long used in airports has been refined. Most of the x-ray beam is reflected back immediately upon encountering an object. Some of the radiation, however, passes through the object. By analyzing the beams that actually penetrate through an object, information on the object's composition is provided. Another version sends two different x rays of different wavelengths through an object. The different beams can distinguish between organic objects, such as food and paper, and inorganic objects.

A chemical detection technology known as gas chromatography has been sped into routine use in airports since the U.S. terrorist attacks of September 11, 2001. The different chemicals present on a cloth that is swiped over an object can be separated based on their different preference for the gas mixture that is pumped through the sample chamber. A target chemical (i.e., an explosive) is detected within seconds.

Chemical detection technologies have also been adapted for use "in the field", such as by United Nations inspectors deployed in Iraq beginning in November 2002, to the presence of missiles that were supposedly destroyed by the Iraqi government in the mid-1990s.

Sound can be used to detect chemicals. For example, the acoustic wave sensor uses a quartz surface to convert incoming sound waves into electrical signals. Over a dozen different chemicals can be detected within seconds, even from biological sources. In another sound-based technique called acoustic resonance, the pattern of vibrations when sound waves are sent inside an object like a missile can reveal whether the missile is filled with a solid or a liquid, and even the type of chemical present.

Light is another means of chemical detection. The use of light is called spectroscopy. Mass spectroscopy determines the mass of proteins, which is important in determining the identity of the chemical or biological agent. Matrix-Assisted Laser Desorption/Ionization Mass Spectroscopy (MALDI-MS) can identify proteins that are unique to *Bacillus anthracis* (the cause of anthrax) and *Yersinia pestis* (the cause of plague). Raman spectroscopy measures the change in the wavelength of a light beam by the sample molecules. Optical spectroscopy measures the absorption of light by the chemical groups and the subsequent emission of light by the same groups as the identification method.

The ability to detect genetic sequences that are unique to certain bacteria (gene probing) has been exploited to develop genetically based microbial detection methods. The best example of gene probing is the polymerase chain reaction (PCR), which can enzymatically detect a target stretch of genetic material and rapidly amplify that region to detectable levels. Handheld PCR detectors (i.e., Handheld Advanced Nucleic Acid Analyzer, or HANAA) were used in the 2002–2003 inspections of Iraqi facilities by United Nations officials.

Biological detection devices can monitor the surrounding air at regular intervals. Air is automatically drawn into the device and analyzed for target genetic sequences using the PCR technology. The results can be electronically relayed to a central base for analysis.

Another biological technology utilizes antibodies that are produced in response to the presence of a specific

microorganism. Tests are available that detect *Bacillus anthracis*, *Clostridium botulinum*, viruses (e.g., smallpox), and chemicals (e.g., ricin) in minutes.

Some older biological detection technologies still prove reliable. Growth of microorganisms on artificial food sources (media) produces populations called colonies. Medium can be selected that produces colonies that have a distinctive appearance and color. Gel electrophoresis separates differently sized pieces of genetic material or other microbial components (e.g., protein) into bands. The banding pattern can be used to identify the microorganism. Finally, chromatography separates compounds from one another based on their differing speed of movement through a gas or a liquid mixture.

FURTHER READING:

BOOKS:

Cilluffo, Frank J., Sharon L. Cardash, and Gordon Nathaniel Lederman. *Combating Chemical, Biological, Radiological, and Nuclear Technologies: A Comprehensive Strategy: A Report of the Csis Homeland Defense Project.* Washington, D.C.: Center for Strategic and International Studies, 2001.

Fritz, Sandy, and Jack Brown. *Understanding Germ Warfare (Science Made Accessible).* New York: Warner Books, 2002.

Lederberg, Joshua, and William S. Cohen. *Biological Weapons: Limiting the Threat (BCSIA Studies in International Security).* Boston: MIT Press, 1999.

United States Department of Defense. *21st Century Bioterrorism and Germ Weapons: U.S. Army Field Manual for the Treatment of Biological Warfare Agent Casualties (Anthrax, Smallpox, Plague, Viral Fevers, Toxins, Delivery Methods, Detection, Symptoms, Treatment, Equipment).* Washington, D.C.: Progressive Management, 2001.

SEE ALSO

Air Plume and Chemical Analysis
Biocontainment Laboratories
Bomb Detection Devices

Chemical and Biological Mass Spectrometer (CBMS).

SEE *Oak Ridge National Laboratory (ORNL).*

Chemical Biological Incident Response Force, United States

JUDSON KNIGHT

The Chemical and Biological Incident Response Force (CBIRF) is a unit of the United States Marines devoted to countering chemical or biological threats at home and abroad. Activated in 1996, the unit served a number of protective functions. Since the terrorist bombings of September 11, 2001, however, its prominence has increased dramatically. Now part of the 4th Marine Expeditionary Brigade (MEB), it has performed homeland security functions that included the removal of suspected toxic agents from House and Senate office buildings during a rash of anthrax attacks in late 2001.

Background and Mission

Chemical agents have been a widespread threat since World War I, when first used by German forces on the Eastern Front in 1915. Soon the British developed their own chemical weapons, and the age of chemical warfare began, forever altering the battlefield equation. Use of chemical weapons by Saddam Hussein on Kurdish civilians, use by both Iran and Iraq during their prolonged war in the 1980s, and use during the 1994 and 1995 attacks by Aum Shinrikyo (a Japanese cult) that released deadly sarin gas into the Tokyo subways and killed 12 civilians, demonstrate that both military and civilian personnel are increasingly vulnerable to chemical attacks.

On June 21, 1995, partly in response to the Aum Shinrikyo attacks, as well as the Oklahoma City bombing on April 19 of that year, the administration of President William Jefferson Clinton issued Presidential Decision Directive 39, "United States Policy on Counterterrorism." The directive called for a number of specific efforts to deter terrorism on America's shores, as well as that against Americans and allies abroad. In response to the need for a response team to deal with chemical and biological threats, the United States Marine Corps established CBIRF (the first two words are sometimes rendered as "Chemical Biological" or "Chemical, Biological) on April 4, 1996.

Training exercises. Writing in the Marine Corps magazine *Leatherneck,* Margaret Bone described CBIRF thus in early 1999: "It's new, it's unique to the Armed Services, and right now, it's the only quick reaction force in the world equipped to help in the aftermath of a chemical, biological, or radiological (nuclear) attack." But the writer went

on to note that "CBIRF is not a counterterrorist group, and it's not direct-action oriented, though there is a security element of more than 120 Marines, with the capability to increase that strength as needed." In the words of a force protection element commander for CBIRF, "We are a consequence management force. Our mission is to respond, to come in and save lives. We bring the full package: self-contained, expeditionary, and task-organized."

During the spring and early summer of 1996, CBIRF was deployed for training in a variety of environments throughout the United States. Its members closely studied the bombing that took place at Centennial Olympic Park in Atlanta on the night of July 27, and practiced coordinating a response with local fire and police. They also undertook an experiment at the Citadel, a military college in Charleston, South Carolina, where CBIRF personnel acted to control lethal agents released by a mock chemical weapons plant. Moving beyond training to real-world situations, CBIRF provided security for President Clinton's second inauguration in January 1997, and for the Summit of Eight in Denver, Colorado, that following summer.

A changing role. In the aftermath of the September 11, 2001, terrorist attacks on the United States, CBIRF's mission became incorporated into the 4th MEB, along with the Marine Security Force Battalion, the Marine Security Guard Battalion, and the new anti-terrorism battalion. (The latter had evolved from the 1st Battalion, 8th Marines, which had been hit in the 1983 terrorist bombings of United States Marine barracks in Lebanon.) In December 2001, CBIRF sent a 100-member initial response team into the Dirksen Senate Office Building alongside Environmental Protection Agency (EPA) specialists to detect and remove anthrax. A similar mission was undertaken at the Longworth House Office Building in October, during which time samples were collected from more than 200 office spaces.

■ FURTHER READING:

PERIODICALS:

Bone, Margaret. "Marines Provide Safety Net to Terrorist Threat." *Leatherneck* 82, no. 2 (February 1999): 50–53.

Cabellon, Paul C. "CBIRF Takes the (Capitol) Hill." *Leatherneck* 85, no. 2 (February 2002): 19.

Garamone, Jim. "Marines to Stand up Anti-Terror Brigade." *Pentagon Brief* (October 2001): 5.

Vogel, Steve. "Cooler Name Prevails for 'Hot' New Marine Corps Club at Indian Head." *Washington Post.* (April 26, 2001): T15.

SEE ALSO

Chemical Safety: Emergency Responses
Chemical Warfare

Chemical Safety and Hazard Investigation Board (USCSB), United States

■ CARYN E. NEUMANN

The United States Chemical Safety and Hazard Investigations Board (USCSB) is a federal agency formed to identify the causes of chemical accidents. Created in 1990 as part of an amendment to the Clean Air Act, the USCSB did not begin functioning until it received funding in 1998. Although its purpose overlaps that of other federal agencies, notably the Occupational Safety and Health Administration (OSHA), the Environmental Protection Agency (EPA), and the National Transportation Safety Board (NTSB), the USCSB differs from these organizations in that it does not have the power to make or enforce rules affecting the routine day-to-day activities of businesses. Instead, the USCSB makes a unique contribution to the protection of workers, the public, and the environment by investigating chemical accidents in the country and attempting to prevent future mishaps. The only regulations put into place by the fact-finding agency involve the reporting of chemical incidences.

The establishment of the Washington, D.C.-based USCSB is a result of the belief that existing hazard investigation agencies, like OSHA, EPA, and NTSB, focus on violations of existing rules while ignoring factors that contribute to a chemical accident, but which do not constitute a violation of existing rules and regulations. By creating this independent, scientific, investigatory agency and modeling it after the NTSB, Congress hoped to produce fuller accident reports that could then be used to formulate new regulations and policies to prevent future dangerous chemical spills and explosions. The amended Clean Air Act of 1990 that gave birth to the USCSB directs the board to investigate and report on the circumstances and the probable causes of chemical incidents resulting in a fatality, serious injury, or substantial property damages; recommend measures to reduce the likelihood or the consequences of such accidents and propose corrective measures; and, lastly, to establish regulations for reporting accidental releases. The board has no enforcement authority, does not issue fines or penalties, and essentially plays a very limited regulatory role.

Accidental releases of toxic and hazardous chemicals occur frequently and often have serious consequences. The USCSB is notified of every chemical release in the country and then decides which accidents to investigate. It is required to coordinate its activities with OSHA, NTSB, and EPA, but when an accident involves transportation, NTSB is the lead agency. Board members, appointed by the president to five-year renewable terms and confirmed by the Senate, are ultimately responsible for the conduct of investigations and the content of accident reports.

Staffers and contractors conduct the actual investigations, which typically involve extensive site visits, evidence collection, and analytical work. Investigators may issue brief summary or detailed investigative reports. Some investigations may conclude without the issuance of any report. Accident reports must be approved by a majority vote of the five board members before they are issued. As of 2000, the USCSB had issued only a handful of reports, in part because of insufficient staffing but also as a result of serious disagreements among board members. Staff levels have since been raised and the board has established a more harmonious working arrangement. The agency is in the process of developing the Chemical Incidents Reports Center, an online database of chemical incidents that have occurred worldwide, in the hopes that the site may inspire researchers to investigate the incidents that the USCSB cannot examine for lack of resources.

The rise in global terrorism and the corresponding fear of a terrorist attack that utilizes chemicals makes the USCSB an important component of American homeland security. By identifying hazardous practices, the agency promotes preventive actions by the public and private sectors that may make it more difficult for terrorists to create chemical incidents.

■ FURTHER READING:

BOOKS:

United States General Accounting Office. *Chemical Safety Board: Improved Policies and Additional Oversight Are Needed.* Washington, D.C.: GPO, 2000.

———. *Chemical Safety Board: Realigned Management Faces Serious Challenges: Testimony Before the Subcommittee on Veterans Affairs, Housing and Urban Development, and Independent Agencies, Committee on Appropriations, U.S. Senate.* Washington, D.C.: GPO, 2000.

ELECTRONIC:

United States Chemical Safety and Hazard Investigation Board. "Chemsafety.gov." <http://www.chemsafety.gov/about> (January 19, 2003).

SEE ALSO

Chemical Safety: Emergency Responses
Chemical Warfare
Chemistry: Applications in Espionage, Intelligence, and Security Issues
NTSB (National Transportation Safety Board)

Chemical Safety: Emergency Responses

■ JUDSON KNIGHT

When the United States as a whole, or any portion or property of the federal or state governments, is threatened by a chemical hazard, a host of agencies go into action. Communities, neighborhoods, and localities are also encouraged—and in some cases required—to develop their own emergency response plans. In the event of a chemical threat, communities are protected by provisions in the Emergency Planning and Community Right-to-Know Act (EPCRA). Passed by Congress in 1986, EPCRA establishes guidelines whereby federal agencies assist local communities in the event of a toxic chemical spill or related incident. EPCRA also provides a framework for action both by citizens and state governments.

There are numerous federal offices assigned to handle threats involving the release, whether intentional or accidental, of hazardous chemicals. Most notable among these is the Coast Guard National Response Center, the first point of contact for information on hazardous-waste spills and a host of other threats to the environment or infrastructure. Within the Department of Defense, the U.S. Army and Marines both have forces designed to respond to chemical threats, as do a number of other departments of the federal government. Likewise, Washington oversees civilian-run installations, such as the Atmospheric Release Advisory Capability, to monitor chemical and other threats. These and other agencies are discussed elsewhere; in the present context, the primary concern is the local, civilian response to chemical hazards.

EPCRA provides a response plan. Motivated by concerns raised by the disaster in Bhopal, India, where in 1984 some 2,000 people lost their lives due to an accidental release of toxic chemicals, Congress passed EPCRA. The latter established requirements for federal, state, and local governments, Indian tribes, as well as for industry, with regard to emergency planning and "community right-to-know" concerning toxic chemicals. In addition to emergency planning and emergency release notification, EPCRA addresses hazardous chemical storage reporting requirements and toxic chemical release inventories.

Under the provisions of EPCRA, each state governor appoints a state emergency response commission (SERC). The SERCs have in turn designated a total of about 3,500 local emergency planning districts nationwide. For each of these, the SERC appoints a local emergency planning committee (LEPC). Under the guidance of the SERC, the LEPC develops a community emergency response plan

A chemical, biological incidence response force (CBIRF) responds to a mock emergency at the Defense Language Institute in Monterrey, California. AP/WIDE WORLD PHOTOS.

designed to identify threats, establish workable emergency procedures, assess preparedness, train local response teams, and take steps to maintain supplies and schedules in preparation for any possible threat.

Federal assistance. In the event of a terrorist attack involving hazardous chemicals, guideline provisions direct that local authorities should establish an incident command system that may eventually become a unified command involving federal authorities. Under such circumstances, the Federal Bureau of Investigation is usually designated the lead federal agency. Meanwhile, the Federal Emergency Management Agency acts as the lead office for coordination of federal support to state and local personnel. Also involved are the National Response Team, Environmental Protection Agency (EPA), Department of Health and Human Services, and Department of Defense.

In accordance with the federal response plan, a national contingency plan for response to disasters, federal agencies are grouped into one of 12 functional areas for emergency support functions (ESFs). For example, EPA, which is heavily involved in oversight regarding EPCRA compliance and preparedness, falls under ESF 10, Hazardous Materials. EPA personnel work to determine the nature of the hazardous substance released, and follow up with environmental monitoring, decontamination, and long-term cleanup of the affected site.

FURTHER READING:

BOOKS:

The EPCRA Compliance Manual: Interpreting and Implementing the Emergency Planning and Community Right-to-Know Act of 1986. Chicago: American Bar Association Section of Environment, Energy, and Resources, 1997.

EPCRA: Emergency Planning and Community Right-to-Know Act. Chicago: American Bar Association Section of Environment, Energy, and Resources, 2002.

EPCRA Section 313 Questions and Answers: Section 313 of the Emergency Planning and Community Right-to-Know Act, Toxic Chemical Release Inventory. Washington, D.C.: United States Environmental Protection Agency Office of Pollution Prevention and Toxics, 1999.

ELECTRONIC:

RCRA, Superfund, and EPCRA Call Center. <http://www.epa.gov/epaoswer/hotline/> (January 29, 2003).

SEE ALSO

Coast Guard National Response Center

Hazardous material response team members don protective gear during an exercise designed to train for an emergency involving chemical weapons stored in the U.S. Army arsenal at Pine Bluff, Arkansas. AP/WIDE WORLD PHOTOS.

Homeland Security, United States Department
United States, Counter-Terrorism Policy

Chemical Warfare

BRIAN HOYLE

Chemical warfare involves the aggressive use of bulk chemicals that cause death or grave injury. These chemicals are different from the lethal chemical compounds that are part of infectious bacteria or viruses. The latter constitute biological warfare.

History of Chemical Warfare

The use of chemicals in warfare began centuries ago, when early combatants learned that smoke from burning sulfur caused discomfort when it drifted into enemy fortifications. The dawn of modern chemical warfare occurred during World War I. On April 15, 1915, German forces released about 160 tons of chlorine gas into the wind near the Belgian village of Ypres. The clouds of the gas drifted into Allied forces, killing some 5,000 soldiers. Two days later, another chlorine attack at the same village killed 5,000 more soldiers.

During the remainder of World War I, German and British forces used chlorine gas, and other chemicals (i.e., mustard gas and phosphene) with increasing tendency. Estimates are that approximately 113,000 tons of chemical weapons were used from 1915 to 1918, killing some 92,000 people and injuring over one million people.

The aerial release of chemicals brought unpredictable results at the mercy of prevailing winds. Shifting winds could send the deadly cloud back to the attacking troops. Later during World War I, more sophisticated use of chemical weapons began. For example, the French used shells filled with an irritant to the eyes, skin, and lining of the nose and lungs, and the Germans fired lead balls coated with similar irritant.

The horrors of chemical warfare during World War I prompted the drafting of the Geneva Protocol of 1925, which banned chemical and biological weapons of warfare. The protocol was initially signed by 38 nations (now over 130 nations). As history has shown, the protocol has

Terrified children run from their village after a U.S. napalm attack during the Vietnamese War. This photograph was pivotal in promoting awareness of the suffering of the Vietnamese people during the war and was particularly effective in arguments against the use of napalm. AP/WIDE WORLD PHOTOS.

not stopped the use of such weapons by rouge states or fringe elements in order to commit terrorism.

Aerial releases of lethal chemicals did not occur in World War II. However, the Germans developed a new class of chemical weapon called nerve agents. During the 1930s and 1940s, agents such as Tabun, Sarin, and Soman were created.

Chemical warfare research continued during the Cold War tensions during the 1950s. During this time, military chemists in the United Kingdom and then in the United States adapted insecticides to produce the most lethal chemical agent then known. The agent was code named VX. The potency of VX was accidentally demonstrated in 1968, when a testing accident at the VX manufacturing plant in Dugway, Utah killed over 6,000 sheep.

During the Vietnam War of the 1970s, the U.S. use of defoliants—chemicals that killed vegetation, permitting a clearer detection of the enemy—was extensive. One of these compounds, Agent Orange, has become infamous as the alleged cause of a variety of physical ailments in veterans of the conflict.

In the last few decades, chemicals have become the tools of terrorists. A particularly well-known example is the release of Sarin gas into the Tokyo subway system by the religious cult Aum Shinrikyo in March of 1995. The gas killed 12 people and injured over 5,500 people in 16 stations.

Chemical Warfare Agents

There are several classes of chemical warfare agents, based on their effects:

- compounds that cause choking or that irritate the lungs,
- blister agents (also called vesicants),
- blood agents,
- nerve agents,
- herbicides, and

A member of a biological and chemical warfare response team wearing a protective suit carries a suspicious envelope in a bag at Jerusalem's Malcha shopping mall in 2001. AP/WIDE WORLD PHOTOS.

- incendiaries

Choking and irritant agents. There are a number of compounds that cause choking or irritation of lung tissue. Examples include chlorine, phosgene (carbonyl chloride), diphosgene, chloropicrin, ethyldichloroarsine, and perflurorisobutylene.

Chlorine gas is suffocating and quickly burns tissues in the nose, mouth, and lungs. The burned tissue can die and slough off, causing lasting damage. Chlorine gas dissipates in the air very quickly. If exposure is not too long, than damage can be minor. In contrast, the compound called disphosgene is a liquid at room temperature, and so persists much longer.

Blister agents. As their name implies, blister agents cause the formation of large and painful blisters on the skin. Eye and lung tissue can also be damaged. A well-known example of a blistering agent dating from World War I is mustard gas. The damage to cells of the skin cause blistering up to 24 hours after exposure to mustard gas. These blisters take a long time to heal and can send the body into a lethal shock reaction.

Other examples of blistering agents include nitrogen mustard, lewisite, and phenyldichloroarsine. The latter compound is a liquid, which can be sprayed onto an enemy or released from a balloon, helicopter, or airplane.

Blood agents. These compounds interfere with the body's ability to transport oxygen in the bloodstream. This is done by either blocking the use of oxygen by cells in the body or by blocking the ability of the blood to take up the oxygen. Examples include hydrogen cyanide (also called prussic acid), cyanogen chloride, arsine, carbon monoxide, and hydrogen sulfide.

Hydrogen cyanide is initially a liquid at room temperature, but it quickly evaporates. This compound is noteworthy in recent world history, as it was used by Iraq in 1988 on an attack on the Kurdish town of Halabja during the Iran-Iraq war. Because of its past use by Iraq, hydrogen cyanide was one of the major concerns of United Nations inspectors who inspected various facilities in Iraq during the winter of 2003.

Compounds such as arsine and carbon monoxide destroy the ability of the hemoglobin component of the blood to bind oxygen. Arsine does this by destroying the red blood cells. Carbon monoxide binds to hemoglobin, blocking the binding of oxygen.

Nerve agents. Compounds that are classified as nerve agents interfere with the body's transmission of nerve impulses. This is done by disrupting the activity of a chemical called acetyl cholinesterase, which functions to bridge the gap between adjacent nerve cells, permitting an electrical nerve signal to pass from one nerve cell to the next.

Nerve agents were first developed in 1936, following the development of organophosphate types of pesticides. The first nerve agent that was made is called Tabrun. It is a member of what is known as the G series of nerve agents. Other G series members are Sarin and Soman. Sarin is particularly lethal; a small amount absorbed through the skin can kill a man within two minutes. When inhaled, death occurs within 15 minutes. Sarin is infamous as the gas released into the Tokyo subway system by the fringe group Aum Shinrikyo in 1995.

Another series of nerve agents are called the V series. Members of this series—which are commonly abbreviated according to their chemical composition—are more potent than the agents of the G series. As well, they persist longer in the environment. They can, for example, be applied to surfaces like roads as a slime.

Examples of V series agents include VX, VE, VG, and VM. VX is extremely potent; a drop of the liquid absorbed through the skin is lethal within a few hours without treatment.

Nerve agents can be contained in missiles or in canisters for lengthy time periods. Examination of caves in Afghanistan that were used as strongholds by the terrorist group al Qaeda has revealed evidence of stores of Sarin and VX.

Herbicides. Herbicides are chemicals that kill vegetation. Such chemicals are often used in everyday life to keep lawns free of weeds (although more environmentally-friendly alternatives are becoming popular). When used in war, herbicides are weapons of mass destruction to foliage. Destruction of plants and the resulting loss of leaf cover remove much of the concealment for an enemy in a forested area. These philosophies led to the massive use of Agent Orange by the United States in the Vietnam War in the 1970s. Since that war, the damaging effects of herbicides like Agent Orange and paraquat on the human nervous and immune systems has become evident.

Incendiaries. Incendiaries are chemicals that cause fires. In warfare, they are also to remove vegetation. An infamous incendiary is napalm. Napalm is a mixture of naphthenic acid, coconut fatty acids, and palm oil. In addition to its highly flammable property, napalm absorbs into exposed skin, where it can cause severe burns if ignited. Napalm was used as an offensive weapon by the United States during the Vietnam War.

Modern Day Chemical Warfare

In 2003, the use of chemical weapons remains a threat from rogue states and terrorists. Current world attention is focused on the former chemical warfare capabilities of Iraq. It is known that Iraq engaged in chemical warfare research and weaponization in the 1980s and 1990s, and as of early 2003, before the U.S. war in Iraq, had not fully complied with United Nations resolutions requiring disclosure and destruction of their chemical weapons program.

FURTHER READING:

BOOKS:

Ellison, D. Hank. *Handbook of Chemical and Biological Warfare Agents.* Boca Raton: CRC Press, 1999.

Harris, Robert, and Jeremy Paxman. *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare.* New York: Random House, 2002.

PERIODICALS:

Macintrye, A. G., C. G. W. Eitzen, Jr., R. Gum, et al. "Weapons of Mass Destruction Events with Contaminated Casualties: Effective Planning for Health Care Facilities." *Journal of the American Medical Association* no. 283 (2000): 252–253.

Munro, N.B., S.S. Talmage, G.D. Griffin, et al. "The Sources, Fate, and Toxicity of Chemical Warfare Agent Degradation Products." *Environmental Health Perspectives* no. 107 (1999): 933–974.

Nakajima, T., S. Ohta, Y. Fukushima, et al. "Sequelae of Sarin Toxicity at One and Three Years after Exposure in Matsumoto, Japan." *Journal of Epidemiology* no. 9 (1999): 337–343.

ELECTRONIC:

How Stuff Works. "How Biological and Chemical Warfare Works." 2002. <http://www.howstuffworks.com/Biochem-war.htm>(10 January 2003).

SEE ALSO

Chemical and Biological Detection Technologies
USAMRICD (United States Army Medical Research Institute of Chemical Defense)

Chemistry: Applications in Espionage, Intelligence, and Security Issues

JUDYTH SASSOON

From the detection of forgeries to the identification of criminal suspects, the techniques of chemistry have many applications in areas relating to espionage, intelligence and security. Analytical chemistry, the branch of chemistry concerned with the analysis of substances, is of particular importance. The study of the chemical composition of a compound gives a qualitative analysis, while the determination if its concentration involves quantitative analysis. Chemists utilize a range of different skills to help security services in areas as wide-ranging as drugs, firearms, toxicology, and fiber analysis. For example forensic chemistry concerns the detection and characterization of substances at crime scenes. These might include bomb fragment analysis, fire investigations, firearms discharge analysis, poison or toxin analysis and various other types of chemical residue analysis. In these instances, sophisticated analytical techniques are used to identify minute residues of paint, fire accelerants, human hair, body fluids or tissues. Advanced spectroscopic and separation procedures can often clarify confusing circumstantial evidence.

Modern analytical chemical laboratories can use both classical "wet" methods (gravimetric or volumetric procedures) employing chemical reactions to perform the analysis, or instrumentation, which makes critical measurements during an analysis. A number of separation methods are useful either prior to chemical analysis or as direct methods in the analysis. These methods include distillation, selective precipitation, filtration, osmosis, and extraction. Most analytical procedures in the forensic laboratory now use some instrumentation and many are fully automated. The instrument-based methods of analysis are divided into categories according to the type of process used to perform the analysis. Optical instruments such

Chemistry students at the National School of Biological Science in Mexico City work with samples of anthrax in October 2001, without customary controls such as biosafety suits and ventillation hoods that are imposed by most other countries. AP/WIDE WORLD PHOTOS.

as spectroscopes comprise the first major group and measure electromagnetic radiation, which is either absorbed (absorption spectroscopy) or emitted (emission spectroscopy) by a sample. The wavelength at which this occurs can be used for qualitative analysis, while the amount of radiation can be useful for quantification. Spectroscopy involves the use of radio, infrared, ultraviolet, visible and x-ray regions of the electromagnetic spectrum.

Of the instrumental separation methods, chromatography and its variations are the most widely used. Chromatography is a technique whereby a mixture is separated into its components by the reactive adherence of each component to a stationary phase while a mobile phase passes over the stationary phase. Chromatography is divided into categories, depending on the physical state of the stationary and mobile phases. Examples include gas-solid, gas-liquid, liquid-liquid or liquid-solid chromatography and also thin layer, paper, and gel permeation chromatography. The applications of these techniques in forensics can provide much intelligence information in the form of physical evidence that can be used subsequently by security forces.

The techniques above are frequently employed in the analysis of substances from sites of criminal or terrorist activity. For example, the examination of debris at the scene of a fire can provide data to show if the fire started accidentally or deliberately. The correct identification of the source and the presence of accelerants can link the fire to an arson suspect. Similarly, detailed laboratory analysis of debris and trace evidence from explosion scenes (domestic, commercial, suspected criminal, or terrorist) as well as a detailed chemical knowledge of the capacity of materials to form explosions can yield information showing the nature of the source. If a firearm is discharged, gunshot residue such as burnt or partly burnt gunpowder and components from the primer compound (e.g. lead, barium, and antimony are also thrown out into the surroundings). Firearms discharge residues that may be deposited on any object near to a gun when it is fired, or on any object that subsequently touches the gun. When an object is shot at a relatively close range, gunshot residues are deposited, and sometimes violently impacted, onto the target. The nature and distribution of these residues can match a target to a weapon and can also be used to determine the distance from the gun's muzzle from point of impact.

Chemical analysis becomes important in the study of glass and building materials from the site of an incident. Glass is frequently broken when a criminal offence takes place and building materials such as plaster, mortar, bricks,

slate or loft insulation may be dislodged if illegal entry is gained into a building. Fragments of either can adhere to clothing and may be recovered from a suspect. A comparison of these with similar materials at the incident scene can link a suspect to a crime. Similarly, paint can be conveyed between surfaces following contact, and analysis of paint composition and layering can be used to connect paint fragments to a crime. The most common occurrence is the transfer of paint between vehicles or objects in road traffic accidents. Paint fragments can also adhere to items of clothing following contact with loose flakes on surfaces such as windows at the scene of burglaries. Paint analysis can also be applicable in circumstances where painted car parts are suspected of having been exchanged between vehicles.

Chemical analysis of cloth fibers, stains and organic materials such as human hair and body fluids provide vital evidence in, for example, homicide cases. In the past, biochemical blood typing using antisera and the matching of hair types could not provide absolute identification of a suspect or victim, although it could narrow the possibilities down. Today, however, even minute quantities of blood, semen, skin cells and hair can yield DNA profiles. DNA from different individuals differs in base sequence and, theoretically every individual with the exception of identical twins, can be identified solely on the basis of their DNA sequences. However, a complete DNA analysis of individuals is a daunting and time consuming task because of the many millions of bases in the human genome. The possibilities for routine genome analysis do not exist at present. Instead, DNA matching is performed by analysing shorter, highly polymorphic single locus genes such as the VNTR genes. This method can establish a "DNA signature" for almost any individual. Biochemical analysis of these sequences can determine whether two DNA samples are from the same person, related people, or unrelated people. Though these methods also do not yield absolute certainties, they are nevertheless more precise than traditional methods such as blood typing.

DNA profiling as a crime intelligence aid involves the use of basic chemical and biochemical procedures. DNA is chemically isolated from the cell or tissue sample, amplified using the enzymes in the polymerase chain reaction (PCR), and then analyzed by electrophoretic methods. The DNA profile from the scene of the crime can be compared with a DNA profile from a suspect and a match can link the suspect to the crime. If there is no suspect, the DNA profile can be matched with profiles stored on to the National DNA Database (NDNAD). If there is no match with the NDNAD, it is sometimes decided to carry out an intelligence-led screen (a mass DNA screen). A target group of individuals, for example, men within a certain age range living in a town or area, are asked to voluntarily provide DNA samples, which are then analyzed and compared with a profile linked to a particular crime. Samples from volunteers are not stored on the NDNAD, and are destroyed if they do not match the crime profile.

Thus, the sensitivity and accuracy of chemical analytical methods lie at the heart of forensic science and, with the advances in biochemical techniques, provide essential tools for crime intelligence investigations.

FURTHER READING:

BOOKS:

Bodziak J., and Jon J. Nordby. *Forensic Science: An Introduction to Scientific and Investigative Techniques.* CRC Press, 2002.

PERIODICALS:

Casagrande, R. "Technology against Terror." *Scientific American.* 287 (2002):59–65.

"Early Warning Technology." *"Med Device Technol* 13 (2002): 70–2.

SEE ALSO

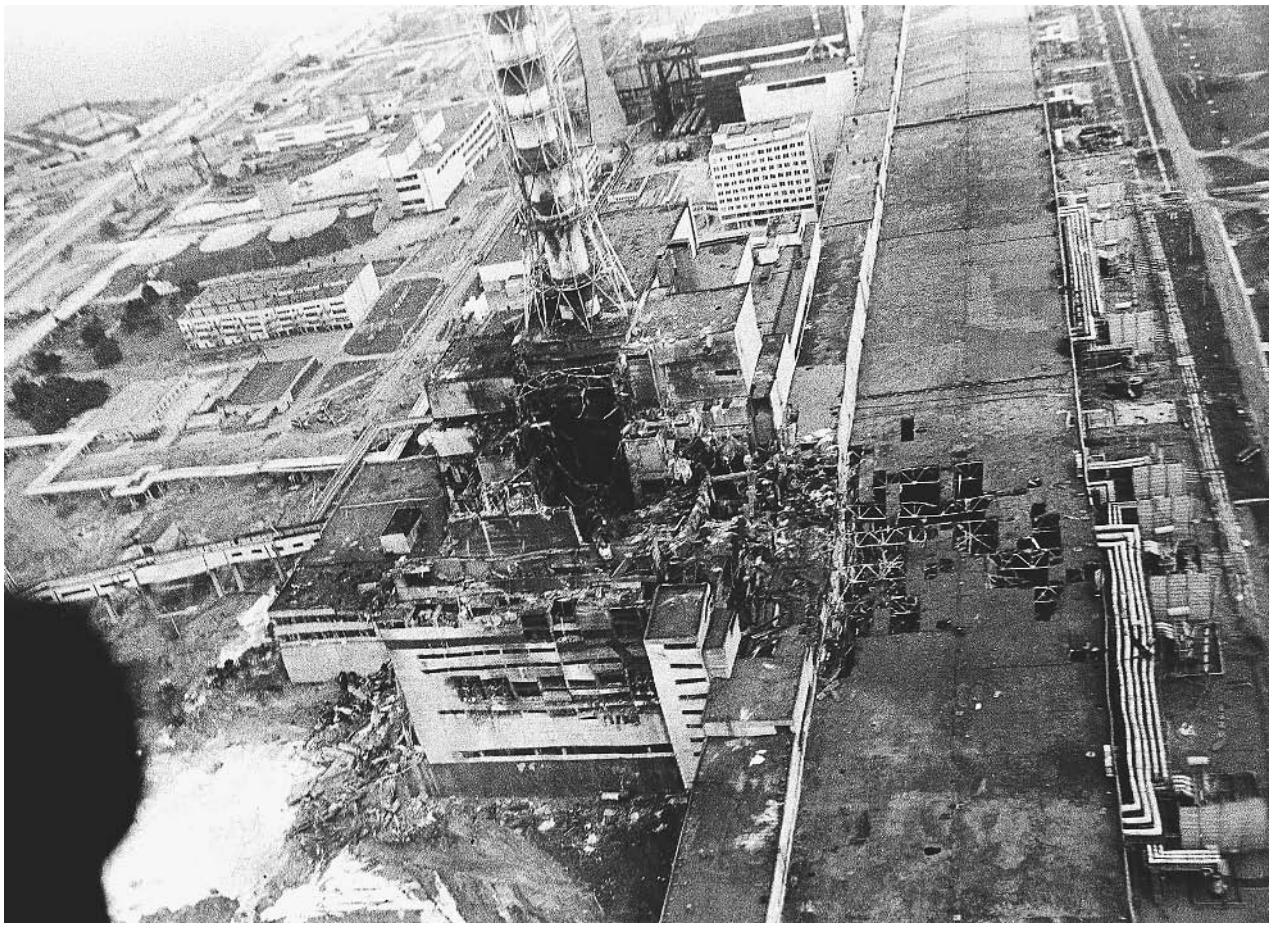
Biodetectors
Crime Prevention, Intelligence Agencies
Explosive Coal
Forensic Science
Microbiology: Applications to Espionage, Intelligence and Security
Molecular Biology: Application to Espionage, Intelligence and Security Issues

Chernobyl Nuclear Power Plant Accident, Detection and Monitoring

LARRY GILMAN

On April 26, 1986, a nuclear reactor in the town of Chernobyl (in the Ukraine, then a member state of the Soviet Union) exploded, collapsing the building in which it was located and releasing a radioactive plume that deposited material over much of Europe and Scandinavia. Although the Soviet government was unwilling to release information, satellite photographs by military and civilian satellites, as well as direct radiation measurements downwind, confirmed the event.

The accident and its consequences. The town of Chernobyl, some 60 miles (96 km) north of the city of Kiev (population 2.5 million), is the site of a nuclear electricity-generating station comprising four identical units of the Soviet-designed RBMK1000 type. Each of the four units is designed to produce 1,000 megawatts of electricity; one of the units is still in operation. On April 25, 1986, operators began an experiment at Unit No. 4 to take advantage a scheduled annual maintenance shutdown. The goal of the



An aerial view of the Chernobyl nuclear power plant is shown in this 1986 photo made a few days after the explosion in Chernobyl, Ukraine. AP/WIDE WORLD PHOTOS.

experiment was to see if the station's turbine generator could deliver temporary power to certain cooling pumps after cutoff of its steam supply. As a first step, the unit's operators deliberately disconnected the reactor's emergency core cooling system; such a system is necessary because every large reactor core can generate millions or billions of watts of thermal power (heat); this energy must constantly be removed by a flow of coolant, or the core may cause a steam explosion, melt down, or even (in reactors using highly-enriched fuel) a relatively small nuclear explosion. The emergency core cooling system is supposed to keep the core cool when the usual systems have failed. Unit No. 4's operators had not left the emergency core cooling system disconnected, but had committed a series of further errors that allowed the reactor's power output to fall far below planned levels. In attempting to restore the reactor's power output, the operators caused it to go out of control. In a period of approximately 5 seconds, the core's heat output increased exponentially to the point where a steam explosion occurred. This blew a 1,000-ton concrete lid off the reactor and damaged the roof of the reactor hall.

A few seconds later, an even larger explosion occurred when hydrogen released by the breakdown of water exploded. Burning chunks of graphite (a form of carbon of which 1700 tons were present in the reactor core) flew through the air and landed on other parts of the complex, starting fires. The remaining graphite started to burn, releasing a plume of radioactive smoke that was carried by the wind first north, toward Scandinavia, and later west and south over much of the rest of Europe. The graphite fire burned for over a week, but was finally brought under control by firefighters, many of whom died of radiation burns. The reactor was eventually encased in a shell or "sarcophagus" of concrete. In the late 1990s, United States and Ukrainian engineers worked together to evaluate conditions inside the sarcophagus, which may be vulnerable to collapse in an earthquake. The sarcophagus may need to be strengthened to prevent future releases of radioactivity from the site.

The Chernobyl accident is one of the worst nuclear accidents to date, surpassed only by the explosion at the Chelyabinsk-65 plutonium-processing facility in the Ural Mountains in 1957, which was kept secret for decades by

the Soviet Union. Over 20 million curies of radioactive material were lofted into the atmosphere by the Chernobyl explosion and ensuing fire. Some of this material sifted down over nearby towns and countryside, while the rest was spread over Europe by winds, exposing 10 to 20 million people to significant fallout. The number of deaths caused immediately by the accident was in the dozens, but the number of deaths caused in the long term by radiation-induced cancer and other health damage will never be precisely known. Although initially dismissed by experts in the West as exaggerations, reports of 30-to-100-fold increases in thyroid-cancer rates among children in Belarus, northern Ukraine, and parts of the Russian Federation have recently been confirmed.

Nevertheless, the accident could have been worse. Total "meltdown," in which the molten uranium of the ruined core would have coalesced into a single superheated mass and melted its way down to the groundwater below the plant, causing a violent steam explosion and dispersing even larger quantities of radioactive material, did not occur.

The role of satellite imagery. The Chernobyl accident occurred on April 26, 1986, but the Soviet government did not acknowledge the event until April 28 and denied the extent of the disaster for some days thereafter. However, the West quickly had definite knowledge of the accident's occurrence. Radiation was detected in Sweden the day after the explosion and was soon being monitored by aircraft equipped with radiation-detection devices, including the U.S. Air Force's 55th Weather Reconnaissance Squadron. Also, Soviet communications were monitored by a geostationary U.S. military satellite called the Vortex, and both military and civilian Earth-imaging satellites were soon in position to image the site. Because of Soviet reluctance to admit observers or release videos, photographs, or accurate announcements about the accident, and because downwind radiation measurements could give no specific information about what was happening at Chernobyl, much news attention in the West focused on the satellite photographs.

The United States' KH-11 spy satellite provided high-resolution images of Chernobyl to the U.S. government on the afternoon of Tuesday, April 29th, three days after the initial explosion. The KH-11, also known as the Keyhole satellite, was the latest in the KH series of spy satellites that the U.S. began launching in the 1960s, primarily to spy on military activity in the Soviet Union. The KH-11 (whose capabilities were still secret in 1986) could resolve details on the ground down to 4–6 inches (10–15 cm) across. (It has since been replaced by the KH-12 satellite, with a resolution of 2.45 inches [6 cm].) U.S. officials were, therefore, soon as well informed about the Chernobyl accident as vertical views could make them. These images were not, however, released to the public; instead, the U.S. government's knowledge was filtered to the media through announcements.

The first civilian satellite to image the accident site was the United States' LANDSAT, which follows a polar orbit 260 to 570 miles (420 to 912 km) high and takes telescopic pictures of the Earth as it passes beneath. The first LANDSAT (for land-sensing satellite) was launched by the U.S. in 1972, and a series of LANDSATs have been launched as technology has improved. (The seventh LANDSAT in the series is in orbit as of 2003.) LANDSAT images first became available to TV news media on Wednesday, May 3, 1986, only one day after KH-11 images became available to the government. The resolution of the LANDSAT images was comparatively poor, however, being on the order of tens of meters, rather than of centimeters. Nevertheless, they gave visual access to the layout of the reactor complex and cooling pond. Infrared LANDSAT imaging showed both the fire in Unit No. 4 and the chilling of the pond, which indicated that the three remaining reactors in the complex had been shut down.

Several days after the accident, a French satellite named SPOT (for System Probetoire d'Observation de la Terre) was able to provide higher-resolution images to news media. These images were also seen throughout Europe and the United States; on May 1, 1986, for example, ABC news broadcast SPOT infrared photos that showed a plume of hot air trailing from the reactor building.

However, it is doubtful that these nonmilitary satellite images were of any substantive benefit. Despite warnings from professional photo interpreters, announcers on the CBS and NBC television networks announced that the LANDSAT images revealed two reactors on fire, a claim that had to be retracted. Little actual news was derived from the LANDSAT or SPOT images. They served to lessen the sense of mystery surrounding the Chernobyl disaster, but did not supply any specific information that was not already available from other sources. They confirmed—but also, through misinterpretation by amateur analysts, confused—reports already received from official sources.

The KH-11 satellite data, on the other hand, were probably of some utility. They at least gave U.S. officials independent information about the scope of the disaster. However, there was little the West could do with this knowledge. The accident was inside Soviet territory and the response to it was entirely a Soviet affair. Complete cover-up of the event would have been impossible even without spy-satellite imagery, due to the detection of radiation downwind.

Nevertheless, the role of satellite imaging during the Chernobyl accident shows that large-scale disasters can no longer be denied, whether as a whole or in detail, by national governments, given the imaging capabilities of both military and nonmilitary satellites. The basic story of Chernobyl, unlike that of the blowup at Chelyabinsk-65, was public property from the beginning.

FURTHER READING:

BOOKS:

Medvedev, Zhores. *The Legacy of Chernobyl.* New York: W. W. Norton & Company, 1990.

Mould, R. F. *Chernobyl Record: The Definitive History of the Chernobyl Catastrophe.* Bristol, England: Institute of Physics Publishing, 2000.

PERIODICALS:

Alper, Joseph. "Navigating Chernobyl's Deadly Maze." *Science.* 5365 (May 8, 1998): 826–827.

Brugioni, Dino A. "Satellite Images on TV: The Camera Can Lie." *Washington Post.* December 14, 1986.

Williams, Dillwyn. "Cancer after Nuclear Fallout: Lessons from the Chernobyl Accident." *Nature Reviews,* vol. 2 (July, 2002): 543-549.

SEE ALSO

Nuclear Power Plants, Security
Russian Nuclear Materials, Security Issues
Satellites, Spy

Chile, Intelligence and Security

ADRIENNE WILMOTH LERNER

Following a coup on September 11, 1973, Augusto Pinochet assumed power of Chile and for nearly two decades, the dictatorial Pinochet regime created and utilized various intelligence and secret police forces to ferret out and persecute political dissidents. The political prisoners seized by Pinochet's forces became known as the *Desaparecidos*, or Disappeared Ones. Little is known regarding the circumstances of their detainment and subsequent execution, but over 3000 Chilean citizens were killed or disappeared during Pinochet's rule. In 1989, Pinochet lost power in Chile. The subsequent government was left to deal not only with the public memory of the era, but also with a massive restructuring of government agencies, most especially within the intelligence community.

After Pinochet seized power, he established the *Dirección Nacional de Inteligencia* (DINA), or the National Intelligence Directorate in 1974. The agency oversaw military intelligence as well as the national police force. DINA had a paramilitary wing and operated a large secret police force. In 1977, the agency was replaced by the more powerful *Centro Nacional de Información* (CNI), the National Information Center. The CNI performed the same duties as DINA, but also wielded significant judicial powers. No distinction was made between military and civilian accused persons, and the agency directed military tribunals that prosecuted civilians. The CNI was chiefly concerned with internal security, espionage, and protecting the Pinochet regime. The agency maintained records on private citizens and organizations, often tapping phones and intercepting private wire and written communications. Agents also located and captured persons who fled persecution by escaping to neighboring countries.

After the end of the Pinochet regime, the new government dissolved the CNI in 1990. Many former CNI intelligence agents and members of the secret police were reassigned to military intelligence units or the newly created *Dirección de Inteligencia de la Defensa Nacional* (DIDN), the Directorate of National Defense and Intelligence. Unlike its predecessor agencies, the DIDN is chiefly concerned with defense, not internal intelligence. DIDN coordinates the operations of national intelligence forces, sometimes including military intelligence. Though not without controversy in its own right, the agency seeks to distance itself from the legacy of the CNI and DINA secret police forces.

The role of the Chilean national police forces also changed with government and constitutional reforms in 1980 and 1990. Chile has two main national law enforcement forces, both of which also have roles in the intelligence community. The Carabineros, the national uniformed police, are charged with public safety and border patrols. Under the operational direction of the Ministry of the Interior, the police force is actually part of the Ministry of Defense. The Carabineros also have a paramilitary units and a counterintelligence arm that combat drug trafficking and enforce border security. One branch of the special paramilitary forces, the *Dirección de Inteligencia de Carabineros* (DIC), or Intelligence Directorate, is a counter-subversive intelligence unit charged with fighting terrorism. While laws established protecting the rights of detained persons are largely followed by the police forces, several journalists, citizens, and even legislators have charged some of the Carabineros' paramilitary forces with human rights abuses, including arrest, prolonged detainment, and torture of political dissidents.

The second Chilean police force is the Investigations Police, which employs, among other law enforcement strategies, civilian plain-clothes forces that oversee surveillance and apprehension of suspected criminals and terrorists. The agency investigates serious crime, such as fraud, theft, and murder, and aids the Carabineros with intelligence and investigative work. The Investigations Police maintains airport security and operates the National Identification Bureau, which keeps biographical and criminal records of all citizens and issues national identification cards. Like the Carabineros, the Investigations Police has weathered public suspicion for alleged abuses of power.

Chile has two major advisory boards that address issues of national security, intelligence, and defense. The *Consejo Asesor de Seguridad Interior* (CASI), or Internal Security Advisory Council, is comprised of the Minister of the Interior and various military representatives. CASI advises the executive branch on matters of domestic

security. A second committee the *Consejo Asesor Político-Estratégico* (CAPE), or Strategic Political Advisory Council, monitors defense planning and external security threats.

In the Chilean government, the executive branch has constitutionally granted control over the nation's military, intelligence, and police agencies. However, this power was severely checked by constitutional reforms in 1990. The Carabineros and various military branches are now more autonomous and the president must appeal to his National Security Council, *Cosena*, to remove and replace heads of the various departments and services.

Constitutional and governmental reforms enacted since the early 1980s have radically altered Chilean intelligence and security agencies. As past abuses and atrocities are investigated and brought to light by the international community, especially following the 1999 arrest and detainment of Pinochet on charges of human rights crimes, current Chilean intelligence agencies seek to distinguish themselves from the reputation of their predecessors, despite continuing to hold similarly broad powers with limited legal and administrative restraints.

■ FURTHER READING:

BOOKS:

Collier, S., and W. F. Sater. *A History of Chile, 1808–1994,* Cambridge: Cambridge University Press, 1996.

ELECTRONIC:

The Government of Chile. <http://www.gobiernodechile.cl/> (14 January 2003).

China, Intelligence and Security

China is the last communist-dominated world power. The nation reserves veto power on the United Nations Security Council, and is a declared nuclear power. Although censorship and restricted civil liberties persist in China, citizens have witnessed a gradual ease of economic and social restraints. Poverty remains an endemic problem, causing an exodus of people from rural areas into already overcrowded cities. In response, the government prohibited moving between regions and towns without express permission. With the transfer of Hong Kong from British control to Chinese administration in 1997 and the advent of the Internet, the Chinese economy, media, and society have been permeated by Western influences.

In Asia, Chinese politics cast a shadow over smaller satellite states, most especially North Korea. In 2003, North Korea reactivated a nuclear reactor and announced that it possessed the capabilities to produce nuclear weapons and intercontinental ballistic missiles. The development arose international suspicion that North Korea received nuclear materials and technology from its closest ally, China. The Chinese government denies aiding North Korea, and maintains that it adheres to global non-proliferation efforts. The Chinese intelligence community, however, is reluctant to share information about North Korea with Western nations, especially the United States.

China's main intelligence agency is the Ministry of State Security (MSS). The Communist Party of China dominates the Chinese government, especially the intelligence community. Political espionage within China, and on Chinese citizens, is endemic. Government reforms in 1983 created the MSS, restructuring the Chinese intelligence community and revising the mission of its predecessor agency to account for technological advances in intelligence tradecraft. The MSS utilizes human, signals, remote, electronic, and communications intelligence in its varied operations. The main mission of the MSS is to protect national interests and preserve government stability. However, the MSS also aggressively targets United States and European businesses and factories in a broad campaign of industrial and economic espionage.

Chinese military intelligence is divided into operational departments that fall under the administration of the central government and individual branches of the military. The People's Liberation Army (PLA), China's defense force, maintains trained intelligence, counterintelligence, and security forces. The operations of these forces are highly secret, but most operations deal with domestic and regional threats to the government. PLA intelligence also guards military instillations and key assets in the nation's nuclear weapons program. The PLA Navy has its own intelligence force, concentrating on surveillance at sea, signals, and communications intelligence. The PLA Air Force's intelligence forces are known as the Sixth Research Institute. Sixth Research conducts intelligence operations similar to other military and civilian organizations, but is also the primary agency for aerial surveillance.

The Second Intelligence Department focuses on foreign intelligence and espionage against rival nations. In addition to monitoring foreign diplomats and foreign interests within China, the agency also conducts political surveillance of Chinese diplomats abroad. Recently, the Second Intelligence Department received a new mandate to work with the MSS to increase industrial, economic, scientific, and technological espionage efforts, especially in Western nations.

Throughout China there are municipal, regional, and national police forces. The Ministry of Public Security administers the national police force. A military trained police force, Unit 8341 General Security Regiment, provides security for government buildings and personnel, and conducts counterintelligence and anti-terrorism operations. The special police force and intelligence unit is maintained by the General Staff Department.

The Chinese government also maintains secret police forces. These forces are mostly plain-clothes officers who use a network of informers to conduct surveillance and political espionage operations on behalf of the government. Some of these police forces have gained a reputation for their arbitrary imprisonment of citizens and garnered international criticism for use of excessive force and coercion.

A primary duty of China's intelligence and security community is media surveillance and participation in state censorship efforts. The government censors all medium of public expression, but in recent years has placed special emphasis on monitoring electronic communication and the Internet. In 1989, the intelligence forces began monitoring all fax transmissions. Five years later, e-mail communication was declared open to state censorship and surveillance. China's aggressive censorship initiatives monitor political dissidents and anti-government sentiment.

China's news service, Xinhua, provides censored news to China's citizens via television, print media, and radio. The news service also plays a crucial role in China's intelligence community. The bureau analyzes reports from informants, foreign diplomats, foreign journalists and news services, and reports to Chinese government officials. Members of the MSS work within the Xinhua, using its network and journalistic credentials as a mean of gathering intelligence information.

In the first case to reach trial under the 1996 Economic Espionage Act, which banned the theft of trade secrets, Hwei Chen "Sally" Yang was found guilty of economic espionage in 1999. AP/WIDE WORLD PHOTOS.

■ FURTHER READING:

BOOKS:

Ebrey, Patricia Buckley. *The Cambridge Illustrated History of China.* Cambridge University Press, 1999.

Fewsmith, Joseph. *China since Tiananmen.* Cambridge University Press, 2001.

SEE ALSO

Clinton Administration (1993–2001), United States National Security Policy
Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
Korean War
Nixon Administration (1969–1974), United States National Security Policy
North Korea, Intelligence and Security
North Korean Nuclear Weapons Programs

Chinese Espionage against the United States

■ JUDSON KNIGHT

The question of Chinese espionage against the United States animated policy and intelligence circles during the second half of the 1990s, driven by a number of factors, not least of which were allegations that members of the administration of President William J. Clinton had accepted campaign donations from Chinese sources. An investigation by the House Select Committee on U.S. Nuclear Security and Military/Commercial Concerns with the People's Republic of China, chaired by Christopher Cox (R-CA), found that the People's Republic of China (PRC) developed a number of key warheads based on U.S. designs, but failed to establish that this information had come through espionage. Still, the issue of Chinese spying simmered, and finally reached a climactic point with the arrest of Wen Ho Lee, a computer scientist at Los Alamos National Laboratory, in 1999.

In October 1996, the *New York Times, Wall Street Journal,* and *Los Angeles Times* ran a number of stories detailing a connection between John Huang, principal deputy assistant secretary of Commerce for International Economic Policy, and Indonesia's Riady family, which had close ties to China. It would eventually be revealed that the PRC had funneled sizeable contributions to the Democratic National Committee through a number of intermediaries. Critcs pointed out that, near the same time, the Clinton administration approved the sale of defense satellite technology to the PRC.

Meanwhile, concerns had arisen with regard to Chinese weapons technology, its links with U.S. technology, possible espionage against the United States, and security breaches that had facilitated that espionage. These were the issues that sparked the investigation by Cox's committee in 1998.

The PRC had never been involved in the kind of broadly based espionage on American soil that the Soviet Union had conducted through the KGB and its U.S. agents. The Chinese did, however, have an interest in U.S. technology that had led to efforts at covert acquisition noted as early as 1984, in a report by the Defense Intelligence Agency.

The Cox Report, as the findings of the House committee were called, asserted that the Chinese had appropriated information on seven warheads, including the W88, deployed on the D-5 submarine launched-ballistic missile. This information, the committee concluded, had come from one of the U.S. weapons laboratories operated by the Department of Energy (DOE).

The investigation. The House committee completed its seven-month investigation in December 1998, as Clinton's impeachment on unrelated charges loomed (he would eventually be acquitted by the Senate), and published its report in May 1999. In the meantime, the FBI had undertaken an investigation, code-named "Kindred Spirit," of persons who had access to W88 information.

If the Chinese had indeed stolen data on the W88, the theft had occurred in the 1980s, long before Clinton was president; therefore, the results of the Kindred Spirit investigation had nothing to do with Clinton per se. However, the Clinton administration's handling of the situation resulted in continued criticism.

The Wen Ho Lee incident. Taiwanese-born computer scientist Wen Ho Lee had been an employee at Los Alamos National Laboratory for 21 years when Energy Secretary Bill Richardson fired him in March 1999. Lee was subsequently arrested by the FBI, charged with not properly securing classified materials and failing to report meetings with individuals from "sensitive" countries, and held for a year. During this time, many observers maintained that Lee was a scapegoat, and some Asian Americans charged that his arrest was motivated by racism. At his trial in September 2000, Lee was convicted on only one of the charges against him—illegally gathering and retaining national security data. Though this was a felony count, the court released him on time served, and ordered him to undergo 60 hours of government debriefing.

Many commentators charged that, if there was an information leak from the Los Alamos lab, and if Lee had anything to do with it, he was only a small part of a much larger problem. Security at the laboratory was considered by many security experts to be inadequate, given the sensitive nature of the work that took place there. For example, in April 2000, two computer drives disappeared from a high-security area and reappeared two months later behind an office copier in another part of the facility. Security breaches such as these prompted Congress to create the National Nuclear Security Administration (NNSA) as a means of better protecting sensitive properties—and partially removing oversight of those materials from Richardson's DOE.

The title of an article in the *Wall Street Journal* called the Wen Ho Lee case a "diversion," and certainly the case did create more questions than answers concerning Chinese espionage. One of the reasons U.S. authorities have had a difficult time pinning charges of spying on the Chinese is that much of their information seems to have come from open sources. This became apparent with the "discovery" of a 1991 volume, published in Chinese in Beijing, titled *Sources and Techniques of Obtaining National Defense Science and Technology.*

Authors Huo Zhongwen and Wang Zongxiao, both PRC intelligence officers, were frank in stating that Western technical journals "are the first choice of rank and file S&T [science and technology] personnel as well as intelligence researchers." Serendipity, combined with failed security measures, also played a part; in the 1970s, the U.S. government had accidentally declassified more than 19,000 documents on thermonuclear weapons. "This incident," wrote Huo and Wang, illustrates that "…there is a random element involved in the discovery of secret intelligence sources, and to turn this randomness into inevitability, it is necessary that there be those who monitor some sectors and areas with regularity and vigilance." This statement is all the more ironic in light of the fact that a copy of *Sources and Techniques,* which first came to U.S. attention in 1999, had been sitting in the Library of Congress for seven years.

Though the intricacies of the putative Chinese spy scandal in the late 1990s will perhaps never be known, it appears that much of the information the PRC acquired was not a result of subterfuge, but rather of Western openness—and, in some cases, the incompetence of individuals charged with guarding secrets. In any case, the point became all but moot after September 11, 2001. Not only did the United States have far worse concerns than China, but President George W. Bush needed Chinese support for America's war on terror. The issue of Chinese espionage, therefore, was not so much resolved as it was set aside.

■ FURTHER READING:

BOOKS:

Cox, Christopher. *U.S. National Security and Military/Commercial Concerns with the People's Republic of China.* Washington, D.C.: U.S. Government Printing Office, 1999.

Stober, Dan, and Ian Hoffman. *A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage.* New York: Simon and Schuster, 2001.

Trulock, Notra. *Code Name Kindred Spirit: Inside the Chinese Nuclear Espionage Scandal.* San Francisco, CA: Encounter Books, 2002.

PERIODICALS:

Broad, William J. "Author to Sue U.S. over Book on China's Nuclear Advances." *New York Times.* (June 18, 2001): A6.

Gordon, Michael R. "A Dangerous Game." *New York Times.* (April 3, 2001): A1.

Gosselin, Peter G. "No Sign Drives Left Lab, Richardson Says." *Los Angeles Times.* (June 19, 2000): A3.

Markoff, John. "Silicon Valley Concern Says It Thwarted Software Theft." *New York Times.* (September 20, 2002): 1.

Purdy, Matthew, and James Sterngold. "The Prosecution Unravels: The Case of Wen Ho Lee." *New York Times.* (February 5, 2001): A1.

Richelson, Jeffrey T. "Uncertain Damage." *Bulletin of the Atomic Scientists* 55, no. 5 (September/October 1999): 17–19.

Rosenthal, Elisabeth. "China Changes Its Approach in the Latest Espionage Incident." *New York Times.* (January 27, 2002): section 1, p. 6.

Schwartz, Stephen I. "A Very Convenient Scandal." *Bulletin of the Atomic Scientists* 55, no. 3 (May/June 1999): 34–39.

"The Wen Ho Lee Diversion." *Wall Street Journal.* (September 19, 2000): A26.

ELECTRONIC:

China's High-Tech Espionage. Counterintelligence News and Developments/National Counterintelligence Executive. June 2000. <http://www.ncix.gov/nacic/news/2000/jun00.html> (March 29, 2003).

SEE ALSO

China, Intelligence and Security
Clinton Administration (1993–2001), United States National Security Policy
DOE (United States Department of Energy)
Los Alamos National Laboratory
NNSA (United States National Nuclear Security Administration)
Satellite Technology Exports to the People's Republic of China (PRC)

Church Committee

Following the Watergate Scandal, the Senate conducted a thorough review of the function, operation, and administration of the United States intelligence community. A special committee, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities was established to conduct the sweeping audit of national intelligence services. Known as the "Church Committee" after its chairman Frank Church, the committee investigated not only the actions and operations of the intelligence and security services, but also abuses of those services by the Office of the president.

Former CIA Director William Colby is sworn in to testify before the 1975 Senator Church Committee looking into activities by the intelligence community. ©WALLY MCNAMEE/CORBIS.

The Church Committee investigated suspected abuses of power by the intelligence community by interviewing hundreds of witnesses and subpoenaing thousands of relevant documents and materials. The main targets of its investigations were the CIA, FBI, National Security Agency (NSA), and Internal Revenue Service (IRS). The committee also closely noted the involvement of the executive branch and President in intelligence affairs.

In 1975 and 1976, the Church Committee issued fourteen reports. Report topics ranged from intelligence and executive branch involvement in the assassination of foreign leaders, an act prohibited by international law, to domestic espionage and political blackmail. Though the committee was initially charged with discovering the abuses of power and intelligence resources that contributed to the Watergate scandal, its investigations encompassed intelligence community operations during the entire post-World War II and Vietnam War era.

The Church Committee issued its final report in April 1976. The Committee concluded that the CIA, FBI, and other intelligence forces, had conducted concerted campaigns of domestic espionage that threatened the Constitutional rights of ordinary citizens. The Church Committee

further decided that such actions could be prevented by the establishment of a permanent means of congressional review for the intelligence community. The Senate created the Senate Select Committee on Intelligence, a modified version of the Church Committee, as an oversight and investagatory committee for the nation's intelligence services. In the 1970s and 1980s, the committee formalized the review and oversight process, and clearly defined instances of abuse of power and illegal activities that warrant committee investigation. The Senate Select Committee on Intelligence continues to operate today.

FURTHER READING:

BOOKS:

Kurland, Philip B. *Watergate and the Constitution (The William R. Kenan, Jr., Inaugural Lectures).* Chicago:University of Chicago Press, 1978.

Kutler, Stanley I. *The Wars of Watergate: The Last Crisis of Richard Nixon.* New York: W.W. Norton and Company, 1992.

ELECTRONIC:

United States National Archives and Records Administration. Watergate resources. <http://www.archives.gov/digital_classroom/lessons/watergate_and_constitution/teaching_activities.html> (01 December 2002).

SEE ALSO

CIA (United States Central Intelligence Agency)

CIA (United States Central Intelligence Agency)

JUDSON KNIGHT

The Central Intelligence Agency (CIA) is an independent government organization, founded under the National Security Act of 1947. The agency is a leader among the 14 agencies and organizations in the United States Intelligence Community. The mission of CIA is to support the president, the National Security Council (NSC), and other officials involved in national security policy by providing accurate, comprehensive, and timely foreign intelligence on national security topics. CIA also supports the chief executive and the national security policy leadership by conducting counterintelligence operations, special activities, and other duties relating to foreign intelligence and national security as directed by the president. The CIA in the 1990s increased its openness with the American public, and provides relatively detailed information about its organizational structure, through which the director of Central Intelligence (DCI) oversees the four directorates (Administration, Intelligence, Science and Technology, and Operations), as well as numerous other offices.

Background

CIA's headquarters is in Langley, a neighborhood in McLean, Virginia; hence the term "Langley" is used as a metonym for the entire organization, or its leadership. (The terms "CIA" and "the CIA" are used interchangeably, while "the Company" is a term by which some employees refer to the agency.) Information on its budget is classified, but the entire U.S. intelligence budget, of which CIA comprises but a portion, was $26.6 billion in 1997, the first year in which such figures were reported. (The 1998 budget figures, the only other ones released as of early 2003, showed an increase of $100 million, to $26.7 billion.)

Also classified is the number of persons employed by CIA, but the agency is more open concerning the variety of personnel it hires. There is no one single type of CIA employee, and the popular image of CIA operatives as cutthroats and assassins is a bankrupt cliché. As of 2003, the agency had a particular interest in hiring scientists, engineers, economists, linguists, mathematicians, secretaries, accountants, and computer specialists, although the scope of employment opportunities exceeded even this wide range.

In order to be considered for employment with CIA, an applicant must have a college degree, with a minimum grade point average of 3.0. The applicant must submit to a polygraph and medical examination, as well as background checks. Once hired, the new employee must be willing to relocate to Washington, D.C., or to CIA stations in various locales throughout the world. Many CIA officers work under some form of cover, either as employees of other government organizations (for example, some CIA operatives serve under diplomatic cover in the State Department), or under nonofficial cover, whereby an intelligence officer lives as a private citizen who ostensibly has no ties to the U.S. government.

In accordance with the CIA's mission, the majority of activity by its operatives is directed toward the gathering, production, and analysis of political, economic, and military intelligence on foreign governments, terrorist groups, and criminal organizations. This information originates from documents obtained either openly or illegally, from human sources (human intelligence or HUMINT), from electronic eavesdropping (signals intelligence, or SIGINT), or from images collected by spy cameras or satellites in space (imagery intelligence, or IMINT). Once gathered, intelligence must be processed and analyzed, after which the CIA passes information on to its clients, which include

President Bush, right, and George Tenet, left, head of the Central Intelligence Agency, pause at the entrance to agency headquarters on the way to a speech in March, 2001, in which the president thanked CIA employees for their service and spoke of the importance of intelligence collection and analysis in a world that includes many new threats to U.S. security. AP/WIDE WORLD PHOTOS.

the president and major cabinet-level departments, including State, Defense, and the Treasury.

CIA officers may also be involved in counterintelligence, which is designed to preserve U.S. national security by protecting American assets from foreign spying. Additionally, operatives of the CIA may at times engage in actions such as the spreading of propaganda or disinformation; the use of blackmail or other means to put pressure on enemy operatives; and give support to overseas political or military groups whose objectives align with U.S. interests.

CIA excesses in the past have prompted a number of countermeasures against it on the part of the federal government. In 1975, President Gerald R. Ford issued an executive order forbidding acts of assassination by the CIA, and Executive Order 12333, signed by President Ronald Reagan in 1981, extended this prohibition to forbidding indirect involvement in assassination. This order also expressly prohibited CIA collection of foreign intelligence on the domestic activities of American citizens. Today, the Executive Office of the president monitors and investigates CIA activities through the president's Foreign Intelligence Advisory Board.

In the mid-1970s, the Church Committee hearings in the Senate and the Pike Committee hearings in the House led to the formation of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Congressional oversight of CIA through these and other committees is an ongoing activity.

Some critics argue that the agency can find ways around the executive and legislative authorities charged with oversight of CIA activities. However, those authorities are privy to information on the CIA far beyond the reach of ordinary citizens lacking an appropriate security clearance and need-to-know, and it is likely that in many cases presidents or legislators have put a stop to activities about which the general public never learned. In light of the increased atmosphere of scrutiny that has attended

CIA activities since the Iran-Contra scandal of the 1980s, the idea that the CIA maintains a government within the government, whereby it exerts its will independent of executive or legislative oversight, is tantamount to conspiracy theory.

The Structure of CIA

Although both Congress and the president exert oversight of CIA activities, it is the president who holds ultimately authority. Only the president, acting usually through the NSC, can direct the CIA to participate in covert actions. By the same token, DCI reports either directly to the president, or indirectly through the NSC.

Under DCI is the deputy director of Central Intelligence (DDCI), who assists DCI as head of the CIA and of the Intelligence Community. DDCI also exercises the powers of the DCI when the holder of that position is absent or disabled. Within the CIA and the Intelligence Community as a whole, the offices of the DCI and the DDCI are intended to function virtually as a single unit.

Three lines of authority. Under the leadership of the DCI/DDCI office are a number of functions within the intelligence community but outside the CIA. These include the DDCI for Community Management and the Assistant DCI for Administration, both of which are statutory positions for which presidential appointment and Senate confirmation is required; the Associate DCI for Military Support; the DCI for Foreign Intelligence Relations; and the National Intelligence Council.

Reporting to the DCI and DDCI are a number of independent offices within the CIA, including the Inspector General, General Counsel (these two are also statutory positions nominated by the president and confirmed by the Senate), Public Affairs, Congressional Affairs, Protocol, and Diversity Plans and Programs. By far the largest chain of command within the CIA, however is the one that runs through the offices of the Executive Director (EXDIR) and Deputy Executive Director (D/EXDIR).

The EXDIR oversees five centers that collectively enable the CIA to carry out its mission: the Chief Financial Officer, Chief Information Officer, Global Support, Human Resources, and Security, each of which have numerous subordinate offices and bureaus. Also under the EXDIR aegis are several independent functions, including the Center for the Study of Intelligence, Office of Equal Employment Opportunity, Ombudsman/Alternative Dispute Resolution, and the Executive Secretary. Finally, the Executive Director's office is in the line of authority between DCI/DDCI and the four directorates.

The directorates. The work of the directorates of Operations and Intelligence are at the heart of what most people think of when they hear the initials "CIA". Operations is responsible for collecting foreign intelligence, including HUMINT, and for overseeing the overt collection of intelligence domestically through persons or organizations that volunteer that information. Within Operations are the Counterintelligence and Counterterrorism centers, the National HUMINT Requirements Tasking Center, and various regional and transnational issues divisions.

The Directorate of Intelligence is responsible for producing the bulk of CIA's finished intelligence, processed from raw data collected in the field. Within this directorate are the offices of Asian, Pacific, and Latin American Analysis; Near Eastern, South Asian, and African Analysis; Russian and European Analysis; Transnational Issues; and Policy Support. Other groups within this directorate include the Collection Requirements and Evaluation Staff, the DCI Crime and Narcotics Center, and the DCI Weapons Intelligence, Nonproliferation, and Arms Control Center.

The Directorate of Administration provides support to CIA activities through a number of administrative and technical offices such as Communications, Facilities and Security Services, Information Technology, and Medical Services. The Directorate of Science and Technology also provides support through research, development, acquisition, and operations of technical capabilities and systems. It directs the Foreign Broadcast Information Service and the National Photographic Interpretation Center.

A Brief History of the CIA

The CIA began operation on September 18, 1947, with Rear Admiral Roscoe H. Hillenkoetter as its first DCI. In its first covert operation, begun late that year, it influenced the general elections in Italy so as to prevent a Communist victory. Despite this success, President Harry S. Truman blamed Hillenkoetter for failing to predict the coming of the Korean War, and replaced him with General Walter Bedell Smith in October 1950. Under Smith's leadership, the CIA helped bring about the overthrow of Iran's Premier Mohammed Mossadegh after the latter nationalized oil fields in his country.

The accession of Allen W. Dulles to the position of DCI in 1953 marked the beginning of a new era. Under his direction, the CIA became highly energetic and enterprising, building both the Berlin Tunnel and the U-2 spy plane, and undertaking covert operations in Guatemala, Egypt, Indonesia, Chile, and the Congo. Despite a number of successes, the CIA under Dulles also experienced several disasters, most notably the shootdown of U-2 pilot Francis Gary Powers over the Soviet Union in 1960, and the abortive invasion of Cuba at the Bay of Pigs in 1961.

The 1960s and 1970s. Under John A. McCone, who replaced Dulles, the CIA regained favor with Kennedy when

it furnished spy plane photos showing Soviet missile emplacements in Cuba, evidence Kennedy used during the Cuban Missile Crisis. Following Kennedy's assassination, President Lyndon B. Johnson appointed fellow Texan William F. Raborn, Jr., who had little background in intelligence. In June 1966, Raborn's DDCI, Richard McGarrah Helms, took the leadership position.

Helms vigorously prosecuted the CIA's secret wars in Vietnam, Cambodia, and Laos, yet struggled with Johnson and President Richard M. Nixon over their demands to conduct domestic intelligence campaigns. Nixon fired him in February, 1973, and after a six-month period in which James R. Schlesinger led the agency, William E. Colby became DCI. Colby's was a difficult tenure, as the CIA came under intense scrutiny from journalists and committees in Congress.

Colby retired in January 1976, and was replaced by future President George H. W. Bush, who put his support behind improvements in satellite technology. When James E. Carter became president, he replaced Bush with Admiral Stansfield Turner, who continued Bush's emphasis on intelligence collection via satellite. Turner sought to distance the agency from its old practices, and covert operations declined dramatically under his leadership.

From the 1980s to the present. The inauguration of a new president, Ronald Reagan, in January 1981 brought with it a new DCI, William J. Casey. Under Casey, a veteran of U.S. intelligence in World War II, the CIA's budget, size, and influence grew enormously. Casey directed funds and arms to rebels fighting Communist regimes in both Afghanistan and Nicaragua, and became heavily involved in the Iran-Contra affair. How great that involvement was may never be known, in part because Casey died on January 29, 1987, during the congressional investigation.

William H. Webster, who served as FBI director from 1978 to 1987, succeeded Casey as DCI and served for four years. Under Robert M. Gates, a former DDCI of long standing, the CIA redirected its efforts from a Cold War orientation and toward a focus on issues such as nonproliferation, terrorism, and drug trafficking. During the tenure of R. James Woolsey, appointed in 1993, the CIA came under criticism with the exposure of Aldrich Ames, a mole for the Soviet Union and later Russia, who had operated within of the agency for many years.

Woolsey resigned in January 1995, and John M. Deutch replaced him. Deutch, who held the position for less than two years, was the first DCI to serve on the president's cabinet. In July 1997, George J. Tenet became the fifth DCI in just six years. Though Tenet's leadership style has won praise from observers of the Intelligence Community, the CIA as a whole came under criticism for perceived intelligence failures prior to the September 11, 2001, terrorist attacks. In the wake of those events, the agency has placed a renewed emphasis on human intelligence, or the gathering of intelligence from human sources.

FURTHER READING:

BOOKS:

Andrew, Christopher M. *For the president's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush.* New York: HarperCollins, 1995.

Jeffreys-Jones, Rhodri. *The CIA and American Democracy.* New Haven: Yale University Press, 1989.

Kessler, Ronald. *Inside the CIA: Revealing the Secrets of the World's Most Powerful Spy Agency.* New York: Pocket Books, 1992.

Prados, John. *President's Secret Wars: CIA and Pentagon Covert Operations Since World War II.* New York: W. Morrow, 1986.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

———. *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology.* Boulder, CO: Westview Press, 2001.

ELECTRONIC:

Central Intelligence Agency. <http://www.cia.gov/> (April 24, 2003).

Central Intelligence Agency. Federation of American Scientists. <http://www.fas.org/irp/cia/index.html> (April 24, 2003).

SEE ALSO

CIA, (CSI) Center for the Study of Intelligence
CIA Directorate of Science and Technology (DS&T)
CIA, Foreign Broadcast Information Service
CIA, Formation and History
CIA, Legal Restriction
DCI (Director of the Central Intelligence Agency)
HUMINT (Human Intelligence)
IMINT (Imagery Intelligence)
Intelligence Community
Intelligence, United States Congressional Oversight
Iran-Contra Affair
NIC (National Intelligence Council)
President of the United States (Executive Command and Control of Intelligence Agencies)
SIGINT (Signals Intelligence)
United States, Intelligence and Security

CIA (CSI), Center for the Study of Intelligence

The Center for the Study of Intelligence (CSI) of the United States Central Intelligence Agency (CIA) is a reference and resource center for scholars and others studying the history and practice of intelligence disciplines. According to CSI's mission statement, the center "seeks to promote study, debate, and understanding of the role of intelligence in American society." This it accomplishes by a number of means, including publications, conferences and seminars, the maintenance of historical records, and

other programs. As of 2003, CSI posted articles from the unclassified, or non-restricted access version, at its Web site.

In accordance with its mission of preserving intelligence history, CSI publishes collections of documents from the Cold War, and conducts oral history projects. It also makes historical records available to scholars and other members of the public. CSI's conference and seminar programs provide a forum for research and discussion, and serve to commemorate major events in the realm of intelligence. An outreach program to institutions of higher learning promotes the teaching of intelligence and related studies. Additionally, CSI sponsors CIA officers-in-residence on selected college and university campuses.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. "Center for Studies of Intelligence." <http://www.cia.gov/csi/> (January 17, 2003).

SEE ALSO

CIA (United States Central Intelligence Agency)
United States Intelligence, History

CIA Directorate of Science and Technology (DS&T)

JUDSON KNIGHT

The Directorate of Science and Technology (DS&T) is one of four directorates within the Central Intelligence Agency (CIA). It provides support to the CIA mission through research, development, acquisition, and operation of technical capabilities and systems. DS&T also directs the Foreign Broadcast Information Service and the National Photographic Interpretation Center (NPIC). Its most notable work, however, is its task as a "spy shop," in which some of the most innovative surveillance technology in history—the U-2 and A-12 spy planes, or the KH-11 and other satellites of the CORONA program—were first envisioned.

Early History

From the earliest days of CIA, itself created in 1947, scientific and technological support has been an important component of the agency's mission. The earliest ancestor of DS&T was the Office of Reports and Estimates, which in December 1948 merged with the Nuclear Energy Group of the Office of Special Operations to form the Office of Scientific Intelligence (OSI). The latter would remain the CIA's principal scientific research laboratory until 1962.

In researching his book on DS&T, *The Wizards of Langley* (2001), intelligence scholar Jeffrey T. Richelson accessed a host of documents that were once highly sensitive, but are now declassified. He posted a number of these at a permanent Web site associated with the George Washington University National Security Archive. One notable early example from the collection is a November 5, 1954, letter from Polaroid chief executive officer Edwin Land to Director of Central Intelligence (DCI) Allen Dulles, urging him to develop a specialized aircraft that could fly at high altitudes and obtain ultra-high resolution photographs. From this letter and other early discussions would come the U-2, developed at Lockheed's Skunk Works facility in California.

Other documents from the 1950s show early CIA plans for the deployment of the first spy satellites. At that time, the Air Force had its own satellite project in the works, but the CIA's CORONA, launched in 1959, would prove much more successful, and would outlast the Air Force SAMOS program by a decade. Much less successful were CIA experiments with psychotropic drugs, including LSD, during the period 1949–1963. Richelson excerpted a January 1975 memo, written just before the CIA became the target for a series of congressional investigations, detailing those experiments, including the infamous MKULTRA program.

The 1960s. In 1962, OSI became the Deputy Directorate for Research, whose name was again changed to Deputy Directorate for Science and Technology in 1963. The directorate assumed its present name in 1965. During this period, the agency developed the A-12 Oxcart, which, though successful, never equaled the U-2 for accuracy. Its satellite programs continued to progress, yet as an NPIC photographic interpretation report from August 1962 showed, even the KH-4 satellite did not offer imagery any better than that obtained by the U-2.

A March 1967 memo, from which several details (including the recipient) were excised, provides an illustration of the folly that sometimes befell DS&T. The memorandum describes a project known as "Acoustic Kitty," whereby DS&T attempted to develop a mobile eavesdropping platform using a cat that had been surgically altered by cutting it open, inserting batteries, and wiring its tail to become an antenna. The unfortunate creature was run over by a taxi before it could be trained for its mission.

The 1970s. More indicative of DS&T's involvement in cutting-edge technology was a report from a June 1971 meeting of the president's Foreign Intelligence Advisory Board in which President Richard M. Nixon, along Land (still highly involved with the Intelligence Community) and others, discussed the idea of developing a satellite that could return images in real time. Today, of course, such a concept is well known, but in an era when satellites still recorded images on film for viewing days or weeks later, the idea of a satellite that could instantaneously

relay images to a ground station seemed farfetched. In December 1976, the vision discussed at this meeting was realized with the deployment of the KH-11 satellite.

Once again, documents selected by Richelson illustrate juxtaposition of scientific triumph with less successful undertakings. Even as KH-11 was being born, DS&T undertook experiments in "remote viewing," or the use of purported psychic knowledge to explore targets of interest that could not be glimpsed by ordinary means. According to a December 1975 report from Los Alamos Scientific Laboratory, remote viewers "saw" a number of objects that, as shown by satellite photography, were not at the site in question. After the end of the Cold War, American scientists visiting the site discovered that it was being used to develop a nuclear-powered space rocket and not—as remote viewers had supposed—for underground nuclear tests.

DS&T Today

Information about more recent DS&T activities is necessarily scanty, but these details from the first 30 years of CIA science and technology illustrate the breadth of activities with which it was associated in the past. As of 2003, the DS&T is tasked with collecting, assessing, and exploiting information to assist the agency in the execution of its mission by applying innovative scientific, technical, and engineering solutions to critical intelligence matters.

The workforce of DS&T incorporates some 50 different disciplines, ranging from computer scientists to engineers to linguists. These specialists develop, design, evaluate, and deploy highly specialized equipment intended to provide the United States with a significant advantage in intelligence and special operations.

DS&T is involved in a whole range of functions that support the entire intelligence cycle. These activities include collecting information and materials of intelligence value from foreign open sources, developing and deploying collection systems against the most challenging intelligence targets, supporting the National Reconnaissance Office in creating efficient satellite systems, providing state-of-the-art technologies for the clandestine collection of intelligence, and researching and developing advanced technologies to provide and maintain an advantage for the United States. In pursuit of these activities, DS&T in 2001 developed In-Q-Tel, a nonprofit corporation intended to seek information technology solutions to critical needs faced by CIA as a whole.

■ FURTHER READING:

BOOKS:

Jeffreys-Jones, Rhodri, and Christopher M. Andrew. *Eternal Vigilance? 50 Years of the CIA.* Portland, OR: Frank Cass, 1997.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

———. *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology.* Boulder, CO: Westview Press, 2001.

PERIODICALS:

Goodman, Melvin A. "Science at the CIA." *Issues in Science and Technology* 18, no. 3 (spring 2002): 90–93.

Mooney, Chris. "Spy Tech." *The American Prospect* 13, no. 2 (January 28, 2002): 39–41.

Prados, John. "Understanding Central Intelligence." *Bulletin of the Atomic Scientists* 58, no. 2 (March/April 2002): 64–65.

ELECTRONIC:

Directorate of Science and Technology. Central Intelligence Agency. <http://www.cia.gov/cia/dst/home.html> (April 24, 2003).

Richelson, Jeffrey T. Science, Technology and the CIA. National Security Archive, George Washington University. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB54/index2.html> (April 24, 2003).

SEE ALSO

Antiballistic Missile Treaty
Aviation Intelligence, History
Biochemical Assassination Weapons
CIA (United States Central Intelligence Agency)
CIA, Foreign Broadcast Information Service
Dual Use Technology
Movies, Espionage and Intelligence Portrayals
Photographic Interpretation Center (NPIC), United States National
Pseudo Science Intelligence Studies
Psychotropic Drugs
Satellites, Spy
U-2 Spy Plane

CIA, Foreign Broadcast Information Service

■ MARTIN J. MANNING

The Foreign Broadcast Information Service (FBIS) is the pre-eminent collector of open source information for the United States government; it collects, translates, and disseminates foreign open source material for U.S. Government use. It started as the Foreign Broadcast Monitoring Service (FBMS), established in the Federal Communications Commission (FCC) by a presidential [Franklin D. Roosevelt] directive on February 26, 1941, to monitor, record, transcribe, and analyze foreign broadcasts. The FBMS was organized after assistant secretary of state Breckinridge Long became concerned about the possible loss of diplomatic reporting and other information if the war in Europe caused American embassies to close. Long suggested radio as a supplemental source of intelligence

and looked to the FCC, which regulated domestic radio, as the best source to further monitor foreign broadcasts.

The FBMS was changed to the Foreign Broadcast Intelligence Service by FCC order on July 28, 1942. Its principal activities included translations of monitored foreign broadcasts; transmission of telegrams and cablegrams to government agencies concerned with war propaganda; and the preparation of daily reports by the Far Eastern, Latin American, and European Sections, with weekly reviews of official foreign broadcasts and radio reports on the Far East. The FBMS's first director, 1941–1943, Harold N. Graves, Jr., directed the FBMS's predecessor, Princeton Listening Center, which was launched in November 1939 at Princeton University with funding from the Rockefeller Foundation. It was the U.S. pioneer in the systematic monitoring, translation, and analysis of broadcasts from Berlin, London, Paris, Rome, and Moscow. One journalist described the FBMS as the "greatest collection of individualists, international rolling stones, and slightly batty geniuses ever gathered together in one organization."

The FBIS's first analytic report, released on December 6, 1941, warned of Tokyo's increasingly belligerent tone. The next day, the Japanese attacked the U.S. Navy fleet at Pearl Harbor in Hawaii, initiating the U.S. entry into World War II. The FBIS became responsible for providing open-source intelligence (OSINT) as its part of the military and civilian wartime intelligence effort. On January 14, 1943, FBIS issued its first special report on Nazi propaganda, prepared by the Analysis Directorate's German Section. FBIS maintained a special telephone connection to the White House, and on September 10, 1943, when Hitler went on the air in reaction to Italy's surrender, eager listeners on the line included British Prime Minister Winston Churchill, U.S. Army Chief of Staff General George C. Marshall, and Roosevelt's advisor Harry Hopkins.

After World War II, the FBIS was transferred to the Military Intelligence Division, War Department General Staff, by order of the secretary of war in January 1946, pursuant to an agreement between the FCC and the War Department. The first issue of the *Daily Report* was published the same month. After a period, as part of the Central Intelligence Group (CIG), National Intelligence Authority, the FBIS became part of the newly created Central Intelligence Agency (1947) and negotiated with the British Broadcasting Corporation (BBC) to divide monitoring responsibilities of most of the world's pertinent news broadcasts of interest to intelligence analysts.

As of 2003, the FBIS continues to monitor, translate, and republish selected foreign radio and television broadcasts, newspaper articles, government news agency releases, and political speeches. The selection of items to be included has been determined by the needs of its primary users, officials of the U.S. government. Political, military, economic, and environmental topics are the major emphases. The translations have been published as quickly as possible, usually within a few days of original publication, in a series of daily reports. Since 1996, the service has been available online through a Worldwide Web site known as the World News Connection and through its website: <http://www.fbis.gov.

Foreign newscasts, as well as documentaries and investigative news programs, are the mainstay of the FBIS global television collection. The material FBIS disseminates is known as "FBIS Reporting" and is assumed to be copyrighted by the foreign originator. Contractual and copyright obligations requires that the information be restricted to official U.S. government use.

From its first, unprepossessing headquarters at 316 F Street, NE, in downtown Washington, the FBIS now resides in more lavish buildings in Reston, Virginia, where it operates 24 hours a day, seven days a week, in the CIA's Directorate of Science and Technology.

■ FURTHER READING:

BOOKS:

Graves, Harold N. *On the Short Wave.* New York: Foreign Policy Association, 1941.

PERIODICALS:

Mercado, Stephen C. "FBIS against the Axis, 1941–1945: Open-Source Intelligence from the Airwaves." *Studies in Intelligence* no. 11 (Fall-Winter 2001): 33–43.

ELECTRONIC:

National Technical Information Service, Department of Commerce. "World News Connection" 2002. <http://wnc.fedworld.gov/> (March 20, 2003).

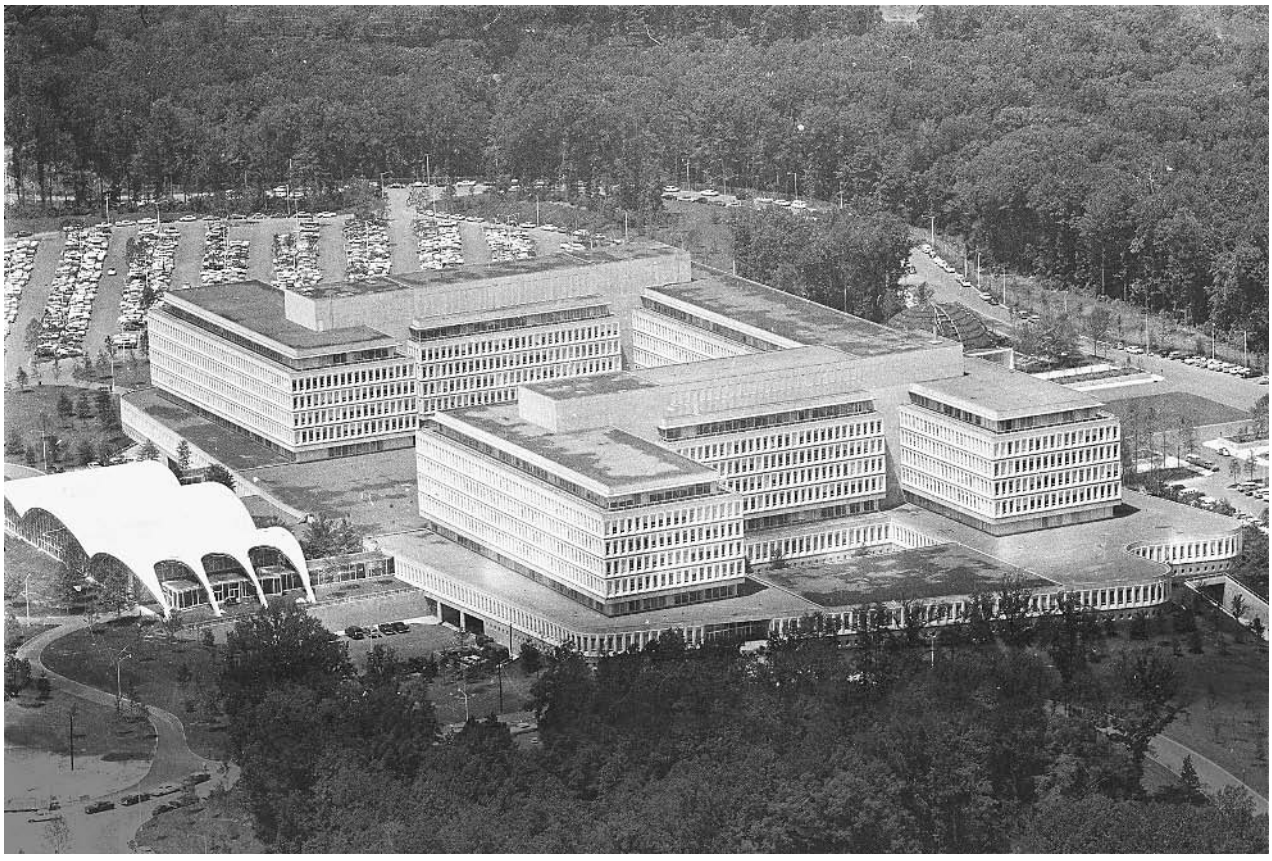
SEE ALSO

COMINT (Communications Intelligence)
Communications System, United States National

CIA, Formation and History

■ MICHAEL J. O'NEAL

United States military planners had always relied on intelligence during wartime, but it was not until World War II that the U.S. government began collecting intelligence systematically. Even before the Japanese attack on Pearl Harbor on December 7, 1941, President Franklin D. Roosevelt had been having doubts about the effectiveness of the nation's intelligence-gathering efforts because they were scattered among the various branches of the military. To correct this deficiency, he appointed William J. Donovan, a New York lawyer who had won the Congressional Medal of Honor as an Army colonel in World War I, to put together a plan for an intelligence service. Out of Donovan's plan emerged the Office of Strategic Services (OSS)



An aerial view of the Central Intelligence Agency (CIA) headquarters in Langley, Virginia, about eight miles from downtown Washington, D.C. AP/WIDE WORLD PHOTOS.

in June 1942. The OSS, under Donovan's leadership, was given the task of collecting and analyzing information needed by the Joint Chiefs of Staff, the heads of all the branches of the nation's military, and to conduct special or clandestine operations that were not carried out by other federal agencies or branches of the military. Throughout the war, the OSS provided policy makers and the military with essential intelligence, including enemy troop strength estimates, that was crucial to planning military campaigns.

In the months and years following World War II, policy makers struggled with two questions: Who should conduct the nation's intelligence-gathering activities? And who should supervise their efforts? These were important questions, for the Cold War rivalry between the United States and its chief adversary, the Union of Soviet Socialist Republics, or Soviet Union, made accurate and timely intelligence about Soviet intentions imperative. Initially, President Harry S. Truman favored dividing responsibilities between military and civilian agencies. In October 1945, he abolished the OSS and transferred its operations to the Departments of War and State. At about the same time, Donovan proposed the formation of a strictly civilian organization that would coordinate intelligence gathering. Such an organization would be authorized to conduct subversive operations abroad, but it would have no police or law-enforcement authority at home. Donovan's plan met with resistance from both the military and the Federal Bureau of Investigation, which feared that the plan would lessen their influence. In January, 1946, Truman struck a middle course. He established the Central Intelligence Group (CIG), giving it the authority to coordinate intelligence gathered by existing departments and agencies. The CIG was placed under the supervision of a National Intelligence Authority, which in turn was made up of the president and the secretaries of the State, War, and Navy departments. For the first time in its history, the United States had a peacetime intelligence organization.

The original CIG and the National Intelligence Authority lasted less than two years. In 1947, Congress entered the picture by passing the National Security Act. This act created the National Security Council (NSC) and placed under its authority the Central Intelligence Agency (CIA). Intelligence gathering was now firmly under the control of civilian authorities, principally the president and his NSC staff.

The growth of the CIA. Throughout the early years, the structure of the CIA changed and its functions were assigned and reassigned to various departments. By the

early 1960s, its broad structure had become largely what it is in 2003. Under the supervision of the Director of Central Intelligence (DCI), one of any president's chief political appointees, are four major departments, or directorates. The Directorate of Administration supervises the business aspects of the agency, including personnel, logistics, training, and the like. The Directorate of Intelligence is the CIA's analysis arm; it interprets raw information and turns it into useful intelligence for the president and the NSC. The Directorate of Science and Technology employs top scientists to develop ever more sophisticated scientific tools to aid in the intelligence-gathering process. Finally, the Directorate of Operations is the traditionally glamorized component of the CIA, for its agents conduct actual intelligence operations in the field.

In its early years, the staff of the CIA consisted primarily of former OSS personnel. Until recent years, the CIA was overwhelmingly a male domain, including mostly academics, lawyers, and journalists. At the time, the CIA had a distinctly academic tone, for the agency recruited top students from the nation's most prestigious universities and placed considerable emphasis on the sober analysis of information. In 1950, the CIA employed about 5,000 people who were housed in various locations in and around Washington, D.C. In 1961, the CIA moved into its current headquarters in Langley, Virginia, and continued to grow. Today the exact number of CIA employees is classified (about 20,000; 6,000 of whom serve in clandestine areas of the organization), but one measure of the agency's size is the nation's budget for intelligence-gathering activities, which in 1998 was $26.7 billion.

In the 1950s and early 1960s, the CIA enjoyed considerable prestige, for it was primarily through intelligence that the United States resisted the expansion of the Soviet Union and the spread of Communism. The CIA, for example, revealed the presence of Soviet nuclear missiles in Cuba during the 1962 Cuban missile crisis. In the 1960s, however, the CIA began to endure some public opinion scrutiny. In 1961, it backed the disastrous Bay of Pigs operation intended to overthrow Cuban dictator Fidel Castro. Later in the decade, as opposition to the war in Vietnam grew, the CIA was seen in many quarters as emblematic of a misguided foreign policy. Further damaging the agency's reputation were revelations that it took part in unsavory operations in Central and South America, often undermining unfriendly regimes and propping up brutal dictators who were friendly to American interests. In 1975, Senator Frank Church led congressional hearings that resulted in restrictions to the entire intelligence community concerning domestic spying and the implementation of stricter oversight of covert operations abroad. Because of these hearings and revelations, the CIA spent much of the 1980s and 1990s refurbishing its image. After the terrorist attacks of September 11, 2001, the CIA took on added luster as the nation looked to the agency as the front line in the fight against terrorism. In the wake of the terrorist attacks, the CIA was again granted increased funding and operational authority to pursue counter-terrorism actions.

Directorate of Science and Technology. In its early years, the CIA relied primarily on field operations, but in the early 1960s Director John A. McCone, whose tenure as DCI ran from 1961 to 1965, concluded that the CIA of the future would have to rely more on science and technology. Until that time, the CIA's science and technology efforts had been scattered among various directorates. With the emergence of "overhead" intelligence-gathering technology, including the U-2 spy plane and reconnaissance satellites, McCone gathered all of the agency's scientific and technological capabilities under one roof. The result was the formation of the Directorate of Science and Technology (DS&T) in 1963. Among the DS&T successes are the design and development of high-tech imagery and eavesdropping satellites, including the KH-11 and RHYOLITE. It monitored Soviet missile capabilities from ground stations in China, Norway, and Iran. Its photographic experts played a key role in monitoring such events as the Chernobyl nuclear power plant disaster in the Soviet Union in 1986 and Iraqi troop movements during the 1991 Gulf War. Many of the DS&T's innovations, including heart pacemaker technology, have had implications for medical research.

■ FURTHER READING:

BOOKS:

Ranelagh, John. *The Agency: The Rise and Decline of the CIA.* New York: Simon and Schuster, 1986.

Richelson, Jeffrey T. *The Wizards of Langley.* Boulder, Colo.: Westview, 2001.

Troy, Thomas F. *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency.* Frederick, MD.: University Publications of America, 1981.

ELECTRONIC:

Central Intelligence Agency. "Key Events in CIA's History." <http://www.cia.gov/cia/publications/facttell/keyevent.htm> (January 2, 2003).

Federation of American Scientists. "Central Intelligence Agency." September 23, 1996. <http://www.fas.org/irp/cia/ciahist.htm> (January 2, 2003).

SEE ALSO

Bush Administration (1989–1993), United States National Security Policy
Bush Administration (2001–), United States National Security Policy
Church Committee
CIA (United States Central Intelligence Agency)
CIA (CSI), Center for the Study of Intelligence
CIA Directorate of Science and Technology (DS&T)
CIA, Foreign Broadcast Information Service
CIA, Legal Restriction
Covert Operations
United States, Counter-Terrorism Policy

James Angleton, former chief of Counterintelligence at the Central Intelligence Agency, answers questions before the Senate Intelligence Committee in 1975 regarding the CIA practice of opening mail of targeted Americans. Proceedings from the committee resulted in tighter controls concerning CIA covert actions. AP/WIDE WORLD PHOTOS.

CIA, Legal Restriction

JUDSON KNIGHT

Although created by legislation in 1947, the Central Intelligence Agency (CIA) operated largely free of legal restrictions for about a quarter-century. This all changed in the early 1970s, when CIA involvement in the Watergate break-in led to investigations in Congress. Simultaneous with this was a series of revelations in the media concerning CIA covert operations in the past, which only further influenced a widespread opinion that the agency had operated for too long without benefit of legal oversight. The result was the formation of House and Senate intelligence committees, as well as other restrictions that have served—with varying degrees of success—to put the agency under legal restraint.

Excesses and reactions. The National Security Act, passed by Congress in 1947, formally established the CIA, even though a presidential directive signed by President Harry S. Truman in January 1946 had established a forerunner, the Central Intelligence Group. The Central Intelligence Agency Act of 1949, rather than limiting the powers of the agency, gave it a virtual blank check: CIA budgets, salaries, and even job titles would be secret; contracts could be awarded without bidding; and the CIA could grant permanent residency to aliens—particularly defectors from the Soviet bloc—and their families.

During the height of the Cold War, the CIA operated with a greater degree of operational freedom. Only in the 1970s, as the Cold War entered a new phase of detente, and as the American public became increasingly suspicious of their government, did the agency come under increased scrutiny and hence, legal restriction. More than even the Vietnam War, the single greatest factor in spawning this distrust was the 1972 Watergate break-in, in which CIA personnel were involved. Watergate, which would lead to the downfall of the Nixon administration, started the CIA on a spiral of diminishing public confidence that would lead to the imposition of greater legal restrictions on the agency.

Just as *Washington Post* journalists Bob Woodward and Carl Bernstein broke the Watergate story, Seymour Hersh of the *New York Times* started a barrage of investigative reports directed at the CIA when in December, 1974

he uncovered evidence of a lengthy domestic intelligence campaign involving interception of private mail. In the years that followed, the public would learn that the agency had been involved in assassinations and attempted assassinations, conducted experiments using LSD and other psychotropic drugs, and lied to the public concerning the development of secret spy planes.

New committees and executive orders. In response to the growing public distrust of the CIA, President Gerald R. Ford on January 4, 1975, signed Executive Order 11828, which created the Commission on CIA Activities, to be chaired by Vice President Nelson Rockefeller. On January 27, the Senate established its Select Committee to Study Governmental Operations with Respect to Intelligence Activities, under the leadership of Frank Church (D-ID). The House of Representatives created its own Select Committee on Intelligence, later chaired by Otis G. Pike (D-NY), on February 19.

The Church Committee submitted its final report on April 26, 1976. Meanwhile, on January 29, just two days before the Pike Committee was to complete its investigation, the House voted not to make its findings public. (The report was eventually leaked to journalist Daniel Schorr, and published in the *Village Voice*.) The Church Committee had already begun to have an impact, and as of May 19, the Senate had put in place its permanent Select Committee on Intelligence. On July 14, 1977, the House established its own such committee.

Ford signed Executive Order 11905, "United States Foreign Intelligence Activities," on February 18, 1976. The order established the Committee on Foreign Intelligence and the Operations Advisory Group, which greatly increased executive oversight of the CIA. The National Security Council (NSC), established at the same time as the CIA, also afforded this oversight, but in the NSC, the Director of Central Intelligence primarily acted in the capacity of an intelligence advisor, whereas the new committees extended the President's involvement in CIA budget planning and resource allocation.

President James E. Carter, on January 24, 1978, signed Executive Order 12036, which changed the shape of the intelligence structure. Among its provisions was a restriction of bugging and domestic surveillance activities, and guidelines whereby the CIA could request surveillance authorization through the Federal Bureau of Investigation. This order was superseded on December 4, 1981, by Executive Order 12333, in which President Ronald Reagan further clarified legal oversight of the intelligence community.

Laws in the early 1980s. The effort to bring the CIA into line continued with a series of congressional acts in the early 1980s, including the 1980 Intelligence Oversight Act. The act replaced the armed services committees as the principal arm of legislative oversight for the CIA in both houses of Congress. Thenceforth, the newly formed intelligence committees would take the lead, though the armed services committees remain involved in monitoring intelligence activities, as did the foreign relations and foreign affairs committees. At its end, the CIA maintains an Office of Congressional Affairs, and provides more than a thousand briefings to Congress, its committees, and their staffs, each year.

In an effort to prevent the pendulum from swinging too far in the opposite direction, Congress passed the Intelligence Identities Protection Act. The act, which Reagan signed into law on June 23, 1982, made it a felony to reveal the names of covert intelligence personnel. On October 15, 1984, Reagan signed the Central Intelligence Agency Information Act, which exempted the agency from the search and review requirements of the Freedom of Information Act. (The latter, passed in 1967 and amended in 1975, had further increased U.S. citizens' protection against domestic intelligence operations by the CIA and other groups.)

Striking a balance. All issues of legal authority over the CIA were not solved in the period from the mid-1970s to the early 1980s, however. Still ahead lay the Iran-Contra debacle, which did not so much lead to new legislation as it further eroded the trust of lawmakers and the public toward the CIA. As a result, by the early 1990s, the U.S. intelligence community found itself so restricted that it could hardly conduct its operations. This fact hit home after the terrorist attacks of September 11, 2001, when it became apparent that a lack of human intelligence had contributed to the government's failure to foresee the attacks. However, the post-September, 2001 emphasis on security portended a relaxation of restrictions on CIA activity.

■ FURTHER READING:

BOOKS:

Legislative Oversight of Intelligence Activities: The U.S. Experience: Report. Washington, D.C.: U.S. Government Printing Office, 1994.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

PERIODICALS:

Cannon, Carl M. "Central Intelligence Agency." *National Journal* 33, no. 25 (June 23, 2001): 1903–1904.

SEE ALSO

CIA (United States Central Intelligence Agency)
CIA, Formation and History
FOIA (Freedom of Information Act)
HUMINT (Human Intelligence)
Intelligence, United States Congressional Oversight of
Intelligence Authorization Acts, United States Congress

NSC (National Security Council)
PFIAB (President's Foreign Intelligence Advisory Board)
President of the United States (Executive Command and Control of Intelligence Agencies)

Cipher Disk

A cipher disk is a handheld coding device for generating a limited number of substitution ciphers, that is, ciphers in which each letter of the regular alphabet is enciphered as a single character from a cipher alphabet. A typical cipher disk consists of an inner ring with the characters of the regular alphabet printed around its outer edge, and an outer ring that fits snugly around the inner ring and can be rotated. Around the outer ring is printed a cipher alphabet that has the same number of characters as the regular alphabet. This cipher alphabet may consist of a scrambled regular alphabet or of other symbols. To encipher a message, the user of the cipher disk first chooses some particular alignment of the outer ring with the inner ring. For example, if the cipher alphabet consists of the numbers 1 through 26 (in order), the user may align the number 10 on the outer ring with the letter A on the inner ring. The letter A will then encipher as 10, the letter C as 12, the letter Z as 9, and so forth. By shifting the outer ring one or more letter-positions, the user obtains a different substitution cipher. Some cipher disks have an internal mechanism that advances the outer ring by one step after the encipherment of each letter; this prevents a given plaintext letter from always enciphering as the same ciphertext letter.

The earliest known description of the cipher disk was penned by Italian artist Leon Battista Alberti (1404–1472) in 1470. Cipher disks produce ciphers that are too simple for practical use in the modern world, but were used in the field by Confederate forces during the United States Civil War (1861–1865). Union cryptographers, however, often had no problem reading the Confederacy's encrypted messages. Cipher disks were also widely distributed in the U.S. in the 1940s as marketing giveaways for radio adventure programs such as *Captain Midnight*. These programs were popular even with adults, including active air crews during World War II, and stories—possibly apocryphal—have circulated claiming that combat forces occasionally put the toy cipher disks to real-life use. More complex ciphering systems based fundamentally on the cipher disk concept, such as Enigma, have seen extensive real-world service.

FURTHER READING:

BOOKS:

Deavours, Cipher, et al. *Cryptology: Machines, History & Methods.* Norwood, MA: Artech House, 1989.

Singh, Simon. *The Code Book.* New York: Doubleday, 1999.

SEE ALSO

Cipher Machines
Codes and Ciphers
Enigma

Cipher Key

A cipher key is a sequence of symbols that a user of a given cipher system must possess in order to use the system. Without a key, a user cannot encipher messages (turn them from plaintext to ciphertext) or decipher messages (turn them from ciphertext to plaintext).

Keys greatly enhance cipher security and are a feature of all modern ciphers. To see the value of keys, consider the following Caesar shift cipher:

Plaintext alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext alphabet:
DEFGHIJKLMNOPQRSTUVWXYZABC

Note that the ciphertext alphabet is merely the plaintext alphabet shifted to the left by three letter-positions (with A, B, and C wrapped around to the right). As it stands, this cipher has no key; it consists of a one-step method that never varies (e.g., in reading the above table, E from the Plaintext alphabit always enciphers to H of the Ciphertext alphabet, the E being directly below the H in the table). Ciphers such as this example are easy to break. Twenty-four similar, but distinct ciphers can be generated, however, simply by shifting the lower alphabet by some number of positions other than three. For example, a left-shift of six letters changes the ciphertext alphabet to GHIJKLMNOPQRSTUVWXYZABCDEF. One can therefore imagine a cipher system in which one specifies a different shift before enciphering each message. The receiver will also need to know the shift, so that they can use the same substitution cipher that the sender used. In this improved cipher, the shift number for each message would function as a *key*. There are 25 possible keys (i.e., shifts) in this system, each of which would cause a different ciphertext to be produced from a given plaintext. This is a general feature of keys: a key modifies the rules for producing or deciphering ciphertext.

In general, an opponent who obtains a key (and who understands the rest of the cipher system) can decipher all the plaintext that has been enciphered using that key. In the example above, there are only 25 possible keys, and the cipher can easily be attacked by exhaustion, that is, by trying all possible keys. In real-world cipher systems, the

number of keys is made too large for exhaustion to be practical. For example, if a 56-bit binary number is used as the key, there are $2^{56} > 7.2 \times 10^{16}$ possible keys. An ideal cipher would be breakable only by exhaustion; in practice, ciphers almost always have subtle weaknesses that make it possible to break them without having to guess all possible keys.

FURTHER READING:

BOOKS:

Mollin, Richard A. *An Introduction to Cryptography.* New York: Chapman & Hall, 2001.

SEE ALSO

Codes and Ciphers

Cipher Machines

LARRY GILMAN

A cipher machine is a mechanical device that assists in the production of ciphertext from plaintext and vice versa. In this broad sense, any mechanical aid from a cipher wheel to a supercomputer can qualify as a cipher machine; however, the term is usually reserved for devices that are fairly complex and that operate on mechanical or electromechanical rather than on electronic principles.

Before World War I, ciphers were implemented using either marks on paper or simple aids such as cipher wheels. After the war, a number of inventors in various countries produced cipher machines that transferred the complexity and tedium of ciphering to a mechanism. These machines allowed the operator, who might be completely ignorant of the cipher's nature, to simply type at a keyboard or enter characters one by one by moving a wheel with their fingers. If plaintext (ordinary written language) was entered into such a machine, ciphertext (apparently random characters) was produced; if ciphertext was entered, plaintext was produced. Cipher machines made it possible to cipher and decipher large numbers of messages with less training for personnel, fewer errors, and higher speed.

Many cipher machines invented in the post–World War I period employed as their key component the scrambler disk or rotor. The typical rotor is a disk a few inches in diameter, with letters and numbers printed around its rim and embedded wires connecting one side to the other. Matching points on opposite surfaces of the disk correspond to the same alphanumeric characters, and each wire running through the disk corresponds to one character to be enciphered or deciphered. By connecting one point on surface A of the rotor—say, the point corresponding to the letter M—to a different point on surface B—say, the point corresponding to the letter Z—the rotor implements a fixed substitution cipher (i.e., replaces every character by some other). In this example, M is enciphered to Z and Z is deciphered to M (or vice versa).

The substitution cipher built into the wires of a single rotor is a trivial one. What the inventors of the rotor-based cipher machines realized was that by lining up multiple cipher disks and continually rotating them as a message was enciphered or deciphered, they could produce much more formidable ciphers. For instance, three rotors could be stacked or aligned so that surface B of rotor 1 met surface A of rotor 2, while surface B of rotor 2 met surface A of rotor 3. Each letter of the input (at surface A of rotor 1) then follows a tortuous path through the wiring of all three disks to the output (at surface B of rotor 3). If the rotors are shifted upon encryption or decryption of each and every message character, the encryption/decryption path is not only tortuous, but also changing. A degree of cipher security that was essentially impossible with pencil-and-paper ciphering was made possible by such machines.

The rotor principle was discovered independently by inventors in several countries, the most famous being German engineer Arthur Scherbius (1878–1929). Scherbius invented a three-rotor cipher machine, the Enigma, in 1918 (the last year of World War I). Scherbius tried unsuccessfully to sell his machine to commercial buyers, but he was ahead of his time; corporations did not begin to use encryption widely until the 1960s. Enigma was, however, purchased by the German government in 1926. At that time, Germany was busy rebuilding its military forces after its defeat in World War I and the humiliating terms of the Treaty of Versailles. Furthermore, the German military leadership had become aware that their pencil-and-paper field cipher, the famous ADFGVX cipher, had been broken by French cryptographers only a few months after its deployment in 1918, leading to at least one significant military defeat for the Germans. In order to prevent a repetition of the ADFGVX debacle, the Germans switched to Enigma as their primary system for secret communications.

The different branches of the German military also employed slightly different models of the Enigma cipher machine. In 1943, the German military deployed the SZ42 cipher machine for use over 26 crucial communications links. The SZ42 employed the stream-cipher technique, in which identical key-streams of pseudorandom characters are generated at both the sending and receiving end of the link and added, character by character, to the individual characters of the plaintext (for ciphering) or ciphertext (for deciphering). The German military did not replace Enigma with the SZ42 for general use because the SZ42's complexity made it too heavy for the field.

The SZ42 cipher proved difficult for allied cryptographers to crack, as did another German cipher machine, the Geheimschreiber, first deployed by the German navy in 1942. However, Allied cryptographers cracked the Enigma, SZ42, and Geheimschreiber ciphers by building specialized devices to systematically try out possible keys

Enigma cipher machines displayed at the National Cryptologic Museum in Fort Meade, Maryland. ©RUBIN STEVEN/CORBIS SYGMA.

for the decryption of messages. The first such devices—"bombes,"invented by Polish mathematician Marian Rejewski (1905–1980) and possibly named for the loud ticking noises they emitted while functioning—were electromechanical (i.e., used a combination of electrical currents and moving parts). Bombes sufficed for the Enigma cipher, but to crack the SZ42 and Geheimschreiber ciphers, the Allies built what is sometimes considered the world's first electronic computer, the Colossus. The Colossus was based primarily on the ideas of British engineer T. H. Flowers (1905–1998) and British mathematician Alan Turing (1912–1954). (An "electronic" computer, as opposed to an electromechanical device, does not use moving parts to perform its calculations.)

Cipher-machine technology reached its peak in the Geheimschreiber and SZ42 cryptosystems, achieving a level of cryptographic security that could only be breached by the invention of a wholly new technology: the electronic computer. Nevertheless, all the major German ciphers of the World War II—and the primary Japanese cipher too, codenamed Purple—were broken by the Allies.

The Allies also used cipher machines during World War II, but with better luck, as the Axis governments did not succeed in breaking Allied ciphers routinely. The United States Army's primary cipher machine descended from a compact device invented by Swedish inventor Boris Hagelin (1892–1983) in the mid 1920s. Hagelin's cipher machine, originally designated the B-21, sold thousands of copies to the French military between 1934 and the French defeat in World War II. The U.S. Army purchased Hagelin's machine after the German invasion of Norway in 1940 and redesignated it the M-209. More than 140,000 M-209s were manufactured before the end of the war. The M-209, like the SZ42, employed the stream-cipher technique, with matched generation of the key-stream at the transmitting and receiving ends of each link. Interestingly, this technique is still used today in applications such as digital pay-TV, file encryption, and communication with secure Web sites; however, electronic, rather than mechanical, generation of the pseudorandom key stream is used.

Cipher machines continued to be used by many countries for some years after the end of World War II, but were slowly rendered obsolete by the increasing availability of general-purpose digital computers. The displacement of cipher machines by computers was inevitable for several reasons. A computer can be flexibly reprogrammed to implement any number of ciphering schemes, whereas a cipher machine can implement only the cipher it is built for. Further, electronic computers operate at far higher speeds than can mechanical devices. Today, all serious

ciphering is performed using digital computers, and the only remaining ciphering machines are in museums.

FURTHER READING:

BOOKS:

Churchouse, Robert. *Codes and Ciphers.* Cambridge University Press, 2002.

Deavours, Cipher, et al. *Cryptology: Machines, History and Methods.* Norwood, MA: Artech House, 1989.

Singh, Simon. *The Code Book.* New York: Doubleday, 1999.

SEE ALSO

ADFGX Cipher
Cipher Pad
Codes and Ciphers
Purple Machine

Cipher Pad

LARRY GILMAN

A cipher pad is a printed list of cipher keys, each intended to be used for the encipherment and decipherment of a single message. Cipher pads (also termed one-time pads) are closely related to one-time tapes and stream ciphers, which are discussed below.

A key is a string of letters or numbers that is needed to correctly encipher or decipher a message. Each distinct key produces a unique ciphertext from a given plaintext (and vice versa). Both sender and receiver must therefore, know the key associated with a specific message if the message is to be successfully enciphered and deciphered. As long as the key remains unknown to an opponent, the enciphered message is secure. If an opponent, however, does manage to steal or guess the key—for example, by systematically trying out all possible keys—then they will have broken the cipher and can decipher the secret message. Another weakness of ordinary key-based ciphering is that the more text is sent using a single key, the easier it is for an opponent to deduce the key by analysis of intercepted messages.

These facts suggest two basic rules of key use: (1) Change keys often. This prevents an opponent from building up a large mass of text, all enciphered by the same key, which can be used to deduce the key. (2) Use long keys. This makes it impractical for an attacker to find the right key by pure guessing. For example, if the key is a 56-bit binary number (as it is for the Data Encryption Standard, a U.S.-government-designed ciphering system widely used since 1977), then there are $2^{56} > 7.2 \times 10^{16}$ possible keys.

A cipher-pad system takes key changing to a logical extreme by using a different key for every message. The keys used are, furthermore, long enough to keep an opponent from simply guessing at them. These selected keys are printed in a book (the cipher pad), the pad is distributed to all senders and receivers, and the keys in the pad are used up one by one as messages are sent. This has the disadvantage that only a limited number of messages can be sent before a new cipher pad must be printed and distributed. Also, as with codebook systems, there is always the danger that a copy of the book will be captured. For these reasons, printed cipher pads have not often been used.

Principle of ciphering. The cipher-pad principle is important, however, when combined with the following fundamental principle of ciphering: *A cipher employing a key that is at least as long as the message itself and is never used for any other message can be made truly unbreakable.* This is easy to verify: imagine a message 50 letters long that has been encrypted using a key 50 letters long. To guess the correct key means trying out all possible 50-letter strings. Even if this were practical—and it is not, for there are $26^{50} > 10^{70}$ such strings, more than the number of atoms in our galaxy—generating all keys 50 characters long is the same thing as generating all messages 50 characters long. Generating all possible messages is the same as simply guessing at what the message is, which is the same as being unable to break the cipher.

The first mechanized application of this principle was the one-time tape system, invented early in the 20th century by U.S. cryptologist Gilbert Vernam (1890–1960) and perfected by Major Joseph Mauborgne of the U.S. Army in 1918. In this system, a message is encrypted as a series of punched holes on a long paper tape. The holes on the message tape are a function of both the message and a randomly generated key (character string) that is as long as the message itself. The key is stored on one tape and the message on the other, and both tapes are shipped by different routes to the intended recipient. The tapes are read simultaneously by a machine that outputs the deciphered text. There is an obvious disadvantage to this technique: the need to send the key. This rules out any kind of telecommunications, for if an enemy intercepted both the key sequence and the message sequence they could decipher the message. Thus, only a perfectly secure transmission channel can be trusted with such information. If the transmission channel is perfectly secure, then there is no need to cipher. The one-tape system is thus, limited to situations in which physical transport of messages is practical.

This limitation is overcome in modern communications by the use of pseudorandom numbers. A truly random number sequence is one that contains no overall

structure or pattern; a pseudorandom number sequence is one that looks like truly random sequence but is in fact produced by a series of arithmetical calculations that can be repeated at will. Pseudorandom number sequences are easy to generate in digital computers using arithmetical procedures termed pseudorandom number generators (PNGs). The bits produced by a PNG can be strung together into a stream that is as long as any desired message. This stream of bits is termed "the cryptographic bit stream" or "key-stream." A message can then be encrypted by performing the EXCLUSIVE OR (XOR) operation pairwise on bits from the message-stream and the key-stream. The XOR operation for two bits is defined as follows:

INPUT 1	INPUT 2	OUTPUT (XOR)
1	1	0
1	0	1
0	1	1
0	0	0

The following is a message-stream, a key-stream, and the encrypted bitstream produced by XORing the message-stream and the key-stream together:

Message-stream:	1 0 1 1 0 0 0 1
Key-stream:	0 1 0 1 0 0 1 1
Encrypted bitstream:	1 1 1 0 0 0 1 0

It is easy to verify that each bit in the encrypted bitstream is the XOR of the two bits above it.

The XOR function is used for encipherment because it has the following useful property: the XOR of the encrypted bitstream and of the key-stream recovers the message-stream.

Encrypted bitstream:	1 1 1 0 0 0 1 0
Key-stream:	0 1 0 1 0 0 1 1
Recovered message:	1 0 1 1 0 0 0 1

In the example above, it is easy to verify that each bit in the recovered message is the XOR of the two bits above it. Because cipher systems of this type work on streams of bits, they are termed stream ciphers.

The discussion so far assumed that the receiver of the encrypted message has access to the same key-stream as the sender. In a cipher-pad or one-time-tape system, agreement on the key sequence is assured by sending the key (on paper or some other medium) to both ends of the link. In a stream cipher, it is assured by generating the key-stream at both ends of the link. Because the pseudorandom bits of the key-stream are generated by a PNG, both ends of the cipher link need only start their PNGs at the same point in its series of operations to generate the same key-stream. This can be accomplished by transmission to the receiver of a group of numbers termed a "seed" or "initializing vector."

Quantum cryptography. Weak points exist even in this system. For example, all PNGs start to repeat themselves eventually, and so do not produce truly random numbers. Also, the initializing vector must be known somehow at both ends of the cipher link. The answer to these difficulties may be resolved using quantum cryptography. In quantum cryptography, stream ciphering returns to the old idea of sending a key-stream along with the message. However, the key-stream is not sent on a paper tape or even as a conventional digital message. It is generated by the sender as a series of truly random subatomic events and shared by the sender and receiver using pairs of "entangled" photons that cannot, by the most fundamental laws of physics as they are now understood, be intercepted without revealing the presence of the eavesdropper.

Real-world quantum-cryptographic systems are being developed rapidly, and proof-of-concept systems have already been built. Thus, there seems to be no basic obstacle to the development of truly unbreakable quantum-cryptographic systems, the ultimate development of the cipher-pad concept.

FURTHER READING:

BOOKS:

Meyer, Carl H., and Stephen M. Matyas. *Cryptography: A New Dimension in Computer Data Security.* New York: John Wiley & Sons, 1982.

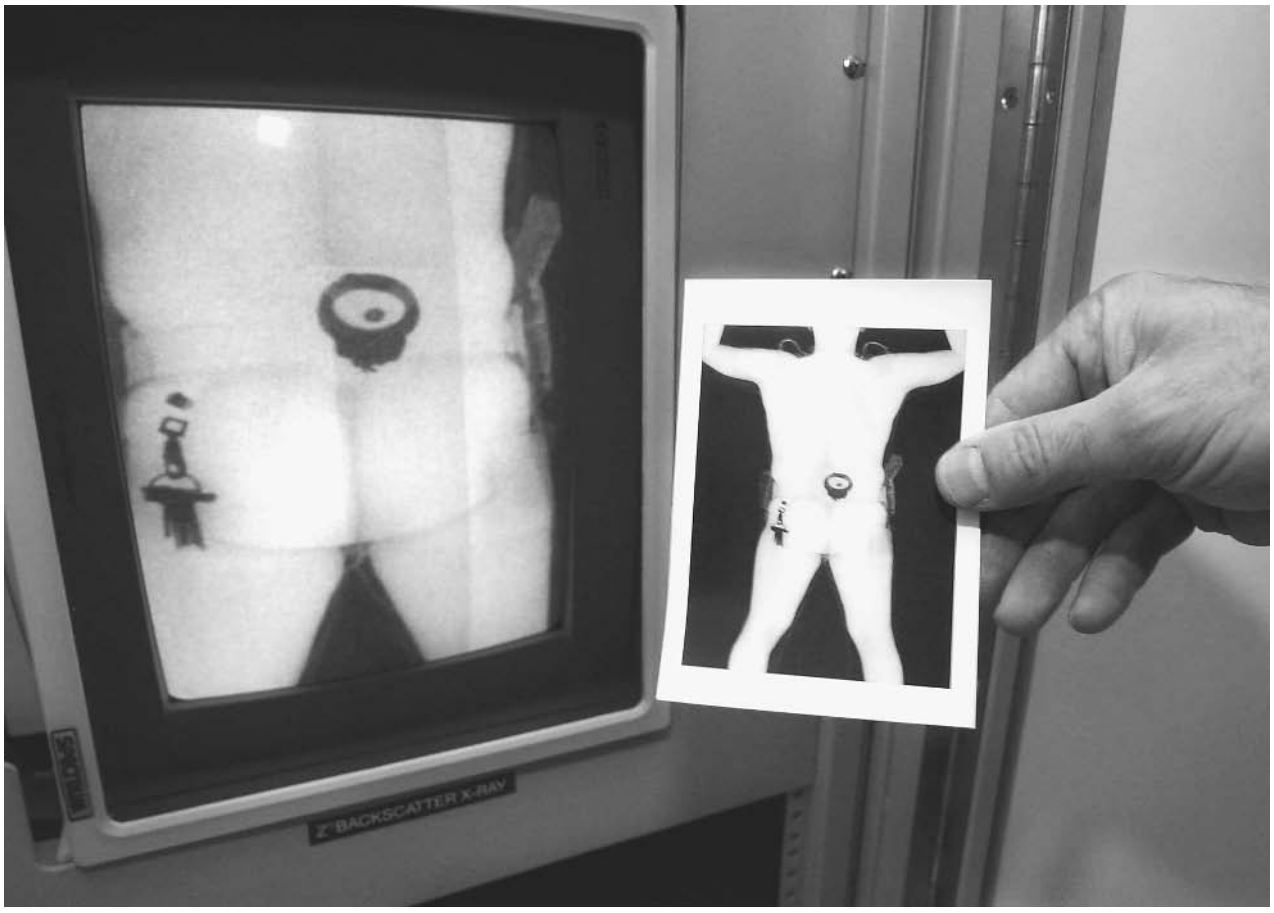
Mollin, Richard A. *An Introduction to Cryptography.* New York: Chapman & Hall, 2001.

PERIODICALS:

Bennett, Charles H., and Peter W. Shor. "Privacy in a Quantum World." *Science* no. 5415 (1999): 747–748.

SEE ALSO

Codes and Ciphers
Quantum Physics: Applications to Espionage, Intelligence, and Security Issues



A customs officer inspects a BodySearch image, which uses x-ray technology to allow inspectors to detect contraband on arriving passengers who choose not to submit to the traditional "body pat down." AP/WIDE WORLD PHOTOS.

Civil Aviation Security, United States

JUDSON KNIGHT

Civil aviation security in the United States is directed by the Transportation Security Administration (TSA), which was created after the terrorist attacks of September 11, 2001, under the Aviation and Transportation Security Act (ATSA). Prior to November 19, 2001, when President George W. Bush signed ATSA into law, the Federal Aviation Administration (FAA) handled civil aviation security. The passage of the new law, and the creation of the new administration, required changes to the federal statutes covering aviation security, which are contained in Title 49 of the Code of Federal Regulations, Chapter XII parts 1500 through 1699.

ATSA mandated increases in the numbers of federal air marshals, and placed airport security screeners under federal control. It required that all screeners be U.S. citizens (a provision later challenged by the American Civil Liberties Union), and that all bags be screened or matched to passengers. It also included provisions for awards of $1.5 billion to airports and private contractors to meet the direct costs of meeting new security requirements.

The law created TSA, to be headed by a Transportation Department undersecretary for security appointed by the president and confirmed by the Senate. Overseeing TSA would be a new Security Oversight Board consisting of cabinet secretaries, or their designees, from the departments of Transportation, Defense, Treasury, Justice, and Homeland Security (the latter, then the Office of Homeland Security, became a cabinet-level department on March 1, 2003), as well as one representative each from the Central Intelligence Agency and the National Security Council.

The undersecretary would appoint a federal security manager at each airport nationwide, and was authorized to provide air marshals as he or she saw fit. Each flight deemed a high security risk would have air marshals, who could be appointed at the undersecretary's discretion. In consultation with airport and law enforcement officials,

the undersecretary would order the safeguarding or airport areas as needed.

In the field of airport security screeners, these were placed under federal control as uniformed TSA employees. Airport security screeners had to be proficient in English, pass background checks, undergo a minimum of 40 hours' classroom instruction or the equivalent, complete 60 hours on-the-job training, and be tested each year.

In addition, the undersecretary was authorized to establish a test program whereby five airports (one from each of five levels of security risk) would be permitted to contract directly with private companies. These companies would have to have standards at least as high as those of the federalized screening force, which would operate at all other hub airports—of which there were 424 total in the United States at the time—for two years. At the end of two years, airports would be allowed to opt out of the federalized screening program if they so choose.

Within 60 days, all checked baggage would have to be screened, either by explosives detection machinery, or manually. The law also authorized the Secretary of Transportation to require airports to use all necessary equipment for the detection of chemical or biological weapons.

FURTHER READING:

PERIODICALS

Croft, John. "Air Security Bill Clears Lawmakers' Logjam." *Aviation Week & Space Technology* 155, no. 21 (November 19, 2001): 46.

"Responses to ASR's Survey on Aviation Security Post-Sept. 11." *Airport Security Report* 9, no. 19 (September 11, 2002): 1.

"S. 1447, Aviation and Transportation Security Act." *Airports* 18, no. 48 (November 27, 2001): 5.

ELECTRONIC

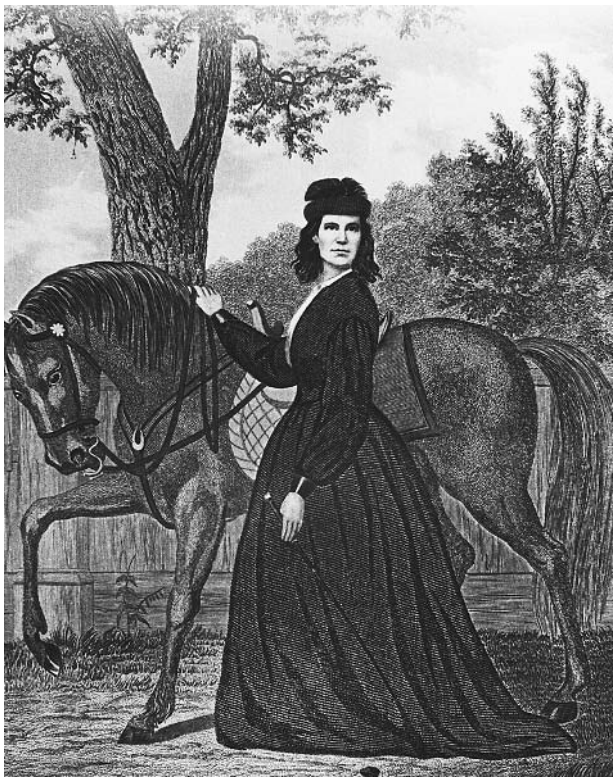
Transportation Security Administration. <http://www.tsa.gov/public/> (March 5, 2003).

SEE ALSO

Air marshals, United States
Aviation Security Screeners, United States
FAA (United States Federal Aviation Administration)
September 11 Terrorist Attacks on the United States
Transportation Department, United States

Civil War, Espionage and Intelligence

WILLIAM J. ENGLE



Portrait of Emma Edmonds, famous woman spy of the Civil War.

During the great American conflict of the middle nineteenth century, the Civil War, efforts by both the North and South to engage in espionage and intelligence-gathering activities were unparalleled in the history of the relatively young nation. Although daring, these efforts were often quite amateurish by modern standards.

The physical environment of America greatly facilitated covert activities. With America as the "melting pot" of the world, people throughout the nation represented every race and nationality in the world. Unionist and secessionist alike came from every corner of the country and both sides consisted of people of every race, creed, and color. Visually, covert combatants could not be easily identified one from another. Americanized English was the common language, but even with many regional dialects, there were few specific speech patterns unique to either side. State or region of origin was no guaranty of which side one might take in the conflict.

People were free to travel practically at will. Boundaries between Union and the Confederate held areas existed primarily as lines on a map and posed no controlled barrier to travel. Many major rivers traversed the land north to south. Major mountain ranges trended north/south. Railroads and roadways had been developed in all directions. Getting to and from one area to another was relatively easy and borders were difficult to control. Spies and agents were free to roam practically at will restricted more by their own skill and courage than any other factor.

With travel being relatively unimpeded it was fairly easy to pass written or memorized verbal messages through the lines. Both sides developed methods to encrypt messages using various forms of alphanumeric sequence codes and cipher wheels. The telegraph was the leading communication technology of the period. Anyone with a portable key set could tap into any line and monitor, receive, and send massages often confusing and countermanding orders being sent over the wire. Confederate cavalry leader John Hunt Morgan habitually included a telegraph operator on his staff just for this purpose. Hunt was so daring as to send a message to the U.S. Commissary Department over telegraph lines operated by the U.S. Army complaining about the quality of mules being supplied to units opposing him and being captured by his men. Requisitions for supplies were often submitted in similar fashion in anticipation of capture from the adversary.

Hot air balloons were introduced by both sides for observing troop movement and disposition, spotting artillery fire and relaying signals.

The Confederacy led in the development of "infernal weapons" such as mines and torpedoes that were, at the time, considered violations of the rules of war as they acted upon unsuspecting prey. The concept of these devices was relatively simple in including a black powder charge within a watertight container and a detonation device. The Brooke buoyant torpedo consisted of a metal dome with contact detonators on top mounted on a metal conical shaped container attached to a wooden spar anchored on the bottom of a waterway. At times a Turtle torpedo containing as much as 100 pounds of explosives would be attached by wire to the base of the spar. Attempts to remove the adjacent buoyant torpedo would pull the wire and detonate the Turtle. Other torpedo designs included floating containers detonated by contact or electrical charge from a shore based agent and free floating drifting mine detonated by an attached propeller mechanism after coming to rest against the hull of a ship. River and sea torpedoes could be placed by agents or troops in advance of the arrival of the opposing force.

However, the Coal torpedo required placement in a fuel storage depot or bunker by an agent and quite often in the presence of the enemy. The Coal torpedo was made of a hollow chunk of iron cast to look like a piece of coal. The fake coal contained a charge of powder and was coated with tar and coal dust and exploded with tremendous effect when fed into the boiler fire of a steam engine either on board a ship, on a train or in a factory.

Agents on the ground were the backbone of the espionage and intelligence gathering efforts of the period. Unfortunately the identity of most of the agents of the conflict was lost as many operated under multiple names; records were often poorly kept, and lost or intentionally suppressed or destroyed. Contraband and escaped slaves served as a primary source of intelligence for the U.S. Army. However, a former barrel maker, sheriff and native of Scotland organized a detective agency in 1850 that served the Union effort extensively and is still in business today. Alan Pinkerton formed the National Detective Agency and gained fame by foiling a plot to assassinate President Lincoln in 1861 and went on to create the secret service of the U.S. Army. Neither Pinkerton nor his agents had any training in intelligence gathering and were notorious for their tactics and the over-estimation of Confederate troop strength. During the Peninsula Campaign over the spring and summer of 1862, General G. B. McClellan (U.S.) had advanced the Army of the Potomac and its 108,000 effectives to within sight of the church spires of the Confederate capital city—Richmond, VA. However, based on intelligence gathered by Pinkerton that suggested a potential opposing Confederate force nearing 200,000 who were well fortified with reinforcements en route, the general paused to plead his case with Lincoln for more troops. In fact, General R. E. Lee never had more than 85,000 effectives under his command during this time, as his smaller force drove the Federal horde before him in full retreat. Pinkerton's unintended misinformation may well have served the defense of the Confederate capital city better than the mythical reinforcements that were not coming. It would be some two and a half years before the U.S. Army would get that close to Richmond again. Yet, Pinkerton and his organization remained in Federal service well beyond the war. Much of Pinkerton's information came from criminals and escaped slaves who lacked the skills of espionage and were thus, prone to exaggeration, along with agents who may have spent more time enjoying Richmond's pleasures than actually counting troops in the field. In time, the Confederates learned to appreciate the value of misinformation and intentionally sent men forward to become captives of the Federal forces and spread inaccurate information.

American culture was still quite Victorian in many ways during the 1860's. Women agents had a decided advantage over their male counterparts, as they were not likely to be as roughly interrogated or possibly executed upon discovery. Both sides took full advantage of the opportunity.

Belle Boyd shot and killed one of two drunken Union soldiers who had entered her Martinsburg, VA home on July 4, 1861. She was acquitted and set free. Thereafter, Boyd voluntarily forwarded her written observations of Union activity in her area to local Confederate authorities. During General "Stonewall" Jackson's Shenandoah Valley Campaign, Union troops occupied the town of Front Royal, VA where Miss Boyd happened to be at the time. Observing the panic that developed among the invading Federals upon their learning of Jackson's approach and overhearing their plans to burn a large supply depot in town and the bridges across the South Fork of the Shenandoah River as they retreated northward, seventeen year old Belle decided to inform the Confederate forces personally. Under fire from Union pickets, Boyd dashed several

miles to carry her knowledge to the approaching Confederate column. The leading elements of the column then dashed forward to save the bridges that later enabled Jackson to drive up the valley driving the forces of Union General Nathaniel Banks before him and freeing the vital area's food supply to Confederate purpose.

Belle Boyd continued her activities until arrested on July 29, 1862, and was transferred to the Old Capital Prison in Washington, D.C. No charges were pressed and she was released one month later, where upon she returned to Richmond and continued her work as a spy. Later she was arrested aboard the blockade runner *Greyhound* outbound for England but managed to persuade Federal Lieutenant Harding, who had been placed as prize master of the captured ship, to permit Confederate Captain Lewis to escape en route to Boston. Before the end of the war, Miss Boyd and Lt. Harding married.

Elizabeth Van Lew, a native of Richmond, VA who had attended a Philadelphia Quaker school, was an ardent opponent of slavery and pro-Union. After the war broke out, Van Lew was granted permission to care for Union prisoners. Many of the prisoners had observations of Confederate positions and troop dispositions that they hoped to get back to Union authorities. Miss Van Lew established a network of couriers, developed a secret code, and began passing messages through the lines to Union forces. Many in Richmond referred to her as "Crazy Bet" as she hummed and mumbled to herself as she traveled the town, while believing her sympathy for the Union was part of her mental illness. "Crazy Bet" is credited with procuring for Mary Elizabeth Bowser, a former slave whom she had freed before the war, a job as a house servant in the home of Confederate President Jefferson Davis. Together, the two women collected valuable information that was passed on to Union officers. "Crazy Bet" managed to maintain her cover throughout the war and was one of the first people to be visited by General U.S. Grant upon the taking of Richmond. Later, President Grant appointed her postmaster of Richmond though the people of the city shunned her once they realized the harm she had rendered to the Confederate cause.

Emma Edmonds, who was able to join a Michigan volunteer company by posing as a man, gathered information for her company by "posing" as a woman.

Legends and folklore are rich with stories of individual daring and accomplishment as agents and double agents during the Civil War, but verifiable documentation is only available in a few cases. Some of the best intelligence gathering opportunities came about as random luck. Perhaps one of the most significant instances of pure luck delivering critical information into the hands of the enemy was the discovery of a copy of General R. E. Lee's order of march as he moved northward in September of 1862. A note was found on the ground wrapped around three cigars by Federal soldiers that contained details of the order of march of General R. E. Lee's divided forces marching through the Shenandoah Valley on their way to carry the war to the North on their home ground. Some historians assume that a member of General D. H. Hill's subordinate command dropped this bit of critical information. Union General G. B. McClellan had been cautiously seeking the Confederate force, and the discovery of General Lee's order of march enabled McClellan to unexpectedly close on them and force an unplanned battle near Sharpsburg, MD along Antietam Creek. The battle unfolded to become the most deadly single day of combat in American history, and ended in a tactical victory for the South in that its army escaped annihilation and withdrew southward in good order after Union forces refused to attack the following day. However, the North claimed a major strategic victory that changed the nature of the war, and ended consideration of European intervention on the side of the South.

Both the Union and the Confederacy had agents working throughout the territory of the other. The Northern media proved to be of great aid to the Southern intelligence gathering effort. Northern papers continually ran articles describing current events, Union troop dispositions, and future movement in such detail that undercover Confederate agents kept a constant supply of daily newspapers heading south from major cities such as New York, Philadelphia, and Boston to commanders in the field.

Spying was not limited only to opponents. There was considerable spying by various political factions on their own battlefield commanders and faction against faction. This was particularly true on the Union side where trust between President Lincoln, the cabinet, prominent congressmen, and the military staff was particularly low during the early years of the war, as the search for a commander who could defeat the secessionists created considerable turmoil. Many Federal commanders also dreaded the political opponents in their rear as much as the combat opponents to their front, as many officers were removed to satisfy public whim.

■ FURTHER READING:

BOOKS:

Coggins, Jack. *Arms and Equipment of the Civil War.* Wilmington, NC: Broadfoot Publishing Company, 1990.

Canton, Bruce. *The Civil War.* New York: American Heritage/Wings Books, 1960.

Foote, Shelby. *The Civil War—A Narrative.*New York: Vintage Books/Random House, 1986.

Stern, Philip Van Doren. *Secret Missions of the Civil War.* New York: Wings Books, 1990.

ELECTRONIC:

University of Virginia, "Hearts at Home: Spies <http://www.lib.virginia.edu/speccol/exhibits/hearts/spies.html>(March 22, 2003).

Alberta Lee, daughter of Los Alamos scientist Dr. Wen Ho Lee, protests her father's imprisonment outside the Federal Building in San Francisco. Lee was arrested in 2000 for mishandling classified information. AP/WIDE WORLD PHOTOS.

Classified Information

JUDSON KNIGHT

Classified information is any data or material that belong to the federal government and relate to sensitive topics such as military plans or the vulnerabilities of security systems. A number of laws or rules govern the control of classified information and access thereto, as well as the declassification of items no longer sensitive. Thanks to Executive Order 12958, a number of formerly classified documents regarding the Cold War and other critical junctures in U.S. security history are now accessible to the general public.

As defined in the Classified Information Procedures Act (CIPA), passed by Congress in 1980, classified information is any information or material that has been determined by the United States government pursuant to an executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph R of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014[y])

The act names executive orders before legal statutes, because these orders—more than acts of Congress, decisions of the Supreme Court, or other rulings—are among the principal governing authorities in matters of security classification and access to classified information. In addition to executive orders, there are also other non-parliamentary government directives that present guidelines on classified information and access.

For the present purposes, it is helpful to be a bit more explicit than CIPA, and—using as a basis various executive orders, as well as historical practice—define classified information as materials or data belonging to, controlled by, and/or produced by the federal government, pertaining to intelligence sources or methods of collecting information; cryptology or codes; and the vulnerabilities, capabilities, or planning of systems, installations, or projects that relate to national security. Access to information thus "classified" is restricted on the basis of its relative importance, the consequences that would follow if it were passed to the wrong parties, and the individual's "need to know" that information.

Laws on classification procedures: An introduction. Federal laws on classification procedures provide for governing authorities who determine what information should be subjected to rules of restricted access. Specifically, Executive Order 12958, discussed below, defines the "original classification authority" as "an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance." This governing authority also determines the level of classification, of which are three major ones: confidential, secret, and top secret. (The levels of security clearance are discussed in more detail elsewhere, within the context of security clearance investigations.)

A number of laws govern classified information, but most are not "laws" in the sense that they were duly reviewed by Congress or the Supreme Court; rather, the majority of guidelines in these matters come from executive orders or presidential directives (which are classified), as well as directives from the National Security Council, the director of Central Intelligence, the Department of Defense, and so on. A rare exception to this is CIPA, the Classified Information Act, which came into being through the ordinary channels of legislative procedure most commonly associated with a republican democracy. Even so, it has often been used to protect the "shadow government" of the security and espionage apparatus.

Classified Information Act (CIPA). Passed by Congress on October 15, 1980, CIPA was codified as 94 Stat. 2025, 18

Speaker of the House of Representatives Dennis Hastert listens as Senate Majority leader Tom Daschle talks with reporters in October 2001, about Congressional leaks of classified information. AP/WIDE WORLD PHOTOS.

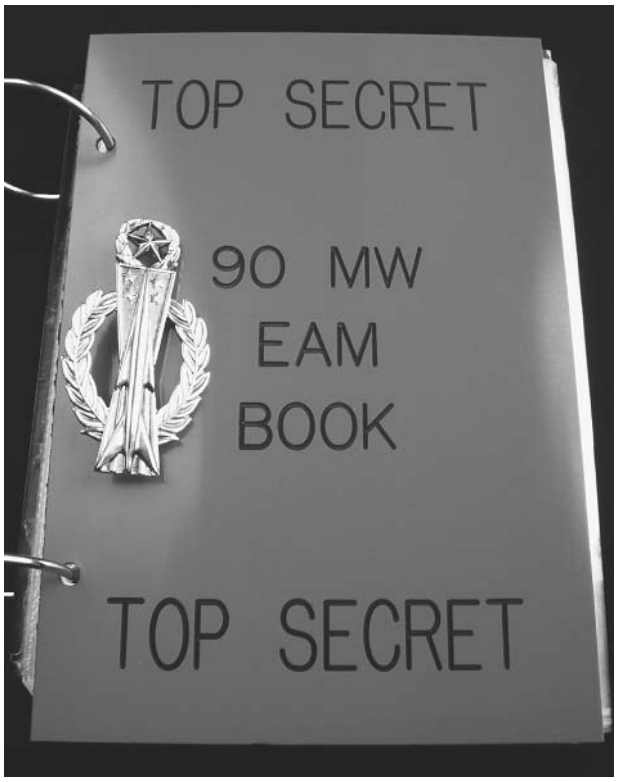
U.S.C. Appendix, and further amended November 18, 1988, in 102 Stat. 4396. Known in legal circles as a procedural statute, CIPA presents guidelines for the use of classified information by both government and defendant in a legal case. As a procedural statute, it neither adds to nor subtracts from the rights of the defendant or the obligations of the government; rather, it is designed to prevent both sides from unauthorized disclosure of classified information, and to apprise the federal government of any security breach that may result from proceeding with a case.

During the Iran-Contra conspiracy trials in 1988, attorneys representing defendants Oliver North, John Poindexter, Richard Secord, and Albert Hakim filed a petition with U.S. District Judge Gerhard A. Gesell, stating that CIPA "imposes burdens on the defense unprecedented in American law." Because so much of their case rested on classified information, the defense argued, it would be legal suicide to disclose all of that information to the prosecution.

CIPA continued to be a theme throughout the proceedings. In July 1989, North's attorneys filed an appeal stating that Gesell, who established guidelines for compliance with CIPA, nevertheless permitted infringement of North's constitutional rights. Later, Senate majority leader George Mitchell complained that CIPA was too lenient, because it allowed Thornburgh to put a stop to the trial of Costa Rica Central Intelligence Agency (CIA) station chief Joseph F. Fernandez for his role in Iran-Contra.

More than a decade after Iran-Contra, attorneys representing Chinese scientist Wen Ho Lee, accused of stealing secrets from the Los Alamos National Laboratory, attempted to use CIPA in a way different from that of North or Poindexter. Instead of withholding information, they were convinced that the release of highly sensitive data that the government had no desire to reveal publicly was a major reason for the government to avoid vigorous prosecution of Lee on the most serious charges.

Executive Order 12958. The most significant presidential provisions regarding classified information are the executive orders 12958 and 12968, both issued by President William J. Clinton. The second of these is discussed elsewhere, in the context of security clearances. The first,



A top-secret procedure manual used for instructing military officers in the event of a nuclear missile launch rests on a desk at the Warren Air Force Base missile launch complex. ©JAMES A. SUGAR/CORBIS

titled "Classified National Security Information," was signed on April 17, 1995. According to its opening sentence, the order "prescribes a uniform system for classifying, safeguarding, and declassifying national security information."

In addition to defining "classification" and the basic levels thereof, as well as types of information that may be classified, the order provides that "If there is significant doubt about the need to classify information, it shall not be classified." Furthermore, "If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level." The order prescribes the use of classification markings to distinguish varieties of classified information, and provides for "derivative classification," or "the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information."

Declassification and Executive Order 13142. Particularly important are the provisions of Executive Order 12958 with regard to declassification, or the removal of restrictions on access to information. Declassification is not to be automatic, "as a result of unauthorized disclosure of identical or similar information." However, except in specific circumstances, information is to be automatically declassified after 10 years. Those specific circumstances include situations in which national security would be jeopardized by disclosure of the information, as well as instances in which automatic declassification could violate a legal statute. A notable example of such a statute is the Privacy Act of 1974.

Executive Order 13142, signed November 19, 1999, amended 12958 by extending the amount of time until certain types of information can be declassified. Specifically, the order addresses Section 3.4 in the earlier order, which provides for the declassification of information more than 25 years old that has been determined to have historical value in accordance with Title 44, U.S. Code. Whereas the earlier order had provided for declassification within five years, 13142 extended this period for 18 months. As the *Washington Times* reported in December 1999, this change angered the American Legion and other veterans' groups eager to search records from the Vietnam era for information regarding prisoners of war (POWs) and others who were missing in action (MIAs).

Post-12958 declassification efforts. An August 1998 White House press release called Executive Order 12958 became "the first effort since the end of the Cold War to reassess the balance between open government and the need to maintain secrets vital to national security." Although critics disputed White House claims as to the extent of the effort, the order did open a vast body of information for declassification. According to the press release, the Interagency Security Classification Appeals Panel established by the order had, in the three years that followed its issuance, reviewed some 96 documents and released 81 of them.

Among these were documents from the administrations of presidents Dwight D. Eisenhower, John F. Kennedy, and Lyndon B. Johnson regarding the deployment and possible use of nuclear weapons in Europe; two 1962 letters from Indian Prime Minister Jawaharlal Nehru to Kennedy expressing fears of an impending nuclear war between his nation and China; State Department communications regarding Israeli nuclear capabilities during the June 1967 Six-Day War; and a September 1967 memorandum to Johnson regarding military options available to the North Vietnamese army. Less than 25 years old were documents from the administration of President Gerald R. Ford concerning nuclear weapons programs in South Korea. Some of the latter information remained classified, because disclosure would endanger a source, or because its release would harm U.S. relations with foreign governments.

NSA and NIMA records. The National Security Agency (NSA) subsequently undertook a review of documents for declassification, a project it named OPENDOOR. As NSA announced in a press release dated April 2, 1996, it had

turned over some 1.3 million pages of declassified documents to the National Archives and Records Administration (NARA). Intriguing as the contents were, these documents were far more than 25 years old; rather, they dated from the beginning of World War I to the end of World War II. Among them were a cryptologic study of the 1917 Zimmermann telegram that precipitated U.S. entry into World War I; information on the Native American "Codetalkers" of World War II; and the captured diary of a Nazi U-boat.

Much more recent were the photographs released by the National Imagery and Mapping Agency (NIMA) in 1996 and again in 2002. These included millions of frames of imagery taken by KH-1 through KH-6 spacecraft, the KH-7 Surveillance Imaging System, and the KH-9 Geospatial Imaging System. Taken between 1963 and 1980, the images from the "Keyhole" satellites included shots of Hanoi and Beijing, Egypt's Aswan Dam, the Eiffel Tower, and the U.S. Capitol building. Still withheld were numerous images, some dating as far back as 1963, that were still considered too sensitive for release.

NARA, CIA, and the Continuing Task of Declassification. Further information regarding documents released in accordance with Executive Order 12958 is available at the NARA Web site. With the help of teams sent by CIA under a project known as "Remote Archives Capture Project," NARA had by the early twenty-first century declassified millions of pages of material. Among these were State Department files offering information on Nazi gold from World War II; Kennedy's tapes of conversations during the Cuban missile crisis of October 1962; the January 1968 incident in which sailors from the U.S.S. *Pueblo* were captured by North Korea; headquarters reports from U.S. military commands in Vietnam and Thailand through 1975; information on POWs and MIAs from Korea and Vietnam; and records of U.S. participation in SALT (Strategic Arms Limitation Talks) negotiations.

It was an intriguing collection, but much remained to be processed by historians, scholars and archivists. Some of the processed information may remain classified indefinitely. According to Michael J. Kurtz, aside from "unique items such as Secret Service records relating to the protection of the President and Internal Revenue Service tax information," items exempted from release fell into four basic groups: information on atomic energy; intelligence sources and methods; sensitive foreign-relations topics (e.g., U.S. discussions on border disputes between other nations, such as that between India and Pakistan over Kashmir); and information from foreign governments that the latter had not approved for release.

■ FURTHER READING:

BOOKS:

Disclosure of Classified Information to Congress. Washington, D.C.: U.S. Government Printing Office, 1998.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* third edition. Boulder, CO: Westview Press, 1995.

PERIODICALS:

Black, Chris. "Mitchell Urges New Classified Data Law." *Boston Globe.* (December 5, 1989): 3.

Elvin, John. "We've Waited Long Enough." *Washington Times.* (December 27, 1999): 26.

Lardner, George, Jr. "Classified Trial-Data Law Attacked." *Washington Post.* (April 30, 1988): A4.

ELECTRONIC:

Declassification and Freedom of Information Act (FOIA). Defense Prisoner of War/Missing Personnel Office. <http://www.dtic.mil/dpmo/foia/> (January 21, 2003).

OPENDOOR. National Security Agency. <http://www.nsa.gov/programs/opendoor/> (January 21, 2003).

U.S. National Archives and Records Administration. <http://www.archives.gov> (January 21, 2003).

SEE ALSO

Clinton Administration (1993–2001), United States National Security Policy
Executive Orders and Presidential Directives
Iran-Contra Affair
National Archives and Records Administration (NARA), Unites States
NIMA (National Imagery and Mapping Agency)
Security Clearance Investigations

Clinton Administration (1993–2001), United States National Security Policy

■ CARYN E. NEUMANN

President William Jefferson (Bill) Clinton argued that the end of the Cold War did not mean that the United States could abandon its long-standing aim of ensuring national security by promoting democratization around the world. Now the sole surviving superpower, the U.S. in the 1990s would continue to assertively support democracy but not in a manner that might place American troops in great jeopardy. Fearful of becoming stuck in a Vietnam-like quagmire, the Clinton administration would employ force as a tool of coercive diplomacy and punishment but avoid full-scale conflict. The national security system, re-designed by the new president, would also de-emphasize military issues in favor of a greater emphasis upon economics in the formulation of policy.

President Clinton entered the White House in 1993 with little experience or enthusiasm for international affairs. The first president to take office after the end of the Cold War, President Clinton was also the first to come of

President Bill Clinton, at the head of the table, meets with national security advisors at the White House in November 1995, to discuss the peace agreement in Bosnia. AP/WIDE WORLD PHOTOS.

age during the Vietnam War and he saw national security through the prism of that conflict. Vietnam shaped the Clinton administration in two ways: it made the president reluctant to commit troops to combat and it damaged his standing with the military because he had not served in the military during the conflict. The relative worldwide calm after the dissolution of the Warsaw Pact and the American triumph in the Persian Gulf War made the marginalization of overseas issues politically possible.

As his first national security measure, Clinton issued a presidential directive to revise and rename the framework governing the work of the National Security Council. The previous Bush administration's National Security Review (NSR) and National Security Directive (NSD) series were abolished in favor of a Presidential Review Directive (PRD). The administration would use PRD to re-evaluate security classifications and the safeguarding of systems to ensure that they were in line with the reality of the current dangers instead of the threat potential that had existed during the Cold War.

The second presidential directive (PRD-2) established a new NSC structure, with a broader emphasis on economic issues than in previous administrations. PRD- 2 also established three levels of deliberative committees under the NSC: a principals committee of main NSC meetings, a deputies committee including deputy chiefs of key agencies, and working groups on a variety of issues. Warren Christopher served as Secretary of State, with Anthony Lake heading the NSC until his replacement by his deputy Samuel R. "Sandy" Berger in 1997.

The Clinton administration argued that the end of the Cold War permitted the U.S. to shift to a foreign policy that rested on support for such values as democracy, market economics, humanitarian relief, and genocide suppression. PRD-20 had recommended this overhaul of U.S. policies after concluding that foreign aid programs were often wasteful, incoherent, and inconsistent with U.S. objectives. The most urgent issues that the NSC dealt with in the first years of the Clinton administration were Bosnia (genocide suppression), Haiti (democracy and humanitarian relief), Iraq (strategic arms control), and Somalia (humanitarian relief). Most of the PRDs remain classified, but it is known that the NSC system also dealt with illegal drugs, United Nations peacekeeping, and global environmental affairs.

As Clinton settled into the presidency, he experienced increasing conflict with Congress and a public angered by his policies. A 1993 PRD to permit U.S. forces to operate under the control of a United Nations commander particularly enraged many conservatives and had to be abandoned. The administration responded to its critics by making overseas actions more modest in scope. In Clinton's second term, the administration sought to integrate Eastern and Western Europe without provoking tensions with Russia; to promote more open trade; to improve defenses against such transnational threats as terrorism and narcotics; and to encourage a strong and stable Asian-Pacific community by seeking trade cooperation with China while avoiding confrontation with it on human rights issues.

Critics of administration argue that it appeared to lack a clear consensus on what constituted vital national interests. The obvious reluctance of the president to risk significant numbers of troops to achieve declared political objectives prompted U.S. allies to express concern about reduced American global military involvement and may have encouraged continued troubles with "rogue" nations such as Iraq.

■ FURTHER READING:

BOOKS:

Drew, Elizabeth. *On the Edge: The Clinton Presidency*. New York: Simon & Schuster, 1994.

Herrnson, Paul S., and Dilys M. Hill, eds. *The Clinton Presidency: The First Term, 1992–96* New York: St. Martin's Press, 1999.

ELECTRONIC:

Digital National Security Archive. "Presidential Directives on National Security from Truman to Clinton." 2003. <http://nsarchive.chadwyck.com/pdessayx.htm>(April 25, 2003).

White House. "History of the National Security Council, 1947–1997." <http://www.whitehouse.gov/nsc/history.html>(April 25, 2003).

SEE ALSO

Cold War (1972–1989): The Collapse of the Soviet Union
Executive Orders and Presidential Directives
Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections)
Iraqi Freedom, Operation (2003 War Against Iraq)
National Security Advisor, United States
National Security Strategy, United States
NATO (North Atlantic Treaty Organization)
NSC (National Security Council)
NSC (National Security Council), History

Clipper Chip

In 1993, officials in the administration of President William Jefferson Clinton announced the proposed use of a cryptographic device intended to protect private communications for all but authorized monitoring by government agencies. Termed the "clipper chip," the device would permit secure encrypted voice communications, but would also allow United States law enforcement and intelligence agencies to monitor those communications by obtaining the algorithm keys to decrypt the transmissions.

As initially proposed the government would allow the keys to be maintained in a database held by an independent agent. Access to those keys would be permitted only as "legally authorized." Critics and privacy advocates immediately questioned the vague and broad use of the term legally authorized."

A chip similar in design and performance specifications, the Capstone chip, could be similarly regulated to allow secure data transmissions that could also be easily decrypted by United States law and intelligence agencies via known algorithmic keys.

An algorithm defines a repeatable step-by-step series of mathematical or language manipulation procedures to encrypt or decrypt a message or communication. Cryptology systems utilize algorithms and the labels, mechanics, recursive procedures, or other solutions are termed "keys" to the algorithm.

Use of the clipper chip was adopted and authorized in 1994. The National Institute of Standards and Technology (NIST) and the Department of the Treasury were designated to be the database repositories or "escrow" agents for the algorithmic keys. Rules regarding access to the keys were developed in accord with state and national security wiretap orders.

The clipper chip utilizes the SKIPJACK algorithm as part of the Escrowed Encryption Standard (EES) program. SKIPJACK was developed as a classified algorithm by the National Security Agency (NSA). SKIPJACk was initially developed as part of the Fortezza encryption suite and is a symmetric cipher with a fixed key length of 80 bits. Security experts assert that multiple encryption programs may eventually replace SKIPJACK like encryption-decryption programs.

■ FURTHER READING:

PERIODICALS:

Baker, Stewart A. "Don't Worry, Be Happy: Why Clipper Is Good for You." *Wired.* June 1994.

Johnson, George. "The Spies' Code and How It Broke," *New York Times, Week in Review.* July 16, 1995.

SEE ALSO

Cipher Key

Cipher Machines
Cryptology and Number Theory
Cryptology, History
NIST (United States National Institute of Standards and Technology)
NIST Computer Security Division, United States

Closed-Circuit Television (CCTV)

LARRY GILMAN

Closed-circuit television (CCTV) involves the use of video cameras to produce images for display on a limited number of screens connected directly to a non-broadcast transmission system (e.g., a network of cables). Commercial cable TV is, technically, an example of CCTV, but the term "closed-circuit TV" is generally reserved for systems serving a small number of screens that are monitored for security purposes. CCTV is a ubiquitous feature of institutional security systems. It is employed by prisons, banks, urban police forces, airports, military organizations, utilities, large corporations, various other organizations, and wealthy individuals. Some specific applications of CCTV are:

- X-ray baggage-inspection devices at airports.
- Remote viewing of dangerous industrial processes, rocket liftoffs, and other operations.
- Perimeter security around power plants, military installations, warehouses, police stations, and other defended facilities.
- Intrusion or theft monitoring of secure spaces, whether indoors (halls, lobbies, specific doors and rooms, etc.) or outdoors (parking lots, automatic teller machines, loading docks, etc.).
- Monitoring of vehicular traffic for traffic-control purposes or detection of illegal activity (speeding, smuggling, etc.).
- Identity-checking of persons desiring entry into a building.
- Computerized recognition of individual faces, with possible identification of "wanted" persons.

Two of the most important CCTV applications are discussed in more detail below.

Perimeter security. Prior to CCTV, in order to secure the perimeter of an area, it was necessary to post guards in such a way that their lines of sight covered the entire circumference of the area. With CCTV, it is possible to reduce the number of personnel needed to secure a perimeter by placing TV cameras at strategic points and transmitting the resulting images to a control room where a few guards can monitor many screens. Ideally, these observers will note any suspicious event on their screens and alert a response team. CCTV has thus for decades been a component of the typical Perimeter Intrusion Detection System (PIDS), which combines CCTV with devices designed to detect intrusion by other means (ultrasonic movement detectors, window alarm-contacts, etc.).

CCTV technology, however, has not proved as effective in PIDS applications as was once hoped. As vigilance studies by psychologists confirm, guards who spend hours "screen gazing" at static scenes (> 20 minutes, in tests) tend to become bored and less efficient, and are then likely to miss low-frequency events, such as a figure running up to and climbing over a fence. In the words of Geoff Thiel, a British CCTV-security expert, "Contrary to popular belief, impressive control rooms with large banks of monitors generally do not provide an effective "real time" surveillance service. The vast majority of installed CCTV cameras remain unwatched and incidents are not likely to be detected while they are occurring. CCTV is therefore reduced to a "post-mortem" tool. . ." (1999 International Carnahan Conference on Security Technology).

Starting in the 1980s, designers sought to combat the bored-guard effect by using automatic Video Motion Detectors (VMDs). These devices are designed to automatically detect scene action by comparing successive image-frames for changes. When change is detected that exceeds a predetermined threshold, an alarm is sounded. A guard then judges whether the alarm is false or valid.

VMDs, however, have not turned out to be a security panacea. There are too many sources of image change, especially in outdoor scenes, for a simple circuit to distinguish meaningful intrusions from nuisance alarms: shifting shadows, wind-shaken foliage, birds, rodents, blowing trash or leaves, camera movement, camera auto-iris adjustments, and the like. Faced with frequent false VMD alarms, guards tend to ignore the system altogether. VMD use is therefore restricted to artificially-lighted indoor spaces or to expensive systems that employ computer processing to reduce the false-alarm rate.

In the 1990s and beyond, artificial intelligence techniques—in particular, expert systems—have been combined with VMD to increase the effectiveness of CCTV. An expert system applies higher-level processing to information extracted from the pixels of the raw CCTV image in order to identify and track objects, usually including human intruders. Such systems are a definite improvement over simplistic VMD, and have proven their potential to ignore waving tree-limbs and rabbits hopping over lawns. However, progress remains slow, as in all artificial-intelligence efforts to navigate uncontrolled, complex, real-world situations. A large number of explicit classification rules, for example, must be generated to enable a program to "understand" a given scene—and a scene may change its appearance radically depending on weather (e.g., fog, snowfall, rain), time of day, number and type of cars in the parking lot, and numerous similar factors. It is,

Nikolay Volodiev Dzhonev, center, appears on a television monitor during his closed-curcuit arraignment in 2002 after he was arrested for attempting to board an airplane en route from Atlantic City, New Jersey to Myrtle Beach, South Carolina, with box cutters and a pair of scissors in his backpack. AP/WIDE WORLD PHOTOS.

therefore, difficult to make a PIDS expert system expert enough to be authentically useful. PIDS designers continue to emphasize that there is no near prospect of intelligent CCTV systems outperforming human guards, with all their weaknesses.

Public-surveillance CCTV. Surveillance by police of sidewalks, train stations, courtyards, parking lots, and other public spaces has proliferated rapidly throughout Europe and the United States during the last decade, propelled largely by the increased availability of inexpensive electronics. Many major cities, including Copenhagen, London, New York, and Washington, D.C., now possess public-surveillance CCTV systems, most often operated by police departments. In some cases, images from these systems are being processed using facial recognition systems (also termed biometric systems, from the Greek for "life measurement"). Facial recognition systems are software algorithms that seek to extract telltale facial features from video images and match faces in photographs to those in a database. Public-surveillance systems are thus advertised as serving two basic purposes, deterrence of crime in watched areas and identification of wanted persons.

Such systems have been criticized on several grounds. In Britain, where public-surveillance CCTV has been in use since the 1980s, studies have cast doubt on whether CCTV has any tendency to reduce crime through deterrence. Crime sometimes decreases in monitored areas, but many criminologists argue that this is because criminals simply move their activities elsewhere. Further, facial-recognition software has an extremely low success rate. Several systems, including ones deployed by the city of Tampa, Florida and by the U.S. Immigration and Naturalization Service, have been abandoned within months of deployment due to their zero or near-zero success rates. Police databases have also occasionally been used by individuals with access for illegal purposes (e.g., stalking exspouses, blackmailing), and public-surveillance CCTV systems, like any powerful surveillance tool, are vulnerable to such abuse. Further, system operators, who are usually male, sometimes use CCTV systems to voyeuristically

observe women; a British study found that 1 in 10 women were targeted for voyeurism by the operators of one public-surveillance system. Studies of operators of public-surveillance systems have also shown instances of selectively monitoring dark-skinned persons. Further, powerful surveillance tools may offer a tempting aid to repression of groups such as political protestors. Many aspects of public-space behaviors that are quite legal are nevertheless confidential or at least personal by nature—courtship behaviors, travel patterns, buying habits, lawyer/client consultations, reading choices, smoking, and more. Many persons dislike the idea of such behaviors being recorded by government officials as a matter of course.

There is also widespread willingness in some countries, however, to give up a large measure of privacy in the quest for security from terrorism. A survey conducted by *Business Week* in November, 2001 found that 63% of U.S. adults favored increasing use of public-surveillance CCTV and that 86% favored the use of facial-recognition software to scan for terrorists in public places (as was done with taped images of over 100,000 attendees at the 2001 Superbowl). CCTV, enhanced by computer processing, will probably play a growing role in both its traditional security applications and in public life in years to come.

FURTHER READING:

BOOKS:

Nieto, Marcus, Kimberly Johnston-Dodds, and Charlene Simmons. *Public and Private Applications of Video Surveillance and Biometric Technologies.* Sacramento, CA: California Research Bureau, California Public Library, 2002.

PERIODICALS:

Notton, John. "The Use of Technology in Policing the City of London," in proceedings from the *International Carnahan Conference on Security Technology,* Larry D. Sanson, ed., IEEE, 35–39, 1998.

Sage, Kingsley, and Steward Young. "Computer Vision for Security Applications," in proceedings from the *International Carnahan Conference on Security Technology,* Larry D. Sanson, ed., IEEE, 210–215, 1998.

Thief, Geoff. "Automatic CCTV Surveillance: Towards the VIRTUAL GUARD," in proceedings from the *International Carnahan Conference on Security Technology,* Larry D. Sanson, ed., IEEE, 42–48, 1999.

Walters, Peter. "CCTV Operator Performance and System Design," in proceedings from the *International Carnahan Conference on Security Technology,* Larry D. Sanson, ed., IEEE, 32–37, 1993.

ELECTRONIC:

American Civil Liberties Union (ACLU). "What's Wrong With Public Video Surveillance?" <http://archive.aclu.org/issues/privacy/CCTV_Feature.html> (December 19, 2002).

SEE ALSO

Biological and Biomimetic Systems
Bio-Optic Synthetic Systems (BOSS)
Biosensor Technologies

Coast Guard (USCG), United States

CARYN E. NEUMANN

One of the world's leading maritime security forces, the United States Coast Guard (USCG), maintains public safety in American ports and shipping lanes while also enforcing laws against drug trafficking, environmental abuses, and illegal immigration. Created from a 1915 merger of the Life Saving Service and the Revenue Cutter Service, the Coast Guard is unique among the nation's armed services in that it has two masters. The Coast Guard has historically been attached to the U.S. Navy during times of war, but as of March 1, 2003, the Coast Guard acts under the direction of the Department of Homeland Security (transferred from the Department of Transportation). The USCG plays a major role in homeland security by screening passenger arrivals and conducting inspections at critical domestic ports as well as engaging in patrols of the American coastline.

The Coast Guard traces its origins to a 1790 act of Congress authorizing the construction of vessels to enforce tariff and trade laws, prevent smuggling, and protect the collection of the federal revenue. The Revenue Cutter Service that grew out of this order gradually assumed the additional duties of derelict destruction, protection of game, and enforcement of environmental laws. When the Revenue Cutter Service merged with the Life Saving Service, the newly formed USCG constituted a new branch of the military but a relatively poorly armed one. For most of its existence, the USCG has relied on light weapons that could be brought topside upon need while vessels operating inland generally had only small arms aboard. In war, USCG ships would add mounted guns, but such weaponry has not been deemed necessary for the routine peacetime activities of combating smuggling, assisting ships in distress, and conducting patrols.

The task assigned to the USCG is a daunting one. Over 95% of America's overseas trade moves by sea through 361 ports along 95,000 miles of coastline. It is more economical to bring in drugs and other illegal products in bulk by sea instead of by air, a fact that has prompted numerous traffickers to try their luck at evading the Coast Guard. To combat maritime smuggling, the service designed radar especially for marine traffic surveillance and control in 1972. At first, only operational in the key ports of San Francisco, Houston, Galveston, New Orleans, Puget Sound, and New York, radar is now commonly used, but the chief counter-smuggling activity of the Coast Guard remains the patrol of American waters by

Members of a six-man U.S. Coast Guard law enforcement Tactical Team North, operating from the USS *Typhoon*, approach the tank vessel *Kara Sea*, designated a high interest vessel because of its gasoline cargo, in the Chesapeake Bay in August 2002. AP/WIDE WORLD PHOTOS.

ships and aircraft. In strategic ports, the USCG works closely with the U.S. Navy to protect naval assets. It has developed a methodology to conduct port vulnerability assessments to identify critical infrastructure and is in the process of establishing port security units to be rapidly deployed to provide law enforcement in the event of emergencies such as terrorist attacks.

About half of the USCG's resources are dedicated to public safety, a percentage that has increased in response to the attacks of September 11, 2001. In order to guard against future terrorist assaults, the Coast Guard screens crew and passenger lists obtained through the advance notice of vessel arrival forms that must be completed by all ships. It has developed a maritime homeland security strategy that involves coordinating USCG activities with the intelligence community, U.S. Customs Service, U.S. Navy, Border Patrol, and Immigration and Naturalization Service; sharing maritime intelligence with other nations; and conducting layered maritime security operations with the aim of deterring, disrupting, and intercepting threats before such dangers can reach American shores.

The survival of the Coast Guard seems assured. Congressional assertions that many of the duties of the USCG could be carried out more cheaply by private contractors have ceased as the threat of terrorism increases. Uniquely positioned to continue to provide the maritime component of homeland security, the USCG has decades of experience in detecting and intercepting unwanted intruders without significantly disrupting the transportation system.

FURTHER READING:

BOOKS:

Gottschalk, Jack A. and Brian P. Flanagan. *Jolly Roger with an Uzi: The Rise and Threat of Modern Piracy.* Annapolis: Naval Institute Press, 2000.

Johnson, Robert Erwin. *Guardians of the Sea: History of the United States Coast Guard, 1915 to the Present.* Annapolis: Naval Institute Press, 1987.

PERIODICALS:

Hessman, James D. "The Maritime Dimension; Special Report: The Coast Guard's Role in Homeland Defense." *Sea Power* (Apr 2002), pp. 26–30.

ELECTRONIC:

United States Department of Transportation. "United States Coast Guard." January 27, 2003. <http://www.uscg.mil/USCG.shtm.asp> (January 27, 2003).

SEE ALSO

Coast Guard National Response Center
Crime Prevention, Intelligence Agencies
Customs Service, United States
DEA (Drug Enforcement Administration)
INS (United States Immigration and Naturalization Service)
NMIC (National Maritime Intelligence Center)
September 11 Terrorist Attacks on the United States

Coast Guard National Response Center

JUDSON KNIGHT

The Coast Guard National Response Center (CGNRC) is the sole national point of contact for reports of oil spills, as well as information regarding discharges of chemical, radiological, and biological discharges into the environment. As a unit of the Coast Guard, CGNRC is part of the Department of Transportation (DOT), but due to the significance of its function, it often reports directly to the president of the United States. The increased terrorist threat following the attacks of September 11, 2001, have only served to further its importance as part of the homeland security apparatus.

The federal government advises individuals who observe oil spills, or evidence of oil spills, in or around the United States, to report that information to CGNRC. The latter will dispatch on-scene coordinators to collect data, and will serve as a liaison for the U.S. National Response Team (NRT). However, the responsibilities and purview of CGNRC extend far beyond the functions one normally associates with the Coast Guard. Not only is CGNRC the principal point of contact regarding oil spills, the same is true with regard to chemical, radiological (having to do with nuclear radiation), biological, and etiological (involving disease) hazards as well.

Working with other departments and agencies. CGNRC assists a vast array of government departments, agencies, and administrations in myriad ways. For the Federal Emergency Management Agency, for instance, it acts as a contact point on reports of natural disasters and the evacuations associated with them. The Federal Railroad Administration (FRA) depends on its 24-hour Rail Emergency Hotline, which receives and disseminates information on hazards ranging from railroad accidents to the refusal of railroad employees to undergo drug testing. CGNRC assists the Department of Defense (DoD) by recording transportation incidents or anomalies involving DoD explosives or other sensitive materials, while the Department of the Interior relies on CGNRC to receive reports of incidents involving Trans-Alaskan Pipeline Oil.

In addition to regularly briefing the secretary of Transportation and the chiefs of modal administrations (e.g., the FRA) regarding transportation emergencies, CGNRC also conducts briefings for the White House and the Department of Homeland Security. In the aftermath of the 9–11 terrorist attacks, the federal government has urged civilians witnessing any suspicious activity around rivers and waterways to report this information to CGNRC. According to the New Orleans *Times-Picayune* in November 2002, "Activities that should be reported include unusual filming, hunting or fishing in unusual areas, lights flashing between boats and the shore, ship crew members recovering or tossing things into the water, and divers entering the water near docks or bridges." Numbers for contacting CGNRC are provided at its Web site, listed below.

FURTHER READING:

PERIODICALS:

Darce, Keith. "Port Still Vulnerable, Its Chief Says." *Times-Picayune.* (New Orleans, LA) (November 20, 2002): 1.

Kreuzer, Heidi. "Westchester Incident Highlights Oil Spill Concerns." *Pollution Engineering* 33, no. 1 (January 2001): 9–10.

ELECTRONIC:

Coast Guard National Response Center. <http://www.nrc.uscg.mil/index.htm> (January 22, 2003).

U.S. National Response Team. <http://www.nrt.org/production/nrt/home.nsf> (January 22, 2003).

SEE ALSO

Coast Guard (USCG), United States
Homeland Security, United States Department
National Response Team, United States

Code Name

A code name is a word or phrase used to refer secretly to a specific person, group, project, or plan of action. Individual spies and large-scale military operations are often referred to by code names to protect their identity. For example, the code name for the United States' project to produce an atomic bomb during World War II was "Manhattan Project," the codename for the U.S. plan to invade Okinawa on April 1, 1945 was "Iceberg," the Nazi German plan to invade England had the code name "Operation Sea Lion," and the code name of Spanish double agent Juan Pujol Garcia, who spied for the British while pretending to spy for the Nazis, was "Garbo." So common is the use of code names that an entire book has been devoted to cataloguing the code names used during World War II.

A code name is a particular type of code word. A code word is any word or phrase that has been chosen to signify a specific message while keeping that message hidden from a third party. Functional codes may contain thousands of code words, some of which may also be code names; however, a code name need not be part of a larger code. It may, in effect, be a code unto itself, comprised of only one word.

FURTHER READING:

BOOKS:

Chant, Christopher. *The Encyclopedia of Codenames of World War II.* London: Routledge & Kegan Paul, 1986.

Churchouse, Robert. *Codes and Ciphers.* Cambridge, UK: Cambridge University Press. 2002.

Mollin, Richard A. *An Introduction to Cryptography.* New York: Chapman & Hall 2001.

Singh, Simon. *The Code Book.* New York: Doubleday,1999.

SEE ALSO

Code Word
Codes and Ciphers

Code Word

A code word is a word or phrase that is used to convey a predefined message that differs from its own literal meaning. For example, the code word IRONBOUND might be used to convey the message "meet by the river at midnight." If a number (e.g., 785) is used instead of a word, it is termed a code number. Both code words and code numbers are also termed code groups.

A code is comprised of a list of messages and the code groups that have been defined for them, usually written down in parallel columns in a codebook. To create or interpret messages in a code, one must have access to its codebook. One advantage of a code, as compared to a cipher, is that a single code group may contain a variable amount of information, even within a single code; the code word IRONBOUND, above, conveys a complete command, while another code word might stand either for a single word or for an entire plan of operation. This makes a well-designed code difficult to crack by examining captured messages for patterns.

Word codes, however, also have disadvantages. First and foremost, if a copy of the codebook falls into enemy hands, then the code becomes useless. Second, only ideas for which code words have been predefined can be communicated using a given code. For example, if a code book contains no code word for "noon," it may be impossible to convey the message, "meet by the river at noon." Codes are therefore limited in flexibility by the number of code words that can be fit into a code book of practical size, whereas ciphers can convey almost any written message .

FURTHER READING:

BOOKS:

Mollin, Richard A. *An Introduction to Cryptography.* New York: Chapman & Hall, 2001.

Singh, Simon. *The Code Book.* New York: Doubleday, 1999.

SEE ALSO

Code Name
Codes and Ciphers

Codes and Ciphers

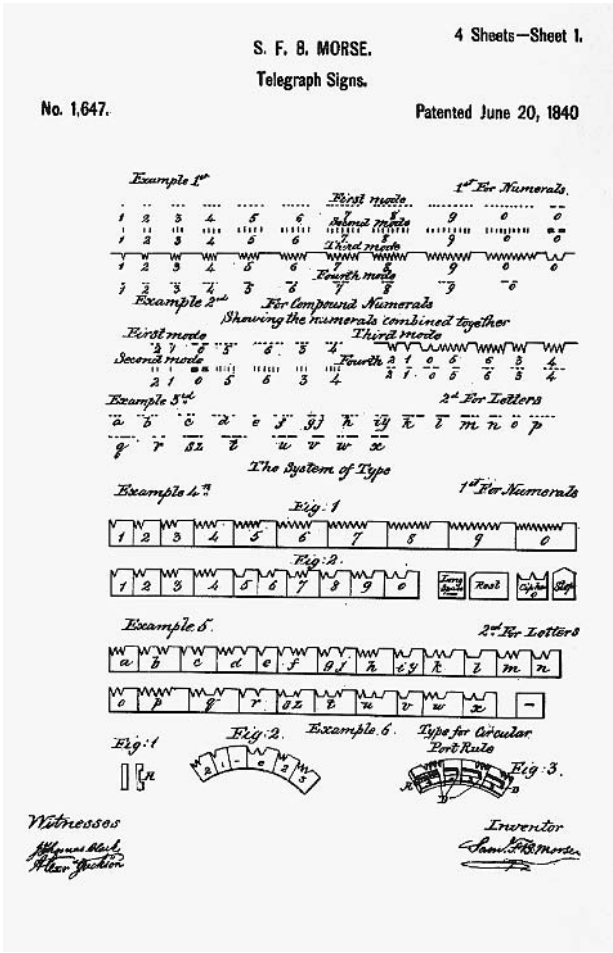
LARRY GILMAN

Codes and ciphers are forms of cryptography, a term from the Greek *kryptos*, hidden, and *graphia*, writing. Both transform legible messages into series of symbols that are intelligible only to specific recipients. Codes do so by substituting arbitrary symbols for meanings listed in a codebook; ciphers do so by performing rule-directed operations directly on original message text. Because codes can only communicate concepts that are listed in their codebooks, they have limited flexibility. Rather, modern cryptography relies almost entirely on ciphers implemented by digital computers, and is widely employed in industry, diplomacy, espionage, warfare, and personal communications.

Codes. A *code* is a set of symbolic strings ("code groups") that are listed, along with their assigned meanings, in a code book.

Codes encrypt messages by substitution, that is, they substitute code groups for components of the original message. "Kill the king at midnight" could thus be encoded, for example, as "OAKEN 7890 SPINDRIFT." Without the code book, it would be difficult for a reader of the encoded message to form an idea of its meaning.

Either a word or a number can be used as a code group. Code groups that are words are termed code words and those that are numbers are termed code numbers. Note that a single code group can encode a single word ("king") or an entire phrase ("deliver the films to agent number 3"). A coded message may, therefore, be shorter than the original message. It can also be made as long as or longer than the original message, if the codebook


S. F. B. MORSE.
Telegraph Signs.
No. 1,647.
4 Sheets—Sheet 1.
Patented June 20, 1840
Witnesses
Inventor

The Morse Code, named for inventor Samuel Morse, was patented in this form in 1840. This code is regarded as one of the great steps forward in international communication. ©BETTMANN/CORBIS.

provides lengthy code phrases for single concepts or nonsense code groups for padding purposes. Such techniques can be used to make encoded messages harder for opponents to read.

Ciphers. A cipher uses a system of fixed rules (an "algorithm") to transform a legible message ("plaintext") into an apparently random string of characters ("ciphertext"). For example, a cipher might be defined by the following rule: "For every letter of plaintext, substitute a two-digit number specifying the plaintext letter's position in the alphabet plus a constant between 1 and 73 that shall be agreed upon in advance." If 46 is the agreed-upon constant, then the plaintext word ZAP enciphers to 724762 as follows:

- Plaintext letter Z = ciphertext 72 (alphabet position 26 + 46).
- Plaintext letter A = ciphertext 47 (alphabet position 1 + 46).
- Plaintext letter P = ciphertext 62 (alphabet position 16 + 46).

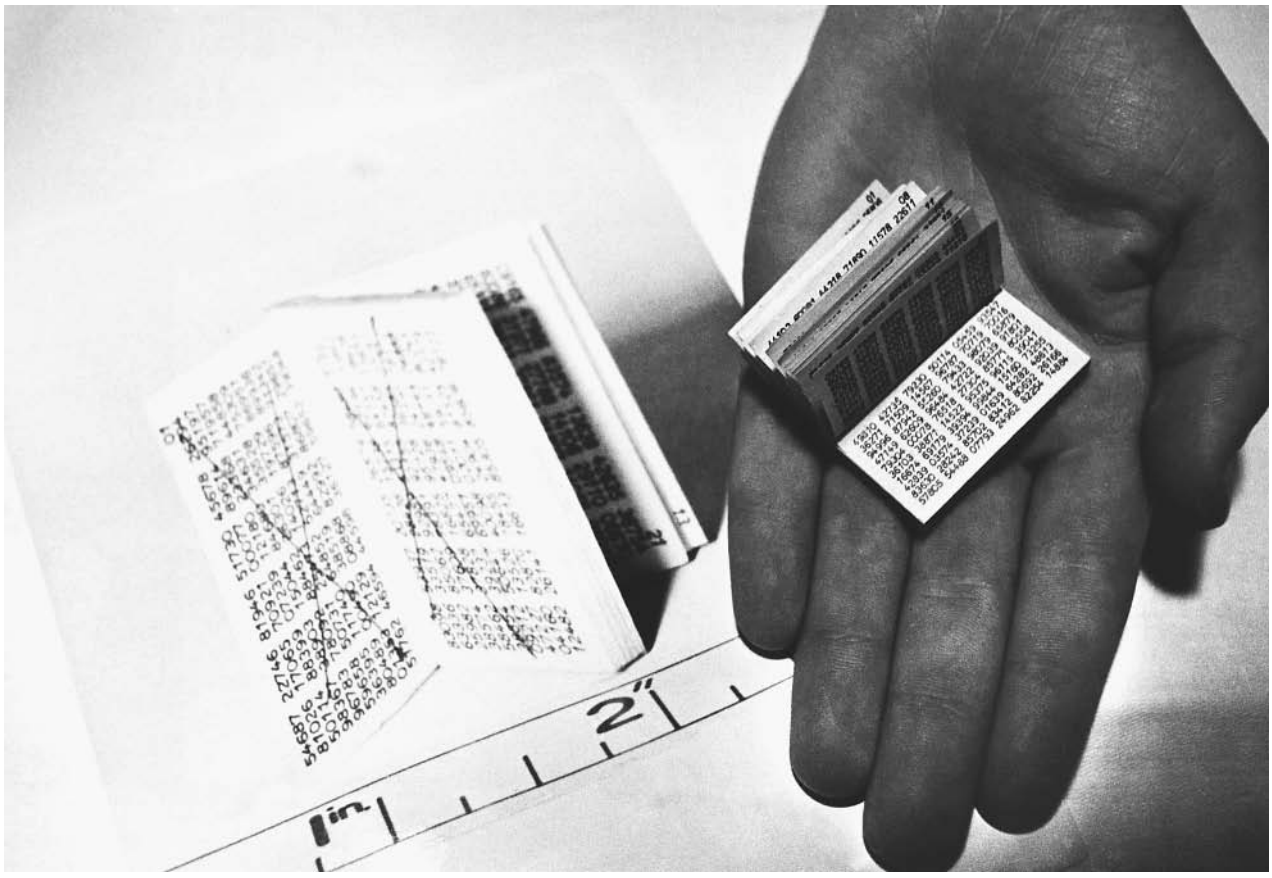
Incorporation of a variable term into a fixed algorithm, as in this example, is typical of real-world ciphers. The variable component is termed a key. A real key would be longer and would have a more complex relationship to the cipher algorithm than the key in this example, but its basic role would be the same: a key fits into an algorithm so as to enable enciphering and deciphering, just as a physical key fits into a lock to enable locking and unlocking. Without a key, a cipher algorithm is missing an essential part. In fact, so important is the concept of the key that in real-world ciphering it is not algorithms that are kept secret, but keys. Cipher designers assume that their algorithms will always become known to their opponents, but design the relationship between key and algorithm so that even knowing the algorithm it is almost impossible to decipher a ciphertext without knowing the appropriate key. Before a cipher can work, therefore, a key or set of keys must be in the possession of both the sender and the receiver.

If the key were always the same, it would simply constitute a permanent part of the algorithm, and keying would have no special advantage over trying to keep one's algorithm secret to begin with. Keys must, therefore, be changed occasionally. A new key may be employed every day, for every message, or on some other schedule.

Comparison of codes and ciphers. Codes have the advantage of simplicity. No calculations are required to encode or decode messages, only lookups in a codebook. Further, because a code uses no fixed system for associating code groups with their meanings (even the amount of meaning assigned to a code word can vary, as seen above), a code may fail gracefully—that is, an enemy may discern the meaning of a few code groups but still be unable to interpret others. In contrast, a cipher produces ciphertext from plaintext (and vice versa) according to a fixed algorithm. Thus, if an enemy determines the algorithm and steals or guesses a key, they can at once interpret all messages sent using that key. Changing the key may restore cipher security, unless the enemy has developed a system for guessing keys. One such system, always possible in theory, is to try all possible keys until one is found that works.

Codes, however, have two great disadvantages. Users can only send messages that can be expressed using the terms defined in the codebook, whereas ciphers can transmit all possible messages. Additionally, all codes are vulnerable to codebook capture. If a codebook is captured, there is no recourse but to distribute new codebooks to all users. In contrast, the key–algorithm concept makes cipher secrecy dependent on small units of information (keys) that can be easily altered.

Secure ciphers, however, entail complex calculations. This made the use of complex ciphers impractical before



A 1968 miniature Kroger's codebook containing a series of numbers that was used by spies to decode messages from Moscow, displayed beside an enlarged photocopy of the text. ©HULTON-DEUTSCH COLLECTION/CORBIS.

the invention of ciphering machines in the early twentieth century; codes and simple ciphers were the only feasible methods of ciphering. Yet, a cipher that is simple to implement is proportionately simple to crack, and a cracked cipher can be disastrous. It is better to have to communicate "in the clear"—to send messages that can be easily read by the enemy—than to suppose that one's communications are secret when they are not. Mary, Queen of Scots (1542–1567) was executed for treason on the basis of deciphered letters that frankly discussed plans for murdering Queen Elizabeth of England; likewise, simple ciphers used by the Confederacy during the U.S. Civil War were easily cracked by Union cryptographers. What is more, even more sophisticated ciphers, such as the Enigma cipher used by Nazi Germany during World War II or implemented today on digital computers, are subject to attack. As soon as any new cipher is invented, someone, somewhere starts attacking it. The result is that ciphers, like some antibiotics, have limited lifespans, and must be regularly replaced.

Historical perspective. Throughout much of the ancient world, writing was either completely unknown or was an arcane art accessible only to priests. There was little motive, therefore, to develop coding or ciphering. Eventually, however, writing came to serve military, personal, and commercial as well as sacred purposes, creating a need for secure communications. To meet this need, ciphers based on scrambling the order of plaintext characters or on substituting other characters for them were developed. The first recorded use of ciphering was by the Greek general Lysander in the fifth century B.C. The *Kama-sutra*, a Hindu text compiled in the A.D. fourth century from manuscripts dating back as far as the fourth century B.C., recommends monoalphabetic substitution ciphering—the replacement of each letter of a plaintext message with a different letter of the alphabet—as one of the 64 arts to be mastered by an ideally-educated woman. By the first century B.C., codes had also been developed.

Cryptography fell out of use during the early Middle Ages, but Arab scholars during the heyday of medieval Muslim civilization, the Abbasid caliphate (A.D. 750–1258), revived it. Muslim writers not only ciphered, but invented *cryptanalysis*, the systematic breaking of ciphers. Ninth-century Arab philosopher Abu Yusuf al-Kindi wrote the earliest known description of the cryptanalytic technique known as frequency analysis, which breaks substitution

ciphers by matching ciphertext letters with plaintext letters according to their frequency of use in the language. In English, for example, the most frequently used letter is E; in an English-language ciphertext produced using a monoalphabetic substitution cipher, therefore, the most frequently used character probably stands for E.

During the late Middle Ages and the Renaissance, a literate ruling class arose throughout Europe, and ciphering regained importance in that part of the world for purposes of intrigue, espionage, and war. English monk and scientist Roger Bacon (1220–1292) wrote a book describing several cryptographic methods; Italian artist Leon Battista Alberti (1404–1472) wrote the first European text on cryptanalysis in 1466. Under pressure from cryptanalysis, codes and cipher systems gradually became more complex.

Beginning in the mid-nineteenth century, the importance of coding and ciphering was rapidly amplified by the invention of electronic information technologies: the telegraph (1837), the telephone (1876), radio (1895), and electronic computers (1940s). Non-secret commercial codes were developed in conjunction with telegraphy to make messages more compact (therefore cheaper); ciphers were widely used (and cracked) during the U.S. Civil War and the first and second world wars. The cracking of German and Japanese ciphers by Allied cryptographers during World War II was of particular importance, enabling the British and Americans to avoid submarines, intercept ships and aircraft, and otherwise frustrate enemy plans. Ciphering has since become basic to military and government communications. Since the 1960s, commercial and personal communications have become increasingly dependent on digital computers, making sophisticated ciphering a practical option for those sectors as well. In the late 1970s, the U.S. government defined a cipher algorithm for standard use by all government departments, available also to the public; this now-elderly algorithm, the Digital Encryption Standard, is today in the process of being replaced by a new algorithm, the Advanced Encryption Standard.

Types of codes. Codes can be generally divided into *one-part* and *two-part* codes. In a one-part code, the same codebook is used for encipherment and decipherment. The problem with this system is that some systematic ordering of the code groups and their assigned meanings must be made, or it will be difficult to locate code groups when enciphering or their meanings when deciphering. (A randomly ordered list of words or numbers thousands of terms long is difficult to search except by computer.) Thus, code groups tend to be arranged in alphabetic or numerical order in a one-part code, an undesirable property, since an opponent seeking to crack the code can exploit the fact that code groups that are numerically or alphabetically close probably encode words or phrases that are alphabetically close. To avoid this weakness, a two-part code employs one codebook for encipherment and another for decipherment. In the encipherment codebook, alphabetically ordered meanings (e.g., A, ABDICATE, ABLE) are assigned randomly ordered code groups (e.g., 6897, 1304, 0045). In the decipherment codebook, the code groups are arranged in order (e.g., 0045, 1304, 6897), for easy location.

Code security can be improved by combining ciphering with coding. In this technique, messages are first encoded and then enciphered; at the receiving end, they are first deciphered and then decoded. A standard method for combining coding and ciphering is the "code plus additive" technique, which employs numbers as code groups and adds a pseudorandom number to each code group to produce a disguised code group. The pseudorandom numbers used for this purpose are generated by modulo-arithmetic techniques closely related to those used in stream ciphering.

Block ciphers. Ciphers that encrypt whole blocks of characters at once—such as 10 letters at a time, or 128 bits—are termed block ciphers. Block ciphers have the advantage that each character in each ciphertext block can be made to depend complexly on all characters of the corresponding message block, thus scrambling or smearing out the message content over many characters of ciphertext. The widely used Digital Encryption Standard (DES) is a block cipher that employs a 56-bit key to encrypt 56-bit blocks. In DES, the key and each message block are used as inputs to a complex algorithm that produces a 56-bit block of ciphertext. The same key is used to decode the block of ciphertext at the receiving end.

Stream ciphers. Stream ciphers operate upon series of binary digits ("bits," usually symbolized as 1s and 0s), enciphering them one by one rather than in blocks of fixed length. In stream encipherment, a series of bits termed the key-stream is made available by some means to both the sender and receiver. This stream is as long as the message to be sent. At the sending end, the key-stream is combined with the message-stream in a bit-by-bit fashion using the exclusive or operation of Boolean algebra, producing the ciphertext. At the receiving end, the same key-stream is combined again with the ciphertext to recover the message stream. This system of ciphering is unbreakable in both theory and practice if the key-stream remains secret. Ongoing breakthroughs in quantum cryptography may soon make perfectly secret key-streams available by exploiting certain properties of photons. If these techniques can be made technologically practical, truly unbreakable cipher systems will have become available for the first time in history.

Public-key ciphers. All ciphers require the use of a secret key. Public-key ciphers, first developed in the late 1970s, are no exception. However, public-key ciphers have the

important advantage that the secret key possessed by the sender need not be the same secret key possessed by the receiver; thus, no secure transfer of keys between the sender and receiver is ever necessary.

Public-key ciphers exploit the computational difficulty of discovering the prime factors of large numbers. (The prime factors of a number are the primes that, when multiplied together, produce the number: e.g., the prime factors of 15 are 5 and 3.) To create a public key, two large (50-digit or longer) primes are chosen and their product calculated. This number (r) is made public. Further mathematical operations by the user produce two numbers based on r; one of these is the user's public key k_p, and the other is retained as the user's private key k_s. Anyone that knows r and a given user's public key k_p can send encrypted messages to that particular user; the recipient decrypts the message using their private key k_s.

Public-key cryptography has seen wide use since the 1970s. Its security is limited by the ability of opponents to determine the prime factors of r, and the difficulty of this task is a function both of the size of r and of the speed of available digital computers. (Large r also makes encryption and decryption more computation-intensive, so it is not practical to defeat opponents by simply making r extremely large.)

Software for a powerful public-key cipher algorithm known as Pretty Good Privacy (PGP) is downloadable for free from many sites on the Internet.

Attacking codes and ciphers. Codes and ciphers can be attacked by two basic means. The first is theft of codebooks or keys—espionage. The second is cryptanalysis, which is any attempt to crack a code or cipher without direct access to keys or codebooks. Cryptanalysis may proceed either by trial and error or by systematic analysis of plaintext and ciphertext. The analytic approach may involve both looking for patterns in ciphertext and solving mathematical equations representing the encryption algorithm.

Cryptanalysis by trial and error usually means guessing cipher keys. A cipher key can be guessed by trying all possible keys using a computer. However, designers of encryption systems are aware of this threat, and are constantly employing larger and larger keys to keep ahead of growing computer speed. Systematic cryptanalysis may seek patterns in ciphertext, either by itself or in conjunction with a known plaintext (the so-called "known-plaintext attack"). Mathematical modeling of cipher algorithms may assist trial-and-error methods by reducing the number of guesses required to within (or near) practical limits. For example, in 2002, cryptographers announced that the recently-standardized Advanced Encryption Standard of the U.S. government might be vulnerable to a mathematical attack that would reduce the number of computations needed for a successful trial-and-error attack from order 2^{256} to order 2^{100}. The latter number is still not computationally practical, but may be soon.

Quantum cryptography holds out the promise of truly attack-proof ciphering. In a quantum-cryptographic system, not only would messages be undecipherable if intercepted, but also the act of interception would always be detectable by the intended receiver. Such systems may become available to military and government users around 2010.

FURTHER READING:

BOOKS:

Charthouse, Robert. *Codes and Ciphers.* Cambridge, UK: Cambridge University Press, 2002.

Meyer, Carl H., and Stephen M. Matyas. *Cryptography: A New Dimension in Computer Data Security.* New York: John Wiley & Sons, 1982.

Mollin, Richard A. *An Introduction to Cryptography.* New York: Chapman & Hall, 2001.

Singh, Simon. *The Code Book.* New York: Doubleday, 1999.

Stinson, Douglas R. *Cryptography: Theory and Practice.* New York: Chapman & Hall, 2002.

PERIODICALS:

Seife, Charles. "Crucial Cipher Flawed, Cryptographers Claim." *Science* no. 5590 (2002): 2193.

SEE ALSO

ADFGX Cipher
Cipher Disk
Cipher Key
Cipher Machines
Code Name
ENIGMA
FISH (German Geheimschreiber *Cipher Machine)*
French Underground During World War II, Communication and Codes
Playfair Cipher
World War I: Loss of the German Codebook
World War II, United States Breaking of Japanese Naval Codes

Codes, Fast and Scalable Scientific Computation

A code is a system for concealing a message by replacing words or phrases with symbols. Codes are used on computers for a number of purposes relevant to espionage and security, among them the development of large-scale scientific simulations. For this to be possible, it is necessary to develop algorithms, or mathematical processes,

that are easily scalable, or adjustable, such that computation time does not increase exponentially.

There are numerous situations for which a computer simulation is preferable to a real-life demonstration, an extreme example being a study of radiation diffusion following a nuclear blast. Performing such a study requires a computer simulation, or a program that emulates and measures the effects of a real-life process. These problems are so complex that they require parallel processing, or the use of two or more computers working in tandem, as well as the development of scalable algorithms.

An algorithm is a method for solving a mathematical problem by using a finite number of computations, usually involving repetition of certain operations or steps. A scalable algorithm is one that is capable of implementing additional computational resources in such a way as to solve increasingly more complex problems. To be truly scalable, the work required to solve an algorithm should grow at a rate smaller than the rate at which the amount of input grows.

FURTHER READING:

ELECTRONIC:

Fast and Scalable Scientific Computation. Defense Advanced Research Projects Authority. <http://www.arpa.mil/dso/thrust/am/faca_1.htm> (January 27, 2003).

Scalable Linear Solvers. Lawrence Livermore National Laboratory. <http://www.llnl.gov/CASC/sc2001_fliers/SLS/SLS01.html> (January 27, 2003).

SEE ALSO

Computer Modeling
Lawrence Livermore National Laboratory (LLNL)
Supercomputers

COINTELPRO

LARRY GILMAN

COINTELPRO (for Counter Intelligence Program) was a set of programs commenced by the United States Federal Bureau of Investigation (FBI) in 1956 and officially terminated in 1971. COINTELPRO included programs variously named Espionage COINTELPRO; New Left COINTELPRO; Disruption of White Hate Groups (targeting the Ku Klux Klan); Communist Party, USA COINTELPRO; Black Extremists COINTELPRO; and the Socialist Workers' Party Disruption Program. Although these were "counterintelligence" programs by name, the FBI did not consider most of these groups to be engaged in intelligence activities (e.g., spying for the Soviet Union). Rather, it deemed their political activities dangerous, and assumed that various court decisions had made it impossible to control them by nonsecret, legal means (e.g., arrests for illegal acts). COINTELPRO began by targeting the Communist Party, but quickly expanded to include other groups. The FBI's "black extremist" category included not only the Black Panthers but the Southern Christian Leadership Conference and its president, Martin Luther King, Jr., the Student Nonviolent Coordinating Committee, and other civil rights groups of the 1950s and 1960s. COINTELPRO also targeted groups opposed to the Vietnam War.

COINTELPRO remained secret until a large number of documents were stolen from the FBI office in the town of Media, Pennsylvania, in 1971. Lawsuits brought by political groups who believed that they were being observed and disrupted by the FBI soon produced other COINTELPRO-related documents. In 1975, a Senate committee—the Select Committee to Study Governmental Relations with Respect to Intelligence Activities, better known as the Church Committee after its chair, Senator Frank Church (D, Idaho)—was appointed to investigate COINTELPRO and other domestic espionage and disruption programs conducted by the FBI, the Central Intelligence Agency, the National Security Agency, Army intelligence, and the Internal Revenue Service. The Church Committee concluded in 1976 that "the domestic activities of the intelligence community at times violated specific statutory prohibitions and infringed the constitutional rights of American citizens," and stated that the FBI had gathered information by illegal means, disseminated that information illegally, and otherwise violated the law in its efforts to disrupt political activities that it considered subversive. The committee's report stated that "the abusive techniques used by the FBI in COINTELPRO from 1956 to 1971 included violations of both federal and state statutes prohibiting mail fraud, wire fraud, incitement to violence, sending obscene material through the mail, and extortion. More fundamentally, the harassment of innocent citizens engaged in lawful forms of political expression did serious injury to the First Amendment guarantee of freedom of speech and the right of the people to assemble peaceably and to petition the government for a redress of grievances."

Disruption techniques used by the FBI during COINTELPRO, according to the findings of the Church Committee, included burglaries; illegal opening and photographing of first-class mail; planting of forged documents to make it appear that individuals were government informants; anonymous letters to spouses, designed to break up marriages; secretly communicating with employers in order to get individuals fired; planting of news articles and editorials (covertly authored by FBI agents) in U.S. magazines and newspapers; anonymous letters containing false statements designed to encourage violence between street gangs and the Black Panthers; anonymous letters denouncing Catholic priests who allowed their churches to be used for Black Panther breakfasts sent to their bishops; requests for selective tax audits; encouragement of violent tactics by paid FBI informants posing as

members of antiwar groups in order to discredit those groups; and others.

■ FURTHER READING:

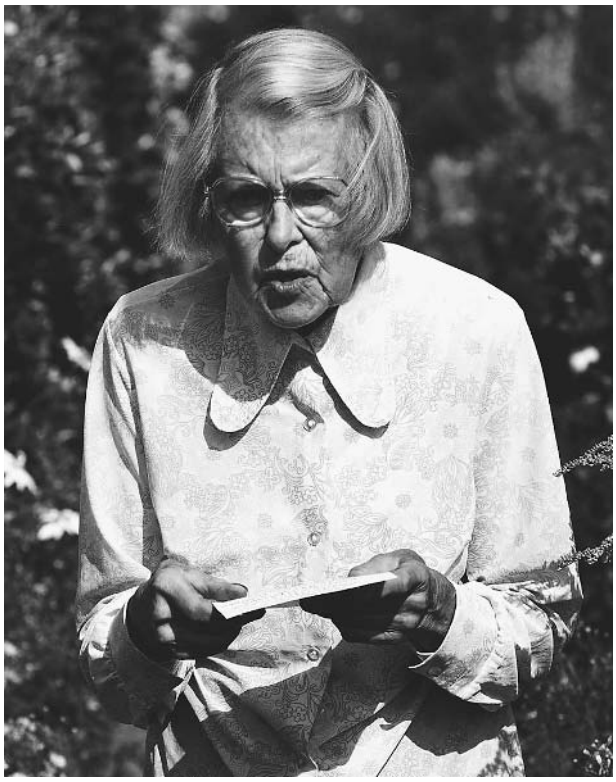
ELECTRONIC:

"Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities." United States Senate. April 26, 1976. <http://www.derechos.net/paulwolf/cointelpro> (March 18, 2003).

Cold War (1945–1950), The Start of the Atomic Age

■ SIMON WENDT

The Cold War was an ideological, political, economic, and military conflict between the United States and the Union of Soviet Socialist Republics (U.S.S.R.), which began in the aftermath of World War II and ended in 1989. From the outset, the Cold War was inextricably linked with the development of the atomic bomb and its use as a military deterrent.



Melita Norwood, an 87-year-old great-grandmother, reads a statement outside her London home after being unmasked as one of the Soviet Union's top Cold War spies who passed atomic secrets to Moscow, giving the Soviet Union a vital edge in the arms race. ©REUTERS NEWMEDIA INC./CORBIS.

Roots of the Cold War. The enmity between the United States and Russia, the largest of the fifteen republics that ultimately constituted the U.S.S.R., stemmed from a long history of mutual distrust. Opposing plans concerning the political and economic future of post-World War II Europe and disputes concerning the development and control of atomic weapons intensified the conflict. The seeds of antagonism date back to 1917. That year, the United States dispatched a contingent of soldiers to assist European allies in overthrowing Russia's new communist regime, which had come to power during the Russian Revolution. Despite the operation's failure, the U.S. government continued to deny the new Soviet Union diplomatic recognition until 1933. After a brief period of cooperation, Russian leaders' suspicions toward America began anew at the dawn of World War II. They considered Western nations' initial refusal to oppose Nazi Germany and Japan with arms part of a capitalist scheme to destroy the U.S.S.R. Americans, on the other hand, assumed that the brutal regime of Soviet dictator Joseph Stalin (1879–1953) was only slightly better than that of Germany's leader Adolph Hitler (1889–1945).

During World War II, Stalin's doubts about the sincerity of American vows to support the Soviet war effort intensified. Soon after the beginning of the war in 1939, the Soviet Union bore the brunt of military action, attempting to fend off a massive German invasion. Although American President Franklin D. Roosevelt (1882–1945) promised the Soviet leader substantial economic aid, the United States managed to provide relatively few supplies. More important, Roosevelt assured Stalin in 1942 that American troops would relieve some of the military pressure on Russia by establishing a second front in Western Europe. However, logistical and production problems postponed an allied invasion for several years. When allied forces finally landed on Europe's shores on June 6, 1944, Roosevelt had reneged on his promise three times. This delay burdened post-World War II U.S.-Soviet relations considerably.

Even before Germany's surrender on May 9, 1945, additional disputes arose over the future of liberated Europe. The United States envisioned democratic and freely elected societies based on the right of self-determination and free trade. By contrast, the Soviet Union sought territorial expansion and spheres of influence that would guarantee the country's national security. Accordingly, during and after the war, Stalin insisted on establishing Eastern European governments supportive of the Soviet Union. He considered countries such as Poland, Bulgaria, and Romania part of an essential buffer zone to prevent future

attacks on the territory of the U.S.S.R. However, this demand was the exact opposite of President Roosevelt's vision of self-determination. These disagreements were aggravated by the U.S. government's decision to provide economic aid with the stipulation that Stalin revoke his adamant stance on the territorial question.

Beginning of the Atomic Age. The atomic bomb became the final divisive issue, contributing to the ultimate breakdown of U.S.-Soviet relations. In late 1938, German physicists had discovered that uranium atoms undergo fission when bombarded by neutrons. They found that this fission triggered a self-sustaining atomic reaction that could release enormous amounts of energy. Their discovery had significant potential for the development of a powerful new weapon. In 1939, a group of European émigré scientists in the United States verified the possibility of a nuclear chain reaction. The group's leader, Hungarian physicist Leo Szilard (1898–1964), worried that Nazi Germany might use this knowledge to develop an atomic bomb. In August 1939, Szillard asked famous physicist Albert Einstein (1879–1955) to sign a warning letter to President Roosevelt to convince him of the necessity to forestall German scientists. But only in early 1942 did the U.S. government finally launch an official research project to develop the new weapon.

In what the United States Army code-named Manhattan Engineer District (later dubbed Manhattan Project) scientific director J. Robert Oppenheimer (1904–1967) assembled a team of American and British scientists and engineers who developed two weapon designs. One relied on the rare Uranium-235. The other, more complicated, design used man-made Plutonium-239, which was produced in nuclear reactors that University of Chicago physicist Enrico Fermi (1901–1954) had invented in 1942. By 1944, three large reactors produced uranium and plutonium for the first American bombs. On July 16, 1945, Manhattan Project scientists tested the Plutonium weapon near Alamogordo, New Mexico, setting off the world's first nuclear explosion.

The decision by President Roosevelt's successor Harry S. Truman (1884–1972) to use atomic bombs in the military conflict with Japan proved the destructive power of nuclear weapons to the world. On August 6, 1945, a B-29 aircraft dropped a Uranium bomb over Hiroshima, Japan, obliterating the city and instantly killing 100,000 civilians. Three days later, a Plutonium bomb killed another 30,000 Japanese citizens at Nagasaki. On August 14, 1945, Japan finally surrendered. Thus, the last chapter of World War II marked the beginning of the atomic age.

The nuclear attack on Japan and the secrecy that surrounded the development of the bomb increased the tensions between the United States and the U.S.S.R. Neither President Roosevelt nor Truman was willing to share information on the bomb with the Soviets. American scientists' appeals to inform Stalin of the new research were ignored. Rather, President Truman sought to use his country's atomic monopoly as leverage in the worsening conflict. Soviet scientists had already learned of the Manhattan Project during World War II through espionage, however, and were now coordinating their own research project on nuclear weapons. They used detailed plans that Soviet spies had supplied them. German-born physicist Klaus Fuchs (1911–1988) in particular provided crucial intelligence that facilitated the acquisition of the atomic bomb by the Soviet Union. As early as 1941, when working on Great Britain's nuclear program, Fuchs began to relay classified information to Russia. Later working on the Manhattan Project, he provided Soviet scientists with facts on virtually every aspect of the project's research. When the U.S.S.R. finally tested its own atom bomb on August 29, 1949, Stalin's scientists detonated a near-perfect replica of the American Plutonium weapon.

During the period between the first nuclear explosion in New Mexico and the end of America's atomic monopoly, a series of divisive events and decisions gradually established the fronts of the Cold War. The year 1946 saw increasingly belligerent language on both sides. Joseph Stalin proclaimed in early February that a new war was inevitable as long as capitalism existed. That same month, Moscow-based foreign-service officer George Kennan suggested in a secret telegram to Washington that the Soviet Union sought to expand its influence and planned to defeat its Western rivals. He argued that only long-term attentive containment of these expansive tendencies would avert disaster. Echoing Kennan's concerns in March, British Prime Minister Winston Churchill (1874–1965) warned of an "iron curtain," with which the U.S.S.R. would shackle Eastern Europe. Churchill also argued that the West needed to resist Communist expansion. Later that year, the Soviet Union provoked a major crisis when it continued to occupy Iran despite an agreement with Great Britain to leave the country after six months of post-war occupation. Threatened with military confrontation, Soviet troops eventually withdrew, but the Iran crisis further strained U.S.-Soviet relations.

The debate on the international control of atomic energy clearly reflected the increasing animosity between the two nations. The final U.S. plan that the administration's representative Bernard Baruch (1870–1965) presented to the United Nations on June 14, 1946, proposed to create an international agency that would supervise the mining of uranium and the manufacture of plutonium. Baruch's scheme encouraged nations to conduct research on the atom's peaceful use, but insisted on the American atomic monopoly. The Soviet Union rejected the plan. When U.S. scientists conducted a new series of nuclear weapon tests at the Bikini Atoll in the South Pacific in the summer of 1946, Stalin denounced it as proof of America's insincerity about international control.

In 1947, President Truman demonstrated that the Cold War already dominated American foreign policy. Early that year, concerns increased that Greece and Turkey might soon come under communist domination. In

what came to be known as the Truman Doctrine, the American president asked Congress on March 12, 1947, to authorize economic and military aid for the two nations to prevent a communist take-over. According to Truman, this was a litmus test of the willingness of the United States to stop the spread of communism everywhere in the world. Couching the conflict in ideological and moral terms, Truman proclaimed that people would have to choose between the alternatives of communist tyranny and democratic freedom. After Truman's impassioned speech, the requested aid package passed Congress easily. The Truman Doctrine prompted most Americans to view the conflict with the U.S.S.R. as a primarily ideological struggle between binary opposites of good and evil.

United States national security policy during the Truman administration revolved, however, around more than ideology. In the eyes of Washington's policy makers, American predominance depended on power, which they defined as the control of resources, industrial infrastructure, and strategic superiority. The National Security Council (NSC) and the Central Intelligence Agency (CIA), created by the National Security Act of 1947, used the same criteria when assessing potential Communist threats and American vital interests. The NSC served as a crucial strategic planning body for security policy. The CIA continued the espionage work of the wartime Office of Strategic Services (OSS). In 1950, a planning document drafted by the NSC, NSC-68, predicted an indefinite period of conflict with the Soviet Union, calling for a vast American military buildup. In the ensuing years, NSC-68 became the basis for American Cold War strategy.

Ideological premises and geostrategic security concerns were inextricably linked with American economic interests. Becoming one the most important initiatives of the early Cold War, the Marshall Plan of 1947 served these economic interests and finalized the division of the world into two hostile camps. Drawn up by secretary of state George Marshall (1880–1959), the plan launched a massive economic aid package for the reconstruction of Western Europe. Healthy capitalist economies, Marshall argued, would provide American companies with new markets and could help weld European nations into an effective bulwark against Communism.

Although the United States invited the Soviet Union and Eastern European countries to apply for economic aid as well, negotiations soon demonstrated that Stalin would never accept the American plan. In fact, the Marshall Plan would not only allow the United States to control the distribution of aid, but would also give them access to the Soviet Union's economic records. Predictably, Stalin withdrew from the negotiations and countered the American economic aid project with the Molotov Plan, a series of bilateral trade agreements with Eastern European countries. The Soviet plan transformed these countries into a Communist counter alliance against the West.

In another confrontation, Stalin attempted to force the United States, Great Britain, and France to revoke their decision to unify their three occupation zones in Germany. On July 23, 1948, the Soviet dictator initiated a year-long blockade of all supplies to the city of Berlin in the Russian zone. The United States responded with a well-organized air lift, which supplied the encircled city for almost one year. In the end, the air lift forced Stalin to give up the blockade. By that time, however, the Soviet Union already dominated Eastern Europe. In February, 1948, Czech and Slovak communists had toppled Czechoslovakia's democratic government and established a pro-Soviet Communist regime, adding the country to the Soviet bloc. In Hungary, Stalin also had imposed Communist rule. When the western part of Germany constituted itself as the Federal Republic of Germany in spring of 1949, the U.S.S.R. initiated the permanent division of the country by establishing the German Democratic Republic in the former Russian occupation zone. On April 4, 1949, the United States, Canada, and ten Western European nations had reacted to Soviet hostilities forming the North Atlantic Treaty Organization (NATO), a military alliance designed to protect its members against a potential Soviet attack.

Thus, by 1950, the framework of the Cold War was firmly in place, prompting both sides to enhance their military capabilities, in particular their nuclear arsenal. By the beginning of the new decade, the United States had amassed three hundred nuclear weapons. However, since the American administration had learned in early September, 1949, that the Soviet Union had successfully tested an atomic bomb, American policy makers considered that the strategic superiority of the United States might be in jeopardy. As a result, President Truman ordered American scientists to develop a weapon that was even more powerful: the hydrogen bomb. By the mid-1950s, both nations had developed and tested this new weapon, marking the beginning of a new round of Cold War confrontations.

FURTHER READING:

BOOKS:

Carlisle, Rodney P., with Joan M. Zenzen. *Supplying the Nuclear Arsenal: American Production Reactors, 1942–1992.* Baltimore: John Hopkins University Press, 1996.

Gaddis, John L. *The United States and the Origins of the Cold War.* rev. ed. New York: Columbia University Press, 2000.

———. *We Now Know: Rethinking Cold War History.* New York: Oxford University Press, 1997.

Herken, Gregg. *Cardinal Choices: Presidential Science Advising from the Atom Bomb to SDI.* rev. and exp. ed. Stanford, CA: Stanford University Press 2000.

Holloway, David. *Stalin and the Bomb: The Soviet Union and Atomic Energy, 1939–1954.* New Haven, CT.: Yale University Press, 1994.

Leffler, Melvyn P. *A Preponderance of Power: National Security, the Truman Administration, and the Cold War.* Stanford, CA: Stanford University Press, 1992.

Roleff, Tamara. ed. *The Atom Bomb.* San Diego, CA: Greenhaven Press, 2000.

SEE ALSO

Berlin Airlift
CIA (United States Central Intelligence Agency)
National Security Act (1947)
NATO (North Atlantic Treaty Organization)
NSC (National Security Council)
Nuclear Reactors
OSS (United States Office of Strategic Services)
Truman Administration (1945–1953), United States National Security Policy
United States, Intelligence and Security

Cold War (1950–1972)

CHRISTOPHER T. FISHER

The Cold War, a contest between antithetical ideologies, democratic capitalism and Soviet socialism, emerged shortly after World War II and dominated global politics for the latter half of the twentieth century. Its origins, however, go back to the late nineteenth century when the United States decried Russia's colonial claims on the Manchurian region of China. In the early twentieth century, opposition stiffened further over Russia's brutal pogroms against its Jewish citizens. The Bolshevik cooptation of the peasant revolution against the Russian Czar in 1917, and their subsequent creation of the Soviet state, heightened mutual suspicion and opened the gulf between Russia and the West. World War II brought a temporary reprieve in animosities, but tensions reemerged over questions concerning the postwar world. President Harry Truman, successor to Franklin Delano Roosevelt, launched the first blow in the Cold War by insisting that Russia honor its prewar commitment to self-determination under the Atlantic Charter, and permit a democratic government in Poland. Soviet leader Joseph Stalin steadfastly refused any concession, and the Polish issue became the first beachhead in Cold War politics. The Polish crisis alarmed American leaders who interpreted it as confirmation that Russia intended to carry the Bolshevik revolution westward.

The thaw caused great anxiety in the United States as it turned to the Pacific theater and planned the settlement of Germany. Each situation loomed ominously with the prospect of an entrenched Soviet presence clouding negotiations. These fears compelled Truman to end the Japanese campaign as swiftly as possible. The administration made the decision to deploy the world's first atomic bomb with both the unyielding Japanese and intransigent Russians in mind.

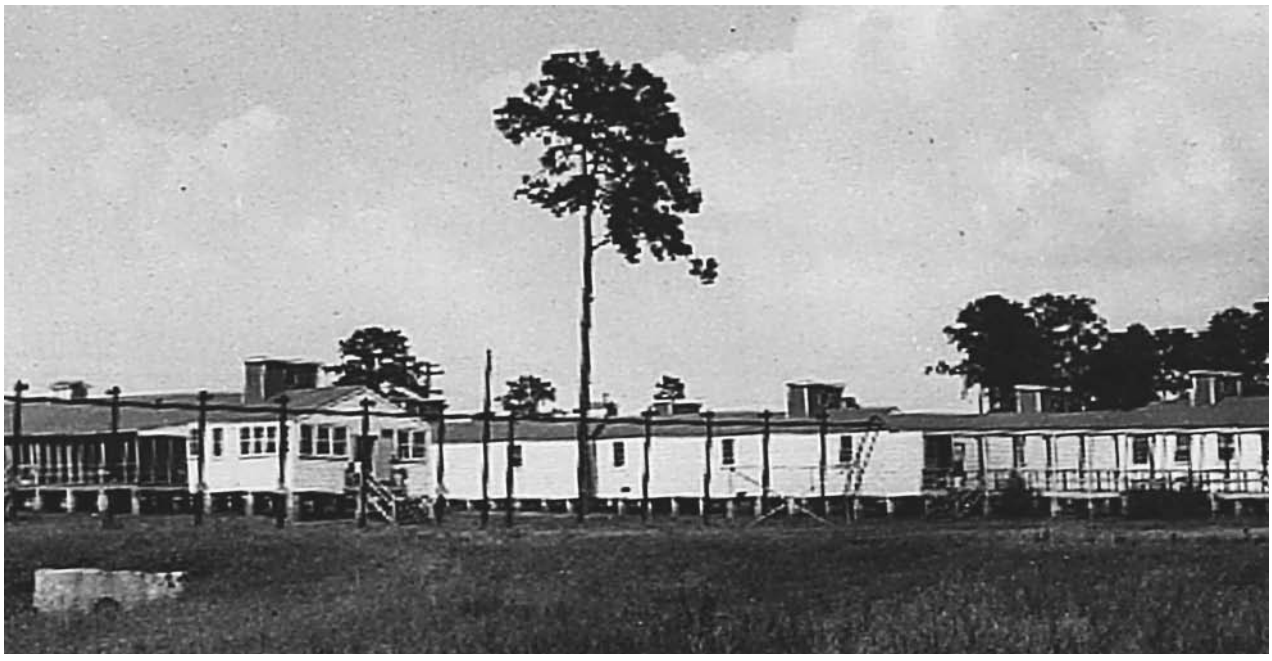
Once the Japanese surrendered in the summer of 1945, the Cold War began in earnest. In almost rapid succession, the threat of Communist infiltration troubled Truman. The war left many nations, particularly those in the Third World, vulnerable to Communist influence. Additionally, a few countries, most notably China, erupted in civil war between Capitalist and Communist factions at the close of World War II. The loss of China's vast natural resources, unlimited commercial potential, and immense population concerned American policymakers, who had supported the ultra-nationalist Chiang Kai Shek from the conflict's inception. To Truman's dismay, Communist leader Mao Tse Tung's made significant strides in battles as early as 1946 and gained the upper hand permanently, forcing Chiang off the mainland to the neighboring island of Taiwan, in 1949.

Simultaneous to the Chinese civil war were political fluctuations in the Middle East. The Soviet schemes on making Iran, Turkey, and Greece strategic footholds in the Mediterranean compelled Truman to take a tough stance. In 1946, America funneled well over $600 million in appropriations to democratic forces battling the Communist led and funded National Liberation Front in Greece for control in the upcoming national elections. While in Iran and Turkey, Truman met Soviet incursions through the newly formed United Nations and with the threat of American military reprisal.

George F. Kennan, charge d'affaires in Russia, provided a rationalization for the events of 1946 in his alarm driven 8000 word dispatch from Moscow on the Soviet postwar intentions. Providing the first part in what became the intellectual mooring of the Cold War, his long telegram depicted Russia as irretrievably expansionist and guided by messianic ideology that the United States to resist. Truman read the events in the Mediterranean through Kennan's lens and assumed it justified a spirited response, even though Truman had made no official declaration of a "cold war" to this point. Stalin and Churchill had already made their Cold War declarations early in 1946, ruman rendered his own salvo in March 1947.

The Truman Doctrine argued that the world's future was split between totalitarianism and democracy. To preserve the American way of life, they would have to respond to Communist-inspired uprisings anywhere in the world. Funding the democratic forces in Greece was the first manifestation of this task; next, Truman requested a larger economic stimulus program for Western Europe that might rescue them from Communist subversion. His request became the European Recovery Program, or Marshall Plan, which the administration intended to supplement with the International Monetary Fund and the World Bank created at the Bretton Woods Conference of 1944. Next, Truman created the North Atlantic Treaty Organization (NATO), a vast military alliance premised upon multilateral response to Communist attack. The Marshall Plan and NATO gave Truman the tools for fighting the Cold War and promoting democratic capitalism in the Third World.

At home, Truman's anticommunist rhetoric energized a Republican Party resurgence. Midterm elections of 1946 ushered a new class of hawkish congressmen, the most notable were Wisconsin Senator Joseph McCarthy and



Training Center One, a secret CIA guerrilla warfare training base at Ft. Benning, Georgia, in 1951, where some menbers of the Air Supply and Comminucation Service (ARC) trained before going overseas. China had discovered that the newly created Central Intelligence Agency and the Air Force were collaborating on a new Cold War weapon, an "unconventional warfare" group whose connection to the CIA remains an official government secret. AP/WIDE WORLD PHOTOS.

California Congressman Richard M. Nixon, who defined themselves as Cold War activists. Republicans accused the Democratic Party with compromising America's postwar ambitions, giving Russia advantage in Western Europe. The capture of Russian spy of Klaus Fuchs in Great Britain, and then American counterparts Ethel and Julius Rosenberg, convicted for selling atomic secrets to the Soviet Union, along with the Alger Hiss case, validated Republican claims for many. Further proof came with the Soviet detonation of a nuclear device in 1949, and victory of Mao Tse Tung in China.

George Kennan again proved a useful guide for Truman with his *Foreign Affairs* article published July 1947 under the pseudonym Mister X. In the X Article, titled "The Sources of Soviet Conduct," Kennan warned that Russia operated on a mechanistic and fanatical faith that America had to meet wherever possible. The Soviet system, he advised, suffered from internal contradictions that would destroy it from within if given exposure. Truman and his secretary of state, Dean Acheson, interpreted Kennan's argument as "containment" and constructed the domestic tools for its execution. That July, Truman presented Congress with the National Security Act, which restructured the military establishment creating the Department of Defense, the National Security Council, and the CIA. Soon thereafter, he created loyalty policies aimed at rooting out Communists in the government.

The preemptory steps were not enough to meet the myriad strategic and political crises of the Cold War; therefore the administration attempted to streamline America's response even more with the creation of National Security Council Memorandum (NSC) 68. As the top-secret blueprint for fighting the Cold War, NSC 68 called for a massive increase in military appropriations, the creation of the enormously more powerful hydrogen bomb, and levying taxes on the American public to pay for the program. Congress was reluctant to appropriate the sums of money needed for the Cold War, so Truman needed a dramatic event to shake them from their parochialism. That event came when North Korea, a Communist nation, crossed 38th parallel and invaded its democratic counterpart South Korea on June 24, 1950.

The Korean conflict proved to be a double-edged sword for Truman; it provided him the public mandate to institutionalize the Cold War, but it also laid the seeds for the political undoing of the Democratic Party. The battle itself swung unevenly, with the North Koreans at first advancing southward, and then United Nations forces led by General Douglass MacArthur recapturing ground. The turning point in the conflict occurred when a "volunteer" force from China crossed the river separating Korea and China, and sent MacArthur's forces into retreat. The Chinese attack threatened war, but Truman decided to quell to situation for the sake of American lives and global peace. His decision placed him at odds with MacArthur, which resulted in a war of words that ended with Truman unceremoniously removing the general from his command.

The Korean War, however, justified NSC 68 and a stronger stance in East Asia. Aside from the decision to support the South Koreans financially and militarily, Truman used it as a vehicle for funding the French colonial

An electromagnetic separation facility in Sverdlovsk, Russia, used for uranium enrichment, is shown in an undated high-altitude photograph taken during the Cold War. Many of the spy photos made of the Soviet Union taken in the urgent context of the Cold War now aid in peaceful purposes, such as disarmament verification. AP/WIDE WORLD PHOTOS.

war against the Vietnamese. Additionally, he created a military alliance for East Asia, the Australia, New Zealand, and United States (ANZUS) pact, and began rearming Germany as a buffer to Soviet advances west.

Domestic politics could not escape the gravitational pull of the Cold War, and its questions particularly burdened the presidential election of 1952. Red-baiters in the Republican Party, most notably Wisconsin Senator Joseph McCarthy, created such a relentless and fantastic attack on Truman's handling that it implicated the entire Democratic Party. The Republican candidate, Dwight Eisenhower (referred to as Ike), stayed above the fray, and allowed his reputation as the great general of World War II's European theater to win him the White House. Eisenhower took a pragmatic approach to the Cold War, and established the tradition that would remain in place until its end.

The death of Soviet Premier Joseph Stalin in March 1953 cast a shroud of uncertainty over Eisenhower's first year as president. Undeterred, however, he began defusing the anxious economy and international policies that dominated Truman's administration, with his "New Look" program. The New Look consisted of nuclear deterrence, designated by what his secretary of state John Foster Dulles called brinksmanship, massive relation, nation building in the Third World, the diffusion of American culture internationally, and a heavy investment in technological innovation. Eisenhower detested wasteful spending and thought a combination of brinksmanship, technological innovation, and massive retaliation would streamline the military, yet preserve the nation's ability to respond quickly to crisis. Eisenhower gauged success in the Cold War effort broadly, thereby making the household washing machine as important in the Cold War arsenal as the B-52. In 1959, this correlation sparked the famous "kitchen debate" between Vice President Richard Nixon and Soviet Premier Nikita Khrushchev at the American National Exhibition in Moscow over which political economy promoted the better home life. As Eisenhower eschewed Truman's containment program for a policy of rolling back Communist expansion, reducing the size of conventional forces meant that the administration had to rely on the CIA to keep order in the Third World through counterintelligence and espionage.

International crises in Iran, Guatemala, and off the coast of mainland China tested Eisenhower's New Look early in his administration. Nationalist leaders in Iran and Guatemala assumed power in an attempt to redress grave social and economic inequalities in their countries, forcing the United States to respond. Although the Cold War implications were not necessarily apparent, America gained access to one of the world's largest oil depository by returning the Shah of Iran to power, and defeating the Arbenz regime guaranteed American businesses open access to the resources of Guatemala. The marriage of

U.S. Army tanks at Checkpoint Charlie, foreground, face Soviet Army tanks in 1961 during the most dangerous of several crises at the Friedrichstrasse checkpoint in Berlin during the Cold War. AP/WIDE WORLD PHOTOS.

Cold War politics and market concerns became a signature attribute of the New Look.

The Tachen Straits crisis presented a different problem. In 1954, mainland China began shelling two of the islands that neighbored Chiang Kai-Shek's Taiwan, Matsu and Quemoy with the threat that it was the start of a full-scale invasion to repatriate it citizens. To the surprise of the entire world, Eisenhower threatened the use of nuclear weapons to defend Taiwan unless China stopped the bombardment. Frightened by the possibility of nuclear calamity, neighboring countries India and Pakistan pressured China to desist, and the Tachen Straits crisis came to an uneasy end. The conflict, however, was a coarse example of brinksmanship and a precursor to America's deepening involvement in East Asia under the auspices of the "domino theory" of foreign policy. The image of Asian democracies, falling like dominos in rapid succession to nationalist or Communist infiltration, justified a greater presence in conflict between France and Vietnam.

Vietnam became a crisis for the United States at the Geneva Conference of 1954, when it was learned the French were on the verge of collapse in the region, signified by their surrender at Dienbienphu. To preserve democracy in Southeast Asia, the United States urged the division of Vietnam at the 17th parallel on the promise the country would have open elections within two years. In an attempt to thwart a potential Communist takeover in the upcoming elections, America installed Ngo Dinh Diem as South Vietnam's prime minister. Additionally, Eisenhower created a regional defense apparatus, the Southeast Asian Treaty Organization (SEATO), modeled after NATO, to protect the new nation as it bloomed into an independent state. Diem was an archconservative with autocratic tendencies who soon declared South Vietnam an independent state and cancelled the scheduled national elections. The United States supplemented Diem with vast amounts of capital, goods, machinery, weaponry, and advisors to train his soldiers. This effort marked the nation-building phase of the Cold War. The decision to build a nation as a response to what was essentially a civil war, committed the United States to the success and failure of South Vietnam, and would have dire consequences for America's place in the Cold War.

The Middle East became bothersome for Eisenhower in the later years of his administration, forcing him to make his own Cold War declaration in 1957. Egyptian president, Gamal Nassar created the Baghdad Pact, a military alliance between Egypt, Iraq, Iran, Pakistan, and Turkey in 1955 with the belief they could exploit the Cold War division for the benefit of Arab and Muslim nations. As part of his "middle road" strategy, Nassar opened relations with communist nations, Czechoslovakia and China, which soured America's attitude toward Egypt and compelled Dulles to cancel funds for the Aswan hydroelectric dam. Nassar responded by nationalizing the Suez Canal and assuming control of the oil traveling into the Mediterranean from the East. The situation escalated when Israel attacked Egypt over disputed territory, and Great Britain and France took that as an opening to seize the Suez Canal. The conflict placed the world oil trade and Middle Eastern stability in jeopardy, and forced Eisenhower to pressure the European nations to relinquish control of the canal. Although resolved, the specter of Soviet influence in the oil-bearing region forced Eisenhower to take a stronger stand in the Middle East. The concern culminated in the "Eisenhower Doctrine," which held that the United States defend any Middle Eastern nation against communism. Eisenhower invoked the doctrine only twice, in the Jordanian uprising that spring and Lebanon in 1958, but it set precedence for future presidents Lyndon Johnson, Richard Nixon, and Jimmy Carter.

By the end of his term as president, Eisenhower faced ironic opposition. His administration privileged modernization, and ended under the suspicion of technological backwardness. Eisenhower created the National Aeronautics and Space Administration (NASA), and began America's reach for the heavens. The Russian launch of Sputnik, the unmanned satellite in late 1957, and the downing of the American U2 surveillance plane in 1960, demanded a greater investment in science and technology. John F. Kennedy drew upon this anxiety when he argued that America lagged behind the Soviet Union in missile production. The Missile Gap critique helped Kennedy capture the White House, but it also placed unrealistic burdens on the way he and his successor Lyndon B. Johnson conducted the Cold War.

In the 1960s, the Vietnam conflict pervaded America's Cold War politics. The decade began with President Kennedy suffering profound Cold War failures, the failed attempted overthrow of Cuba's Communist leader Fidel Castro at the Bay of Pigs, the CIA-sponsored assassination of Congolese Prime Minister Patrice Lumumba, the Cuban Missile Crisis, and the construction of the Berlin Wall. Needing to silence critics, Kennedy decided to take a more rigid stand against the Communists in South Vietnam. With Diem's popularity at a nadir due to his oppressive policies, Kennedy signed off on a plan to depose him. During the junta, however, the operatives assassinated Diem, foreshadowing Kennedy's own murder three weeks later.

When Lyndon B. Johnson assumed the presidency, he inherited the burden of not losing the Cold War in Vietnam. Weighted by fluctuations in the civil rights movement and burgeoning antiwar sentiment, Johnson accelerated both nation building in South Vietnam and military resistance to Communists. The entire conflict, and to some degree American prestige, came crashing to the ground in 1968 when Communist forces launched a massive attack against American and South Vietnamese forces in the major cities. Although the siege only had temporary success, it had a leveling effect on domestic sentiment. Cold War arguments carried less significance and the trouble became finding a way out. That responsibility fell to Richard Nixon who inherited the Vietnam and the Cold War in 1969.

In the midst of the conflict, Nixon and his secretary of state, Henry Kissinger, began to redefine the Cold War into a mutual understanding of the boundaries between the U.S. and Russia. He coupled this with the Nixon Doctrine, which held that America would relinquish some of its military commitments. Breaking precedent, Nixon went to China and began arms reduction talks, or détente, with the Russians. To counter his critics, Nixon coupled détente with a brinkmanship-like tactic he called the "mad man theory." According to this strategy, American allies would warn Third World nationalists that Nixon was insane and willing to use nuclear weapons to end disputes. The crazy man tactic had little to no effect on its intended audience, North Vietnam, or any of the other Cold War dissidents. Nixon's Strategic Arms Limitation Talks (SALT I), begun in 1969 and concluded May 1972, between the United States and Brezhnev regime exemplified the spirit his doctrine. While SALT I failed to reduce the creation and stockpiling of new, more destructive weapons, it was a progressive gesture toward an international dialogue on nuclear weapons.

Buoyed by the apparent success of détente and the belief that China could help end the war in Vietnam, Nixon went into the presidential election of 1972 confident in his Cold War program. Indeed, twenty-five years had shifted the Cold War from security concerns, to a contest of development, to Nixon's program of limited contact, and ended the 1960s with the possibility of an uneasy coexistence between Soviet socialism and democratic capitalism. Many questions were still unanswered regarding the conflict in Vietnam, rising nationalism in the Middle East, the global economy, domestic dissent, and nuclear control. These issues would dominate the last seventeen years of the Cold War.

FURTHER READING:

BOOKS:

Gaddis, John Lewis. *We Now Know: Rethinking Cold War History.* Oxford University Press, 1998.

La Feber, Walter. *America, Russia, and the Cold War.* McGraw-Hill Humanities, 2001.

McDougall, Walter. *The Heavens and the Earth: A Political History of the Space Race.* Baltimore: Johns Hopkins University Press, 1997.

McMahon, Rober. *The Cold War on the Periphery.* New York, Columbia University Press, 1994.

Wagnleitner, Reinhold. *Cocacolonization and the Cold War.* Chapel Hill, The University of North Carolina Press, 1997.

PERIODICALS:

Frank Costigliola, "Unceasing Penetration": Gender, Pathology, and Emotion in George Kennan's Formation of the Cold War." *Journal of American History* 83 (March, 1997): 1309–1939.

SEE ALSO

Berlin Airlift
CIA (United States Central Intelligence Agency)
Cold War (1945–1950), The Start of the Atomic Age
Cold War (1972–1989): The Collapse of the Soviet Union
National Security Act (1947)
NATO (North Atlantic Treaty Organization)
NSC (National Security Council)
Nuclear Reactors
OSS (United States Office of Strategic Services)
Truman Administration (1945–1953), United States National Security Policy
United States, Intelligence and Security

Cold War (1972–1989): The Collapse of the Soviet Union

JOSEPH PATTERSON HYDER

By the early 1970s, the Soviet Union was at the peak of its power. The Communist Party remained the sole political force in the Soviet Union, but decades of post-Stalinist economic reforms left the Soviet empire with a seemingly robust economy and an increased standard of living for Soviet citizens. Wages in the Soviet Union increased sharply. The Soviet Union was the world's leading producer of steel and oil. Urban dwellers enjoyed modern appliances, such as televisions and dishwashers, and lived mostly in the plentiful newly-constructed single-family apartments.

In addition to these economic advantages at home, the Soviet Union attempted to assert itself as the world's dominant superpower. For nearly every Soviet success in the early 1970s, the United States suffered a setback. While the oil-rich Soviet economy continued to grow, the economy of the United States strained under the pressure of the OPEC imposed oil embargo of 1972 and 1973.

The Soviet Union also prevailed on the international stage. Soviet-backed North Vietnamese forces expelled American troops after a prolonged conflict. The communist victory in Vietnam, coupled with U.S. public opposition to the conflict, signaled an end to the American policy of communist containment in Southeast Asia. With further containment of communism in doubt, the United States had to reposition itself on the international scene. The administration of President Richard M. Nixon embarked on a policy of détente with China, culminating with Nixon's trip to China, and, to some degree, with the Soviet Union. The pace of Soviet nuclear weapon production greatly alarmed Washington. Fearing a Soviet advantage in the arms race, Nixon signed the Strategic Arms Limitations Talks (SALT I).

In addition to Southeast Asia, Soviet ideology was gaining support in other parts of the world, including Latin America. Soviet-supported troops in Central and South America alarmed American officials, who feared communist expansion in the Western Hemisphere. Still deeply

Berliners sing and dance on top of the Berlin Wall in front of the Brandenburg Gate to celebrate the opening of East-West borders in 1989. Built of barbed wire and concrete in 1961, the wall divided Berlin and became the most powerful symbol of the Cold War. AP/WIDE WORLD PHOTOS.

wounded by opposition to the Vietnam War, however, America resorted to conducting covert operations in Latin America. During the administration of President James E. Carter, communist backed Sandinistas overthrew Nicaragua's government. President Ronald Reagan later provided financial and material support to anti-Sandinista rebels. Reagan also backed anti-communist forces in El Salvador, even though Congress did not always agree with the White House on the issue of Nicaragua and El Salvador.

With proxy victories in Southeast Asia and Latin America and with a booming national economy, the power of the Soviet Union appeared formidable under Soviet Premier Leonid Brezhnev. To many outside observers, the Soviet Union appeared to be on the verge of winning the Cold War. The post-Brezhnev years, however, would see the internal collapse of the Soviet Union. Even while the Soviet Union was soaring to new heights, cracks were beginning to form in the monolithic empire. Economic troubles, military failures, and emerging nationalism would soon result in the end of the Soviet Union and communist regimes in Eastern Europe.

Economic stagnation and the arms race. The vigorous Soviet economy of the late-1960s and early 1970s quickly fell victim to the very factors that had contributed to its success, central planning and raw materials allocation. Brezhnev recognized that the Soviet economy was slowing, and attempted to patch problems rather than completely overhaul the system. His efforts failed. Even if Brezhnev had attempted to overhaul the Soviet economy, the highly entrenched special interests that made their living by manipulating the Soviet Union's centrally planned economy could have defeated Brezhnev's efforts.

Throughout the 1970s and into the mid-1980s, the Soviet Union's GNP and industrial output continued to increase, but at a lessening pace, eventually leading to economic stagnation. The Ninth Five Year Plan (1970–1975) saw a growth rate of approximately 3%. The period of 1975–1980 experienced a growth rate of between 1% and 1.9%, depending on whether revised Soviet numbers or the West's estimate is examined. Likewise, 1980–1985 saw a further decline in economic growth, between 0.6% and 1.8%. Declining economic growth rates were not confined to the Soviet Union. Eastern Europe, with its economies intertwined with the Soviet Union's, suffered a similar fate.

This declining growth rate in the 1970s and 1980s resulted in the Soviet Union receiving a diminishing rate of return on capital investment. This proved disastrous for the Soviet economy, because by 1980, the Soviet Union

was spending nearly one-third of its GNP on capital investment, with most of the sum dedicated to the military. The military was consuming such a large portion of the Soviet economy for two reasons: the Soviet involvement in Afghanistan and the arms race with the United States. These two events would weigh heavily in the Soviet economic demise and lead to its inevitable fall. A weak economy prevented the Soviet Union from reacting appropriately to each experience.

The stagnant Soviet economy of the 1970s would have faired far worse had it not been for vast oil and natural gas production propping up the economy. By the late 1970s, technological backwardness and poor management under the centrally planned Soviet economy resulted in depleted oil and gas reserves. This led Brezhnev to turn his eye towards the oil and gas reserves of Central Asia. Afghanistan had long been a relatively undeveloped country comprised of numerous semi-autonomous ethnic groups. Brezhnev assumed that the Soviet Union could achieve a quick and decisive victory over the country and expand its influence of Communism into Central Asia.

The United States and the rest of the world quickly condemned the Soviet invasion of Afghanistan in 1979. The United States also provided covert support to the mujahideen, or Afghani resistance fighters. Rapid turnover in Soviet leadership following the death of Brezhnev in 1982 also hampered the war effort. The short-lived regimes of Yuri Andropov and Konstantin Chernenko provided for an inconsistent Afghan policy. The Soviet military operation quickly bogged down and faced stiff resistance in the harsh terrain of Afghanistan.

The Soviets erroneously assumed that since the Afghans were economically disadvantaged, they would be quickly defeated and embrace communism. The opposite result happened. As the Afghans had little to lose by continuing to fight, instead of driving Afghanistan to communism, the Soviet invasion forged the Afgani Islamic resistance. A decade after the invasion, Soviet troops withdrew.

The war in Afghanistan had an even more adverse effect on the Soviet Union than the Vietnam War had on the United States. Thousands of Soviet troops died in a conflict that resulted in the defeat of a superpower by a developing country. Moreover, the conflict strained an already weak economy. The conflict angered Soviet citizens, and they began demanding accountability from the state. Brezhnev and his successors intended the war in Afghanistan to reassert the supremacy of the Soviet Union. Instead, the conflict proved that the superpower's might was waning.

The war in Afghanistan also distracted the Soviet Union from its arms race with the United States, thus allowing America to gain a technological advantage. The United States ratcheted up pressure on the U.S.S.R. through several means. The Reagan administration began placing missiles in Western Europe, primarily in Western Germany, strategically located to intimidate Eastern Europe and the Soviet Union. Reagan also began building up the U.S. military. Reagan commissioned new aircraft carriers and expanded America's stealth aircraft program. To the Soviets, these actions signaled a widening weapons gap, particularly in terms of technologically advanced weapons.

Perhaps the greatest threat to the Soviet Union was the United States' Strategic Defense Initiative (SDI), also known conventionally as Star Wars. The SDI was a planned satellite based weapons system that would detect and destroy missiles fired at the United States. Such a technological advancement would have rendered Soviet ICBMs useless. The Soviet Union tried to dissuade the United States from implementing the SDI, but the Reagan administration refused to back away from the proposal. In reality, the SDI was only in the technological planning stages; the Soviets, however, bought America's bluff, prompting a quick and expensive advance in their lagging military technology. This increased spending further accelerated the Soviet economic decline.

Realizing a weapons gap, the Soviet Union began pushing the Reagan administration for nuclear arms talks following the death of Brezhnev in 1982. The U.S. soon entered negotiations over the Strategic Arms Reduction Treaty (START). However, numerous changes in post-Brezhnev Soviet leadership, Solidarity strikes in Poland, and other issues prevented the completion of the START during the Reagan administration.

Gorbachev and the end of the Cold War. After a decade of over-inflated military expenditures, dwindling oil revenue, and a centrally-planned economy that was too rigid to adapt to consumer demands, Mikhail Gorbachev, upon assuming office, declared the Soviet economy to be in a "pre-crisis." Gorbachev immediately transformed the face of Soviet politics. Gorbachev quickly appointed new members to the Politboro and Secretariat, ridding each of many hardline, longtime bureaucrats. Gorbachev also attempted to reform the KGB, replacing many agents and bureaucrats. Despite the shake-up, the KGB's operational power emerged from Gorbachev's early reforms relatively unscathed.

After reforming the government, Gorbachev set out to reform the economy and ultimately, Soviet society. Gorbachev's economic reforms (*perestroika,* or restructuring), were perceived as noble, but poorly executed. The Twelfth Five Year Plan tried ambitiously and quickly to reform the Soviet economy. Gorbachev sought to update industrial equipment and computer systems, while simultaneously expecting workers to produce higher quality products in greater quantities. Gorbachev also tried to decentralize the economy by giving different regions greater control over industry. All of these goals proved to be unrealistic given Gorbachev's timetable to dismantle the gargantuan Soviet bureaucracy in favor of a more streamlined and efficient system.

By 1986, Gorbachev also began experimenting with the notion that greater democracy, if presented in the

proper format, would lead to increased socialism. Gorbachev wanted to strip away Stalinism and its accompanying bureaucracy and return to the communism of Lenin. Initially, Gorbachev underestimated the effect that allowing Soviet citizens to question the past, in particular the brutality of Stalin, would have upon the citizenry, leading them to follow their lines of questioning up to the present day. Soon, however, Gorbachev came to accept and embrace the concept that he termed *glasnost,* or "openness."

Glasnost initially allowed only the divulgence of information by the state. Gorbachev held that if the Soviet Union was more open and honest about its past, then Soviet and Eastern European citizens would be more likely to follow Gorbachev's economic lead. Even a large number of bureaucrats in the KGB supported glasnost. The KGB's information network had become burdened and as ineffective as the bureaucracy that it supported. Therefore, many KGB officials assumed that fostering an atmosphere of openness would result in new and better informants.

Although Gorbachev intended glasnost to strengthen the communist regime, he did not initiate a crack-down when Soviet citizens went beyond the original intent of glasnost. Soviet intellectuals began questioning the very tenets of Soviet Communism and attacked the Communist Party in newspapers, journals, film, and books. Eastern European thinkers followed the lead of their Soviet counterparts.

Consequently, glasnost had the unintended effect of spurring nationalist and anti-communist movements in Eastern Europe and the Soviet republics. Dissidents in Poland, East Germany, Czechoslovakia, and other Soviet-satellite states staged labor demonstrations. Citizens took to the streets, demanding that the Communist Party step aside and allow democratic elections. In fall 1989, the Berlin Wall, long a symbol of the division between Eastern Europe and the world, fell, allowing East and West Berliners to cross freely. The Communist Party and its East Germany secret police organization, the Stasi, had lost power. Within months of the fall of the Berlin Wall, other Eastern European countries broke away from Moscow's influence and expelled their communist leaders. With the exception of Romania, most of the revolutions of 1989 and early 1990 were relatively peaceful.

In the wake of the Eastern European revolts and the euphoria that followed, the Soviet Union had little choice but to allow greater freedoms. In February, 1990, the Communist Party agreed to relinquish its political monopoly. Many of the civic groups that had been voicing displeasure with the Soviet system formed political parties. Most of these new parties, especially those outside of Russia had a nationalist agenda. Within a month, the Baltic republic of Lithuania declared itself an independent state. Other Soviet republics quickly followed.

In June 1991, Gorbachev allowed free elections to choose a president of the Russian Republic. Boris Yeltsin, a former Gorbachev-supporter, won a landslide victory over Gorbachev's chosen candidate. In August, 1991, a group of communists hardliners attempted a poorly organized coup while Gorbachev was on vacation at the Black Sea. The coup failed, and strengthened Boris Yeltsin, the primary target of the coup. The coup also undermined the leadership of Gorbachev, who continued to govern ineffectively until his resignation on December 25, 1991. The following day, the Supreme Soviet officially declared an end to the Soviet Union.

FURTHER READING:

BOOKS:

Baucom, Donald. *The Origins of SDI.* Lawrence, KS: University Press of Kansas, 1992.

Brown, Archie. *The Gorbachev Factor.* Oxford: Oxford University Press, 1997.

Colton, Timothy, and Robert Legvold. *After the Soviet Union.* New York: W. W. Norton, 1992.

McGuire, Michael. *Perestroika and Soviet National Security.* Washington, D.C.: Brookings Institute, 1991.

McMahon, Robert. *The Cold War on the Periphery.* New York: Columbia University Press, 1994.

SEE ALSO

Carter Adminstration (1977–1981), United States National Security Policy
Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Ford Administration (1974–1977), United States National Security Policy
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*
Nixon Administration (1969–1974), United States National Security Policy
Reagan Administration (1981–1989), United States National Security Policy

Colombia, Intelligence and Security

Colombia emerged as an independent nation in 1830, following the collapse of Spanish rule in the region, then known as Gran Colombia. Large-landowning and military interests alternately dominated the nation's politics, causing long-standing political tension. In the 1960s, political extremists and paramilitary insurgent groups began attacking government interests in the capital. The conflict escalated in the 1990s, destabilizing the Colombian government and allowing areas of the countryside to fall to

guerilla control. Violence and sporadic fighting continue to be endemic in the nation, but the government restructured intelligence, police, and military forces to combat the problem.

Colombia's main intelligence service is the National Intelligence Service (SIN). The SIN coordinates civilian intelligence efforts, including those of subsidiary departments such as counter-intelligence, anti-terrorism, and surveillance forces. SIN operations cover both domestic and foreign intelligence, but focus on combating political insurgency and threats to national security. The agency works with the Colombian National Police to investigate criminal activities related to drug cartels or paramilitary groups, as well as instances of government corruption.

The Department of Administrative Security (DAS) works to protect government officials and buildings. The DAS also conducts limited counter-espionage operations to ensure the safety and security of government information and communication systems.

Military intelligence in Colombia is the responsibility of the army and the Intelligence Department (F-2). Military intelligence assesses external threats to Colombian national security, and conducts surveillance of paramilitary and rebel groups within national borders.

After a series of constitutional reforms in the early 1990s, the Colombian government began negotiations with leftist rebel and right-wing paramilitary groups. The government in Bogotá ceded control of some remote areas to opposition control, but the transfers of power did little to abate continued violence. The government continues to use intelligence and security forces for both anti-paramilitary operations and political espionage with some success. Creation of the Anti-Kidnapping Squad has reduced the number of government officials, journalists, and foreign businesspeople taken by insurgent forces who seek to intimidate the government or extract ransom payments.

In the midst of political chaos, the presence and influence of drug trafficking rings, cartels, and crime syndicates has increased in Colombia and throughout the surrounding region. The Colombian government has pledged support to international efforts to reduce the cultivation, production, and trafficking of illicit drugs. With the aid of the United States, and other nations, Colombia patrols its countryside with aerial surveillance, has implemented tighter security in its ports, and begun a campaign to seize illegal funds and halt money laundering operations.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. "Colombia" CIA World Factbook <http://www.cia.gov/cia/publications/factbook/geos/co.html> (April 8, 2003).

Colossus I

DAVID TULLOCH

Colossus I was the world's first programmable computer. Colossus I was created during World War II by the British to speed up the decryption of German messages encoded by the Lorenz Schlüsselzusatz (SZ) 40 and 42 machines.

In 1940, the British began to intercept German non-Morse teleprinter text that used the Baudot Code, an international standard where each letter is represented by five binary elements. In modern binary notation, A is 11000, B equals 10011, and G is 01011. The Lorenz machine used a code devised by Gilbert Vernam (1890–1960) in 1918. Obscuring letters were added in modulo 2 addition, where adding like to like gives a 0, while like and unlike equals 1.

The Lorenz machine added two obscuring letters generated by two sets of five-toothed wheels, and two motor wheels arranged in any order and starting position. The British did manage to break this system when multiple messages were sent using the same initial settings, but decoding was time-consuming and only partially successful. Eventually, the internal workings of the SZ machines were deduced, and allowed decoding, providing the starting position of the wheels could be found. Decoding by hand, however, took several weeks. Max Newman (1897–1984) used the ideas of Alan Turing (1912–1954) to design a machine to speed up the process. Called "Robinson" after Heath Robinson, the British cartoonist and designer of fantastic machines, it compared the coded text with another piece of tape that represented the Lorenz wheel settings. However, keeping the two paper tapes in sync at high speed was difficult, and they frequently tore.

Tommy Flowers (1905–1998), an engineer, had the idea of representing the Lorenz wheel settings electronically, doing away with the need for synchronised tapes. Despite many doubters, Flowers spent ten months building the Colossus Mark I, completed on December 8, 1943. Colossus contained 1500 valves, more than had been previously used in a single device, and used photocells to read punched paper tape at 5000 characters per second. It had a limited memory, of five-bits, and used pluggable logic gates. The wheel settings of the Lorenz ciphers were simulated in collections of thyratons, gas-filled triodes that acted as one-bit stores. The results were then printed via a typewriter.

The Colossus Mark I was quickly outdated by the Colossus II, the first of which was finished by June, 1944. Nine Mark IIs were built, and the original machine was upgraded to become the tenth machine, each one occupying a large room. The Colossus II used around 2500 values and read the tape five times as fast as its predecessor.

The Colossus machines counted through the length of the encoded text many times, effectively trying out billions of combinations to determine which initial wheel

settings of the Lorenz encoder were statistically significant. The Colossus output did not give a decoded message, but rather the settings of the first set of five wheels. Humans, using a combination of statistics, language skills, and intuition did the remaining decoding. Finally, the complete wheel settings were fed into a device that produced the deciphered message. Later, the versatile Colossi were reprogrammed to do more of the code-breaking work, but there was always considerable input from their human operators.

Breaking the Lorenz cipher gained the Allies crucial information that aided in major operations, such as the Battle of Kursk, and the D-Day landings. Colossus showed that Turing's ideas of a universal computer could be made into practical machines. However, the existence of Colossus was kept secret for many years, and so the American Electronic Numerical Integrator and Computer (ENIAC), completed by the U.S. Army in 1946, was considered the world's first computer until information on Colossus was finally declassified in the 1970s. In 1996, a Colossus was reconstructed, and it can be seen at the Bletchley Park Museum.

FURTHER READING:

BOOKS:

Hinsley, F. H., et al. *British Intelligences in the Second World War: Its Influence on Strategy and Operations,* Volume Three, Part I. London: Her Majesty's Stationary Office, 1984.

Sale, Anthony E. "The Colossus of Bletchley Park—The German Cipher System," in Raùl Rojas and Ulf Hashagen *The First Computers: History and Architectures.* Cambridge, MA: MIT Press, 2000.

Smith, Michael. *Station X: The Codebreakers of Bletchley Park.* London: Channel 4 Books, 2000.

ELECTRONIC:

WWII Codes and Ciphers. <http://www.codesandciphers.org.uk> (December 19, 2002).

SEE ALSO

Cipher Key
Cipher Machines
Codes and Ciphers
Enigma

COMINT (Communications Intelligence)

JUDSON KNIGHT

COMINT or communications intelligence is intelligence gained through the interception of foreign communications, excluding open radio and television broadcasts. It is a subset of signals intelligence, or SIGINT, with the latter being understood as comprising COMINT and ELINT, electronic intelligence derived from non-communication electronic signals such as radar. During the early part of the modern intelligence era, the terms "signals intelligence" and "communications intelligence" were used virtually interchangeably, and therefore, much of what was described as signals intelligence in World War II is more properly understood as COMINT.

Early History of Army and Navy COMINT

COMINT is the province of several services, both military and non-military, most notably the National Security Agency (NSA) and the United States Army Intelligence and Security Command (INSCOM). Until the establishment of NSA in 1947, however, the majority of COMINT took place under the aegis of "signals intelligence" activities in the two principal military services. Though military cryptanalytic and cryptographic operations dated back at least to World War I, and included activities at the War Department Military Intelligence Division under the direction of Herbert O. Yardley, the first true COMINT organization was the Army's Signal Intelligence Service (SIS).

Established on April 24, 1930, SIS not only undertook cryptographic and cryptanalytic tasks, but developed cipher machines and produced studies on cryptology. Its greatest achievement was its breaking of the Japanese diplomatic ciphers with the PURPLE code machine prior to World War II. In June 1942, after the outbreak of war, SIS acquired an intercept operation in the form of the 2nd Signal Service Battalion, which conducted radio intercepts at Vint Hill Farms in Warrenton, Virginia.

A tale of two services. The interaction of army and navy COMINT activities during the war is rather like a morality tale of two brothers, the older one highly favored, but failing to live up to expectations, and the younger one coming from behind to triumph. In this analogy, the army was the "older brother," and the navy, which lacked a true COMINT organization during the war, the surprising dark horse. After its initial victory with PURPLE, SIS conducted a long and frustrating effort to crack Japanese military codes, succeeding only in 1944.

The Navy had, at the end of World I, a cryptologic bureau that had emerged during the war. The bureau provided codes for the use of President Woodrow Wilson during the Paris Peace Conference, but when Yardley demonstrated his ability to break the naval codes, the Office of Naval Intelligence (ONI) closed down the cryptologic bureau in July 1918. Navy COMINT efforts then retreated to the shadows—a fitting place for intelligence operations.

Naval successes in the 1920s. Operating through the Research Desk at the Office of Naval Communications, the Navy's informal COMINT unit, designated OP-20-G, consisted of Lt. Laurence F. Safford and a four-person civilian staff. Denied any help from the army, the unit, which began operation in 1924, turned its attention to Japanese naval codes.

By then the navy, in collaboration with the Federal Bureau of Investigation and the New York City police, had already undertaken several attempts to—quite literally—steal codes from the Japanese Consulate in New York City. A series of breaks-in during the 1920s led to the compilation of a Japanese codebook. Because of the book's red binding, the code itself was thenceforth known as RED.

COMINT cooperation during the war. The navy actually played a critical role in decoding PURPLE: the machine that broke the code was constructed at the Washington Naval Yard in 1940. Thereafter SIS and the naval unit worked together to break the Japanese diplomatic code. At the same time, the navy had more success than the army in breaking the codes of its Japanese counterpart—but unfortunately, a change of code on December 1, 1941, helped make the United States vulnerable to the attack on Pearl Harbor that occurred six days later.

However, the navy was able to penetrate Japan's naval codes several other times, reacquiring them after changes by the Japanese, and thus contributed to American success in the battles of the Coral Sea and Midway in mid-1942. By the end of the war, the status of naval COMINT had risen to such a degree that SIS actively sought its help.

The postwar era. Between 1942 and September 1945, SIS went through a staggering number of name changes, to Signal Intelligence Service Division, Signal Security Division, Signal Security Branch, Signal Security Division (again), Signal Security Service, and Signal Security Agency. In September 1945, it became the Army Security Agency, which was replaced by the Army Intelligence and Security Command in January 1977.

The naval COMINT office only acquired a formal name in 1968, when it was designated the Naval Security Group. Later it was placed under NSA, which replaced the Armed Forces Security Agency, a shortlived (May 1949-October 1952) attempt to consolidate cryptology operations of all the services.

An E-3 Sentry airborne warning and control system aircraft (AWACS) lands at Kadena Air Base on Okinawa, Japan.

FURTHER READING:

BOOKS:

Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence.* Woodstock, NY: Overlook Press, 2002.

Alvarez, David J. *Allied and Axis Signals Intelligence in World War II.* Portland, OR: F. Cass, 1999.

Andrew, Christopher M. *Codebreaking and Signals Intelligence.* Totowa, NJ: F. Cass, 1986.

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

Gilbert, James L., and John Patrick Finnegan. *U.S. Army Signals Intelligence in World War II: A Documentary History.* Washington, D.C.: U.S. Government Printing Office, 1993.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

Sexton, Donal J. *Signals Intelligence in World War II: A Research Guide.* Westport, CT: Greenwood Press, 1996.

West, Nigel. *The SIGINT Secrets: The Signals Intelligence War, 1900 to Today: Including the Persecution of Gordon Welchman.* New York: W. Morrow, 1988.

ELECTRONIC:

Pearl Harbor Revisited: U.S. Navy Communications Intelligence, 1924–1941. U.S. Naval Historical Center. <http://www.history.navy.mil/books/comint/> (March 29, 2003).

SEE ALSO

Army Security Agency
Cryptology, History
INSCOM (United States Army Intelligence and Security Command)
Intelligence
NMIC (National Maritime Intelligence Center)
NSA (United States National Security Agency)
SIGINT (Signals Intelligence)

A section of structural steel beam recovered from the World Trade Center hovers over members of the media during a 2002 press conference at the Commerce Department's National Institute of Standards and Technology. A 24-month study was announced to examine the structural failure and collapse of the WTC buildings during the terrorist attacks of September 11, 2001. AP/WIDE WORLD PHOTOS.

Commerce Department Intelligence and Security Responsibilities, United States

JUDSON KNIGHT

In addition to promoting trade and industry, the United States Department of Commerce (DOC), through it various bureaus, conducts the census, maintains standards of weights and measures, and monitors the oceans and atmosphere. The department has a number of intelligence and security functions, ranging from protecting computers against hackers to overseeing exports of suspicious transfers to hostile nations.

Founded in 1903 as the Department of Commerce and Labor, the Department of Commerce emerged in its present form after the Department of Labor separated from it in 1913. The modern Commerce Department includes, among other offices, the bureaus described briefly below.

The Economics and Statistics Administration (ESA) is responsible for compiling, analyzing, and producing reports based on economic and demographic data. Similar in mission is the Bureau of Economic Analysis (BEA), which is dedicated to collecting statistical information with the aim of producing an accurate picture of the U.S. economy. Closely related to ESA and BEA is one of the most well known sections of Commerce, the Bureau of the Census. In addition to the decennial (once every decade) census, the Census Bureau conducts demographic and

economic censuses, and produces more than 200 annual surveys, many for other government agencies.

At the center of the traditional Commerce Department mission are three bureaus. The International Trade Association (ITA) promotes U.S. exports of manufactured goods, nonagricultural commodities, and services. Assisting minorities and the economically disadvantaged are the Minority Business Development Agency (MBDA) and the Economic Development Administration (EDA). The first of these promotes minority-owned business, while the EDA helps economically distressed communities by providing grants, assisting in job retention, and stimulating industrial and commercial growth within these communities.

Science, technology, and national security. Commerce bureaus with a special scientific focus include the National Institute of Standards and Technology (NIST, covered elsewhere) and the National Oceanic and Atmospheric Administration (NOAA). NOAA is concerned with environmental assessment and prediction, protection of public safety, weather forecasting, and the protection of marine resources.

In the area of technology are three other bureaus: the National Telecommunications and Information Administration (NTIA), the Patent and Trademark Office (PTO), and the Technology Administration (TA). NTIA acts as the principal advisor to the president on matters of telecommunications policy with regard to economic and technological advancement, as well as regulation. It is one of several government agencies concerned with the operation of the Internet. Like the Census Bureau, PTO is another office of the Commerce Department whose functions are well known; not only does it serve as a registry for new inventions and processes, it acts to protect this information, and to promote innovation. As for TA, it is concerned with promoting the economic competitiveness of U.S. technology companies.

The Bureau of Industry and Security (BIS) is concerned with issues of national security, including efforts to stop the proliferation of weapons of mass destruction. At the same time—and in a function more commonly associated with the Commerce Department in the popular imagination—BIS also seeks to further the growth of U.S. exports.

Other intelligence and security matters. Most of the above-named bureaus fall under one of a half-dozen Commerce undersecretaries. In addition, other offices are directed by officials, among them the General Counsel, who report directly to the Secretary of Commerce. Furthermore, a presidential directive in 1998 placed the Critical Infrastructure Assurance Office (CIAO; see entry) under the Commerce Secretary's direction without establishing an obvious chain of command.

Among the Commerce offices involved in intelligence functions are the Office of Executive Support (OES, formerly the Office of Intelligence Liaison), which reports to the General Counsel; the Office of Export Enforcement (OEE), which reports to the undersecretary for international trade; and the Office of Foreign Accountability (OFA), whose leadership comes from the assistant secretary for export administration.

OES, as its old name (changed in 1996) made clearer, serves as a liaison between the Commerce Secretary and the intelligence community, especially where technology transfer issues are concerned. OEE oversees the export of sensitive technology, and continually monitors trade data with an eye toward national security. As for OFA, during the Cold War, its task was to promote advantages for U.S. companies competing against Soviet and Chinese exports. Since the early 1990s, however, it has been more concerned with the proliferation of nuclear and ballistic missile technology, as well as with chemical and biological weapons.

Under the administration of President William J. Clinton, the Commerce Department became an area of security concern. These issues first emerged when Ron Brown, Clinton's first Secretary of Commerce, was reported to be packing overseas trade missions with high-volume donors to the Democratic Party. Later, Clinton replaced Brown (who died in a 1996 plane crash) with William Daley, but more problems emerged with revelations that Deputy Assistant Secretary for Trade Missions John Huang had obtained a high-level security clearance while maintaining close contact with the Chinese government. In February 1998, Daley announced plans to tighten security and limit access to classified information within the department.

FURTHER READING:

BOOKS:

Bowers, Helen. *From Lighthouses to Laserbeams: A History of the U.S. Department of Commerce.* Washington, D.C.: U.S. Department of Commerce, 1995.

PERIODICALS:

White, Ben. "Commerce Secretary Unveils New Security Policy." *Washington Post* (February 11, 1998): A19.

ELECTRONIC:

Department of Commerce. <http://www.commerce.gov> (January 28, 2003).

SEE ALSO

Clinton Administration (1993–1997), United States National Security Policy
Critical Infrastructure Assurance Office (CIAO), United States
NIST (United States National Institute of Standards and Technology)
Port Security
Satellite Technology Exports to the People's Republic of China (PRC)

Elsie Meeks, the first American Indian member of the U.S. Commission on Civil Rights, in her Kyle, South Dakota office in 2001. AP/WIDE WORLD PHOTOS.

Commission on Civil Rights, United States

JUDSON KNIGHT

Established under the Civil Rights Act of 1957, the United States Commission on Civil Rights serves in an investigative, fact-finding role with regard to allegations of discrimination or denial of equal protection under the laws. The commission, as it is known, has no enforcement powers, but works closely with the federal, state, and local agencies that have powers of enforcement.

Unlike a number of federal agencies whose upper echelons consist almost exclusively of appointees chosen by the current administration, the commission is designed to be independent. Four of its eight members are appointed by the president, but the presence of persons who would likely be friendly to the administration is counterbalanced in large degree by the other half of the commission, whose members are appointed by Congress.

It is significant that the commission began life at a time when both houses of Congress were dominated by Democrats, while Dwight D. Eisenhower, a Republican, held the White House—an ideal situation for a politically diverse Commission. Though the years since have seen long periods in which Democrats controlled both the executive and legislative branches (1961–69, 1977–81, 1993–95), as well as a brief period in 2001 when Republicans enjoyed the same advantage, differences between White House, Senate, and House leaders have helped to ensure a healthy degree of political diversity on the Commission. Furthermore, its rules hold that no more than four members at any one time shall be of the same political party.

Political independence. Although the president appoints the chairperson and vice-chairperson, one incident from the administration of George W. Bush serves to illustrate the commission's independence from the Chief Executive. The commission ordered a study of the controversial November 2000 balloting in Florida, which resulted in a deadlock between then-Governor Bush and his Democratic opponent, Vice President Albert Gore, Jr. Ultimately the United States Supreme Court declared Bush the victor, but only after five weeks of bitter legal wrangling. The commission concluded in June 2001, by a vote of 6–2, that the voting in Florida had been characterized by "injustice, ineptitude, and inefficiency" that resulted in the loss of some voting rights by minority participants in the election.

The conclusion, which the two dissenting board members described as based on faulty analysis, resulted from findings that minority voters' ballots were more likely to be rejected than those of their white counterparts.

Responsibilities and powers of the commission. The Florida study is an example of the commission fulfilling one aspect of its mandate: investigation of allegations that citizens have been denied their right to vote either by fraudulent practices, or by reason of their race, color, sex, religion, age, disability, or national origin. The commission also studies and compiles information regarding discrimination or denial of equal protection in the administration of justice, or because of race and the other characteristics named previously. It submits reports and recommendations to the White House and Congress, and issues public service announcements designed to discourage discrimination or the denial of equal protection under the law.

The commissioners, who serve six-year terms, meet on a monthly basis, except during August, and meet several other times each year to hold hearings, conferences, consultations, or briefings. In the process of producing documents, the commission can call witnesses and issue subpoenas within a state at which a hearing is held, and within a 100-mile radius of the site of the hearing, whichever is larger. The commission maintains advisory committees at the state level, and refers the many complaints it receives to appropriate federal, state, or local agencies (including ones concerned with law enforcement), as well as private organizations.

The results of commission studies usually see publication, and the commission produces a number of pamphlets on a yearly basis. Among those that appeared in 2002 were *Briefing on Civil Rights Issues Facing Muslims and Arab Americans in Minnesota Post-September 11* (the commission also produced a similar study on Wisconsin); *Voting Rights in Florida 2002: Briefing Summary;* and *Haitian Asylum Seekers and U.S. Immigration Policy.*

■ FURTHER READING:

ELECTRONIC:

Civil Rights Commission Approves Report Assailing Florida Vote. Cable News Network. <http://www.cnn.com/2001/ALLPOLITICS/06/08/florida.vote/> (January 29, 2003).

United States Commission on Civil Rights. <http://www.usccr.gov> (January 29, 2003).

Communicable Diseases, Isolation, and Quarantine

■ BRENDA W. LERNER/K. LEE LERNER

Isolation and quarantine remain potent tools in the modern public health arsenal. Both procedures seek to control exposure to infected individuals or materials.

Isolation and quarantine are not synonymous. Isolation procedures are used with patients with a confirmed illness. Quarantine rules and procedures apply to individuals who are not currently ill—but who are known to have been exposed to the illness (e.g., the person has been in the company of a infected person or come in contact with infected materials).

Isolation and quarantine both act to restricts movement and slow or stop the spread of disease within a community. Depending on the illness, patients placed in isolation may be cared for in hospitals, specialized health care facilities, or in less severe cases, at home. Isolation is a standard procedure for active tuberculosis patients. In most cases, isolation is voluntary; however, isolation can be compelled by federal, state, and some local law.

Severe Acute Respiratory Syndrome (SARS) is the first emergent and easily transmissible disease to appear during the twenty-first century. Patients with SARS develop flu-like fever, headache, malaise, dry cough and other breathing difficulties. Many patients develop pneumonia and in 5% to 10% of cases, the pneumonia and other complications are severe enough to cause respiratory failure and death. SARS is caused by a virus that is transmitted mainly from person to person by the aerosolized droplets of virus.

SARS cases provided a test of recent reforms in international health regulations that were designed to increase surveillance and reporting of infectious disease—and to enhance cooperation in preventing the international spread of disease. Although not an act of bioterrorism, because the very same epidemiologic principles and isolation protocols might be used to both determine and initially respond to an act of bioterrorism, intelligence and public heath officials closely monitored the political, scientific, and medical responses to the outbreak. In many regards, the SARS outbreak provided a real and deadly test of world public health responses, readiness, and resources.

Common to both the responses of the 2003 SARS outbreak and a potential deliberate biological attack using pathogens—including smallpox or anthrax—is the need to rapidly develop accurate diagnostic tests, treatment protocols, and medically sound control measures.

At the end of April, 2003, SARS had the potential to become a global pandemic. Scientists, public health authorities, and clinicians around the world struggled to both treat and investigate the disease.

The first known case of SARS was traced to a November, 2002, case in Guangdong province, China. By mid-February, 2003, Chinese health officials tracked more than 300 cases, including five deaths in Guangdong province from what was described at the time as an "acute respiratory syndrome."

Many flu-causing virsues have previously originated from Guangdong Province because of cultural and exotic cuisine practices that bring animals, animal parts, and humans into close proximity. In such an environment, pathogens can more easily leap from animal hosts to humans. The first cases of SARS showed high rates among Guangdong food handlers and chefs.

Chinese health officias initially remained silent about the outbreak and no special precautions were taken to limit travel or prevent the spread of the disease. The world health community had no chance to institute testing, isolation, and quarantine measure that might have prevented the subsequent global spread of the disease.

On Feb. 21, Liu Jianlun, a 64-year-old Chinese physician from Zhongshan hospital (later determined to have unknowingly been a "super-spreader"—a highly contagious infected individual) traveled to Hong Kong despite the fact that he had a fever to attend a family wedding. Epidemiologists subsequently determined that Jianlun passed on the SARS virus to other guests at the Metropole Hotel where he stayed—including an American businessman en route to Hanoi, three women from Singapore, two Canadians, and a Hong Kong resident. Jianlun's travel to Hong Kong and the subsequent travel of those he infected allowed SARS to spread from China to the infected traveler's immediate destinations.

Johnny Chen, the American businessman, grew ill in Hanoi, Viet Nam, and was admitted to hospital. Chen infected 20 health care workers at the hospital including noted Italian epidemiologist Carlo Urbani who cared for him, and who worked at the Hanoi World Health Organization (WHO) office. Urbani first formally identified SARS as a unique disease on February 28, 2003. By early March, 22 hospital workers in Hanoi were ill with SARS.

Unaware of the emerging problems in China, the Urbani report drew increased attention among epidemiologists that in mid-March, Hong Kong health officials had also discovered an outbreak of an "acute respiratory syndrome" among health care workers. Unsuspecting hospital workers admitted the Hong Kong man infected by Jianlun to a general ward at the Prince of Wales Hospital because it was assumed he had a typical severe pneumonia—a fairly routine admission. The first notice that clinicians were dealing with an usual illness came—not from health notices from China of increasing illnesses and deaths due to SARS—but from the observation that that hospital staff, and those subsequently determined to have been in close proximity to the infected persons, began to show signs of illness. Eventually, 138 people, including 34 nurses, 20 doctors, 16 medical students, and 15 other health-care workers at the hospital contracted pneumonia.

One of the most intriguing aspects of the early Hong Kong cases was a cluster of more than 250 SARS cases that occurred in high-rise apartment buildings—many housing health care workers—that provided evidence of a high rate of secondary transmission. Epidemiologists conducted extensive investigations to rule out the hypothesis that the illnesses were related to some form of local contamination (e.g., sewage, bacteria on the ventilation system, etc.). Rumors started that illness was due to cockroaches or rodents, but no scientific evidence supported the hypothesis that the disease pathogen was carried by insects.

Hong Kong authorities then decided that those sufferingfrom the flu-like symptoms would be given the option of self-isolation, with family members allowed to remain confined at home or in special camps. Compliance checks were conducted by police.

One of the Canadians infected in Hong Kong, Kwan Sui-Chu, returned to Toronto and died in a Toronto hospital on March 5. As in Hong Kong, because there were no alerts from China about the SARS outbreak, Canadian officials did suspect that Sui-Chu's son and five health workers had been infected with a highly contagious virus. By mid April, Canada reported more than 130 SARS cases and 15 fatalities.

Increasingly faced with reports that provided evidence of global dissemination, on March 15, the World Health Organization (WHO) took the unusual step of issue a travel warning that described SARS is a "worldwide health threat." WHO officials announced that SARS confirmed and potential cases had been tracked from China to Singapore, Thailand, Vietnam, Indonesia, Philippines, and Canada. Although the exact cause of the "acute respiratory syndrome" had not, at that time, been determined, the official issuance of the precautionary warning to travelers bound for South East Asia about the potential SARS risk severed notice to public health officials about the potential dangers of SARS.

Within days of the WHO warning, SARS cases were reported in United Kingdom, Spain, Slovenia, Germany, and in the United States.

WHO officials were initially encouraged that isolation procedures and alerts were working to stem the spread of SARS, because some countries reporting small numbers of cases experienced no further dissemination to hospital staff or others in contact with the SARS victims. However, in some countries, including Canada, where SARS cases occurred before WHO alerts, SARS continued to spread beyond the bounds of isolated patients.

WHO officials responded by recommending increased screening and quarantine measures that included mandatory screening of persons returning from visits to the most severely affected areas in China, Southeast Asia, and Hong Kong.

On March 29, Urbani, the scientist who first reported a SARS case, died of complications related to SARS.

In early April, WHO took the controversial additional step of recommending against "non-essential travel to

Hong Kong and the Guangdong province of China. The recommendation, sought by infectious disease specialists, was not controversial within the medical community, but caused immediate concern regarding the potentially widespread economic impacts.

World attention—focused largely on the ongoing war in Iraq—began to focus on SARS. Within China, under a new generation of political leadership, a politically unique event occurred when a Chinese official publicly apologized for a slow and inefficient response to the SARS outbreak. Allegations that officials covered up the true extent of the spread of the disease caused the dismissal of several local administrators including China's public health minister and the mayor of Beijing.

Mounting reports of SARS showed an increasing global dissemination of the virus. By April 9, the first confirmed reports of SARS cases in Africa reached WHO headquarters, and eight days later, a confirmed case was discovered in India.

Scientists scrambled to isolate, identify and sequence the pathogen responsible for SARS. Modes of transmission characteristic of viral transmission allowed scientists to place early attention on a group of viruses termed coronaviruses—some of which are associated the common cold. There was a global two-pronged attack on the SARS pathogen, with some efforts directed toward a positive identification and isolation of the virus, and other efforts directed toward discovering the genetic molecular structure and sequence of genes contained in the virus. The development of a genomic map of the precise nucleotide sequence in the virus would be key in any subsequent development of a definitive diagnostic test, the identification of effective anti-viral agents, and eventually a vaccine.

The development of a reliable and definitive diagnostic test was considered of paramount importance in keeping SARS from becoming a pandemic. A definitive diagnostic test would not only allow physicians earlier treatment options, but would also allow the earlier identification and isolation of potential carriers of the virus. Without advanced testing, physicians were forced to rely on less sensitive tests that were unable to identify SARS prior to 21 days of infection—- in most cases too late to effectively isolate the patient .

In mid-April 2003, Canadian scientists at the British Columbia Cancer Agency in Vancouver announced that they that sequenced the genome of the coronavirus most likely to be the cause of SARS. Within days, scientists at the Centers for Disease Control offered a genomic map that confirmed more than 99% of the Canadian findings.

Both genetic maps were generated from studies of viruses isolated from SARS cases. The particular coronavirus mapped had a genomic sequence of 29,727 nucleotides—average for the family of coronavirus that typically contain between 29,000 to 31,000 nucleotides.

Proof that the coronavirus mapped was the specific virus responsible for SARS would eventually come from animal testing, as rhesus monkeys were exposed to the virus via injection and inhalation, and then monitored to determine whether SARS like symptoms developed and if sick animals exhibited a histological pathology (i.e., an examination of the tissue and cellular level pathology) similar to findings in human patients. Other tests, including polymerase chain reaction (PCR) testing helped positively match the specific coronavirus present in the lung tissue, blood, and feces of infected animals to the exposure virus.

Identification of a specific pathogen can be a complex process, and positive identification requires thousands of tests. Testing is conducted with regard to testing Koch's postulates—the four conditions that must be met for an organism to be determined to the cause of a disease. First, the organism must be present in every case of the disease. Second, the organism must be able to be isolated from the host and grown in laboratory conditions. Third, the disease must be reproduced when the isolated organism is introduced into another, healthy host. The fourth postulate stipulates that the same organism must be able to be recovered and purified from the host that was experimentally infected.

Early data indicate that SARS has an incubation period range of 2 to 10 days with an average incubation of about four days. This innoculation period allows the virus to be both transported and spread by an asymptomatic carrier. With air travel, asymptotic carriers can travel to anywhere in the world. The initial symptoms are nonspecific and common to the flu. Infected cases then typically spike a high fever (100.4°F) (38°C) as they develop a cough, shortness of breath, and difficulty breathing. SARS fulminates (reaches it maximum progression) in a severe pneumonia that can cause death.

As of May 1, 2003, no single therapy was demonstrated to show clinical effectiveness and physicians could offer only supportive therapy (e.g. administration of fluids, oxygen, ventilation, etc.).

Before the advent of vaccines and effective diagnostic tools, isolation and quarantine were the principal tools to control the spread of infectious disease. The term "quarantine" derives from the Italian *quarantine* and *quaranta giorni* and dates to the plague in Europe. As a precautionary measure, the government of Venice restricted entry into the port city and mandated that ships coming from areas of plague—or otherwise suspected of carrying plague—had to wait 40 days before being allowed to discharge their cargos.

The legal basis of quarantine in the United States was established in 1878 with the passage of Federal Quarantine Legislation in response to continued outbreaks of yellow fever, typhus, and cholera.

The public discussion of SARS related quarantine in the United States and Europe renewed tensions between the needs for public heath precautions that safeguard society at large and the individual liberties. During the

later years of the nineteenth century and throughout the twentieth century, the law bent toward protecting the greater needs of protecting society. The fact that the poser of quarantine was sometime used to contain and discourage immigration, often made the use quarantine a political and well as medical issue. In other cases such, as with Tuberculosis (TB), quarantine proved effective and courts wielded wide authority to isolate, hospitalize, and force patients to take medications.

States governments within the United States have a general authority to set and enforce quarantine conditions. At the federal level, the CDC's Division of Global Migration and Quarantine, is empowered to detain, examine, or conditionally release (release with restrictions on movement or with a required treatment protocol) individuals suspected of carrying certain listed communicable diseases.

As of April 27, 2003, the Centers for Disease Control and Prevention (CDC) in Atlanta recommended SARS patients be voluntarily isolated, but had not recommended enforced isolation or quarantine. Regardless, CDC and other Public Heath officials, including the Surgeon General, sought and secured increased powers to deal with SARS. On April 4, 2003, U.S. President George W. Bush signed Presidential Executive Order 13295 that added SARS to a list of quarantinable communicable diseases. The order provided heath officials with the broader powers to seek ". . .apprehension, detention, or conditional release of individuals to prevent the introduction, transmission, or spread of suspected communicable diseases…"

Other diseases on the U.S. communicable disease list, specified pursuant to section 361(b) of the Public Health Service Act, include "Cholera; Diphtheria; infectious Tuberculosis; Plague; Smallpox; Yellow Fever; and Viral Hemorrhagic Fevers (Lassa, Marburg, Ebola, Crimean-Congo, and others not yet isolated or named)."

Canada, hit early and much harder by SARS than the U.S., responded by closing schools and some hospitals in impacted areas. Canadian health officials advised seemingly healthy travelers from areas with known SARS cases to enter into a 10-day voluntary quarantine. Once in isolation, individuals were asked to frequently take their temperature and remain separated from other family members. Within a month, almost 10,000 people were in some form of quarantine. Despite the mounting medical and scientific evidence, Canadian government officials, including the Prime Minister Jean Chrétien complained bitterly when, on April 23, the WHO recommended a postponement of non-essential travel to Toronto. Chrétien's government fearful that Canada's economy—already strained from tensions caused by the Chrétien—led government's failure to support the United States during the U.S. war against Iraq—might suffer further economic isolation.

Faced with a more immediate danger and larger numbers of initial cases, an authoritarian government in Singapore was less hesitant in ordering quarantine of victims and those potentially exposed to the virus. One of the three Singapore women initially infected in Hong Kong turned out to be a super-spreader who infected more than 90 people. She recovered, but both her mother and father died of SARS.

Passengers arriving in Singapore coming from other countries with SARS are required to undergo questioning by nurses in isolation gear and then are required to walk through a thermal scanner calibrated to detect an elevated body temperature. Soldiers immediately escort those with elevated temperatures into quarantine facilities. Those subsequently allowed to remain in their homes are monitored by video cameras and electronic wristbands.

By late April 2003, WHO officials had confirmed reports of more than 3,000 cases of SARS from 18 different countries with 111 deaths attributed to the disease. Each new day brought new reports that increased these totals. United States health officials reported 193 cases with no deaths. Significantly, all but 20 of the U.S. cases were linked to travel to infected areas and the other 20 cases were accounted for by secondary transmission from infected patients to family members and health care workers.

In China, fear of a widespread outbreak in Beijing caused a late, but intensive effort to isolate SARS victims and halt the spread of the disease. By the end of April, 2003, schools in Beijing were closed as were many public areas were closed. Despite these measures, SARS cases and deaths continued to mount into late April. Many of China's neighbors considered closing borders to all but essential travel. Health authorities assert that the emergent virus responsible for SARS will remain endemic (part of the natural array of viruses) in many regions of China well after the current outbreak is resolved.

On April 28, 2003, the WHO declared that Vietnam was the first country to control its SARS outbreak, as no new cases were identified in 20 days (twice the usual incubation period). By August 2003, the initial outbreak was contained.

■ FURTHER READING:

PERIODICALS:

Ksiazek, T. G., et al. "A Novel Coronavirus Associated with Severe Acute Respiratory Syndrome." *New England Journal of Medicine* 10.1056 (April 10, 2003): a030781.

Rosenthal, E. "From China's Provinces, a Crafty Germ Spreads." *New York Times.* (April 27, 2003).

ELECTRONIC:

CDC. "Severe Acute Respiratory Syndrome (SARS)." April 3, 2003. <http;//www.cdc.gov/ncidod/sars/isolationquarantine.htm> (April 27, 2003).

World Health Organization. Communicable Disease Surveillance & Response (CSR). April 24, 2003 <http;//www.who.int/csr/sars/en/> (April 27, 2003).

SEE ALSO

Biological Warfare, Advanced Diagnostics
Biological Weapons, Genetic Identification
Bioshield Project
Bioterrorism
Bioterrorism, Protective Measures
CDC (United States Centers for Disease Control and Prevention)
Public Health Service (PHS), United States

Communications System, United States National

JUDSON KNIGHT

The United States National Communications System (NCS) brings together representatives of numerous government departments, using a wide variety of technologies, to provide a single, integrated communications network in the interests of national security. Created in 1962, when Cold War tensions highlighted the need for reliable intra- and international communication, NCS underwent significant changes in 1984, but its core mission—to provide for the communication needs of the president and the national security apparatus—has not altered significantly.

The "Red Telephone" and the reality of NCS. One of the great fixtures of American national-security lore in the modern era is the "Red Telephone." According to legend, this piece of equipment is exactly what its name implies: presumably an ordinary-looking phone colored a standard shade of red—but with a key difference. As it is depicted in movies and the popular imagination, the Red Telephone has no dial or buttons, because it is designed for communication between two sites only: the Oval Office and the Kremlin. In a moment of grave national danger, so the legend goes, the president of the United States picks up the Red Telephone and is instantly connected to his counterpart in Moscow.

The Red Telephone, in fact, is a figment of overactive imaginations. There is no Red Telephone, per se; rather, the president communicates with world leaders through various secure lines, which are maintained by NCS. The latter organization—and, perhaps, the myth of the Red Telephone itself—emerged from a period when the United States came as close as it ever would to nuclear war with the Soviet Union.

Early history. During the two weeks of the Cuban Missile Crisis in October 1962, as President John F. Kennedy spent a great deal of time communicating with Soviet General Secretary Nikita Khrushchev, as well as with other world political and military leaders. Faulty communications technology threatened to further complicate interchanges, and thus exacerbate tensions, a situation that prompted Kennedy to action after the crisis subsided.

The president ordered a study of available security communication capabilities. Subsequently an interdepartmental committee, formed by the National Security Council (NSC), conducted this investigation. The committee recommended the creation of unified system designed to serve the security communication needs of the president and other top political, military, national security, and diplomatic figures. As a result, Kennedy established NCS by a presidential directive signed on August 21, 1963.

Its initial mandate called on NCS to link, improve, and extend the communications technology and capabilities of the relevant federal agencies and departments, with a focus on interconnectivity and the ability to survive ruptures in the communication system. It was a bold mission at a time when telephones had dials, few homes had more than one phone (let alone more than one phone line), and few offices possessed any equipment other than a phone and a typewriter. For the next two decades, the system continued on the model set for it in the early 1960s; then, on April 3, 1984, President Ronald Reagan greatly altered its structure with Executive Order (E.O.) 12472.

NCS participants and NS/EP responsibilities. Under the terms of E.O. 12472, NCS grew from six member agencies and departments to 22, and set about coordinating national security and emergency preparedness (NS/EP) plans to provide communications in the event of crisis or disaster. Today NCS works with all the departments of the federal government, as well as the Central Intelligence, National Security, and Federal Emergency Management agencies; the Joint Staff; the General Services, National Aeronautics and Space, and National Telecommunications and Information administrations; the Nuclear Regulatory and Federal Communications commissions; the Federal Reserve Board; and the United States Postal service.

A particularly notable example of a department with critical NS/EP responsibilities is the Department of Defense (DoD). Among the telecommunications assets it oversees are the Advanced Research Projects Agency (ARPA) computer network; the Direct Communications Link (the Washington-Moscow hotline that constitutes the real-life "Red Telephone"), the Defense Satellite Communications System; the Worldwide Military Command and Control System; and several others.

Along with the other 21 members, DoD is represented on NCS through the Committee for National Security and Emergency Preparedness. The committee, formerly known as the NCS Committee of Principals, was established by E.O. 12472, and renamed October 2001 according to E.O. 13231, "Critical Infrastructure Protection in the Information Age." In late 2002, NCS was slated for inclusion in the new Department of Homeland Security.

■ FURTHER READING:

BOOKS:

National Communications System, 1963–1998: 35th Anniversary. Arlington, VA: National Communications System, 1998.

National Communications System for Emergency Response Personnel. Washington, D.C.: Government Printing Office, 2001.

PERIODICALS:

Caterinicchia, Dan. "When Duty Calls." *Federal Computer Week* 16, no. 36 (October 7, 2002): 25–26.

McConnell, Bruce. "Telecom Role Model." *Federal Computer Week* 16, no. 40 (November 11, 2002): 27.

ELECTRONIC:

National Communication System. <http://www.ncs.gov> (January 29, 2003).

SEE ALSO

Cuban Missile Crisis
National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States
NSC (National Security Council)

Comprehensive Radiation Sensors (CRS).

SEE *Environmental Measurements Laboratory.*

Comprehensive Test Ban Treaty (CTBT)

■ LARRY GILMAN

The Comprehensive Test Ban Treaty (CTBT) is an international agreement designed to end the testing of nuclear explosives. As of March, 2003, the United States is one of the 166 states that have signed the treaty, but the CTBT will only "enter into force" (i.e., take on the force of law for all ratifying states) when 44 "nuclear-capable" countries specifically listed in the treaty have all ratified the treaty. Of these 44 states, India, Pakistan, and North Korea have refused to sign, and 13 (including the U.S.) have signed but not ratified.

Nuclear Testing. Nuclear testing is the detonation of nuclear weapons for test purposes. Testing is needed to verify new bomb designs and to observe the effects of nuclear weapons (e.g., types and amounts of radiation produced). The first nuclear test, codenamed Trinity, was conducted by the United States on July 16, 1945, near Alamagordo, New Mexico. Since that time, six other nations—China, France, India, Pakistan, the Soviet Union, and the United Kingdom—have conducted nuclear tests. (Some experts assert, based on U.S. intelligence satellite data, that Israel and South Africa may have conducted a joint nuclear test at sea in 1979.) The most recent nuclear test was conducted by India, on May 30, 1998.

Nuclear tests can be conducted underground, under water, in space, or in the atmosphere. No nuclear weapon has ever been tested in space, but approximately 2050 have been detonated in various environments on Earth. Before 1962, most tests were conducted in the atmosphere; the U.S. conducted 193 atmospheric tests between 1946 and 1962, and the Soviet Union conducted 142 such tests between 1948 and 1962. During the late 1950s and early 1960s, these atmospheric tests became a global political concern because of the radioactive substances they released into the air (fallout). The most problematic of these byproducts was iodine 131, a radioactive isotope of iodine. Iodine 131, which is chemically identical to ordinary iodine, can settle on grass, be consumed by cows, concentrate in milk, and further concentrate in the thyroid glands of human beings who drink the milk, especially children. Atmospheric testing in the 1950s and early 1960s released large quantities of iodine 131 into the atmosphere; in 1997, the U.S. National Cancer Institute estimated that 160 million people in the United States had been exposed to some level of iodine 131 from U.S. nuclear tests conducted in Nevada, and that these exposures would, over time, cause 30,000–75,000 cases of thyroid cancer. Although the extent of fallout exposure was not known at the time to be this large, public sentiment against testing became strong. As a result, the U.S., United Kingdom, and Soviet Union signed the Limited Test Ban Treaty on July 25, 1963. The Limited Test Ban Treaty forbade the detonation of nuclear weapons in the air, the sea, or space. The treaty went into effect on October 11, 1963; both superpowers conducted a flurry of atmospheric tests before the deadline, after which testing moved underground. The U.S. and Soviet Union had attempted to negotiation a "comprehensive" test ban treaty in 1963—that is, an agreement to ban *all* nuclear tests—but could not come to agreement on technical details. Also, military officials of both countries opposed a comprehensive test ban, wishing to continue developing new varieties of nuclear weapon. The Limited Test Ban Treaty committed its signatories to continuing to seek, in the words of the treaty's first article, "the discontinuance of all test explosions of nuclear weapons for all time"—in other words, a comprehensive test ban treaty.

The next legal step toward this goal occurred in 1974, when the Treaty on Underground Nuclear Weapons Tests (also known as the Threshold Test Ban Treaty) was signed by the U.S. and Soviet Union. This treaty forbade either

nation to conduct an underground test of any nuclear weapon with an explosive force greater than 150 kilotons (i.e., equivalent to that of 150,000 tons of TNT [trinitrotoluene]). The treaty has been observed by both parties since 1974, but did not enter into full legal force until December 11, 1990, when U.S. concerns about verification had been met. (Verification of a nuclear test ban treaty requires the collection of seismic and other data to assure that no test has been secretly performed that exceeds the limits of the agreement.)

In 1991, Soviet President Mikhail Gorbachev announced that the Soviet Union would unilaterally cease nuclear testing for one year. In 1992, a bill was passed by both houses of the U.S. Congress mandating a unilateral U.S. testing moratorium to respond to the Soviet testing halt. This bill was signed into law by President George H. Bush on October 2, 1992. Neither Russia (the nuclear inheritor-state of the Soviet Union) nor the U.S. have, as of early 2003, conducted any nuclear tests since the beginnings of these moratoria.

Multinational negotiations toward a CTBT began in Geneva, Switzerland on January 25, 1994. In June 1995, while CTBT negotiations were still under way, France announced that it would resume nuclear testing. This decision aroused official protest from many governments, including that of the United States, and a worldwide boycott of French-made goods. China, too, was continuing to perform sporadic nuclear tests during this period, and on June 20, 1996 India announced that it would not sign the CTBT. Nevertheless, on September 10, 1996, the CTBT was approved by a 158-to-3 vote of a special session of the United Nations General Assembly. President Clinton signed the CTBT for the U.S. on September 24, 1996, and was soon followed by representatives of many other states, including China, the United Kingdom, France, and Russia.

Since signing of the CTBT began in 1996, the only nuclear explosions to have taken place have been the nuclear tests by Pakistan and India in 1998, a total of 11 explosions.

Ratification. President Clinton's 1996 signature did not make the CTBT binding law for the U.S. U.S. commitment to such a treaty, like that of most other states, occurs in two steps: first "signature" (by a president or qualified ambassador), then "ratification" (formal agreement to the treaty by the legislative body of the state, e.g., Parliament or Congress). Many states obey the terms of treaties that they have signed but not yet ratified, while reserving to themselves the right to begin disregarding the provisions of the treaty at any time.

The U.S. signed the CTBT in 1996, but the Senate refused in 1999 to ratify (51 to 48). As of March 2003, United States president George W. Bush's administration has stated that it intends to continue observing the CTBT's ban on testing, but will not support ratification of the CTBT. Also, administration officials have indicated that the U.S. may, at some time, withdraw from the treaty altogether. The Bush administration's Nuclear Posture Review of 2002, a document designed to guide nuclear-weapons strategy for years to come, has recommended that the U.S. develop a class of relatively low-yield nuclear weapons that would dive deep into the ground (probably at thousands of miles per hour) before exploding; the goal of such weapons, termed Robust Nuclear Earth Penetrators or "bunker busters," would be to destroy deeply buried targets. In order to develop such devices, the U.S. would have to resume testing of nuclear weapons.

Verification. Verification of the CTBT is accomplished by a global system of sensors termed the International Monitoring System (IMS). The IMS consists of sensors that detect bomb-type vibrations in the Earth, oceans, and air (termed seismic, hydroacoustic, and infrasonic vibrations, respectively) and that test the air for radioactive substances (radionuclides) which would reveal the occurrence of nuclear tests. The IMS is designed to accomodate 170 seismic monitoring stations, 11 hydroacoustic stations, 60 infrasound stations, and 80 radionuclide-detecting stations. These automatic sensors, deployed to provide global coverage, will report their data in real time via satellite to a monitoring center in Vienna, Austria, the International Data Centre (IDC). The IMS and IDC are run by an independent group, the Comprehensive Nuclear-Test-Ban Treaty Organization. (Since the CTBT is not officially "in force," the Comprehensive Nuclear-Test-Ban Treaty Organization has been funded by nonbinding international agreement.) Construction of the IMS began in 1997. Regardless of the legal future of the CTBT itself, the IMS will probably continue to provide high-quality, publicly-available information about nuclear testing worldwide.

■ FURTHER READING:

BOOKS:

Galindo, Marta and John Newton. "Installation of New Stations in the Hydroacoustic Monitoring Network for the Comprehensive Test Ban Treaty," in proceedings from the *Oceans 2000 MTS/IEEE Conference and Exhibition,* IEEE, 797–801, 2000.

ELECTRONIC:

"The Comprehensive Nuclear Test-Ban Treaty." United States Department of State. January 10, 2001. <http://www.state.gov/www/global/arms/treaties/ctb.html> (March 10, 2003).

"The Limited Nuclear Test-Ban Treaty." United States Department of State. [No date on Web page.] <http://www.state.gov/t/ac/trt/4797.htm> (March 10, 2003).

SEE ALSO

Antiballistic Missile Treaty
Nuclear Weapons
Start I Treaty
START II

Computer and Electronic Data Destruction

Computers are often the repository of an astounding amount of information. Even in a stand-alone computer that is not linked to the Internet, millions of conventional pages of text and images can be stored in the hard drive and on peripherals, such as a floppy disk or on a compact disk (CD).

For sensitive operations, the security of computer data must be ensured. This is particularly true when data is erased. The convention version of data removal involves the deletion of a file, by the movement of the file to a "garbage can" (i.e., the "Recycling Bin" in the various Windows operating systems). This form of deletion instructs the computer to use the slice of hard or floppy disk space for something else. Eventually, the file will be overwritten. But, until that occurs, the information is recoverable.

The true cleaning of a hard or floppy disk involves overwriting the actual data. Computer data is recorded as a series of 0s and 1s. Irrevocable erasure of data can be achieved by rewriting the relevant sector of a drive with 0's. Others advocate for a hexadecimal pattern (i.e., 110000001) followed by a "second pass", which overwrites the hexadecimal pattern as 00111110. In this way, every unit of information has been changed at least once.

True cleaning of a CD is also possible. The data layer that was previously "burned" onto the CDs surface can be removed and ground into fine powder. The original polycarbonate disk that remains contains no trace of the original data. The CD, which is rendered unusable, can be conventionally disposed of.

Destruction can also be a brute force physical process. For example, a hard drive can be physically damaged so that it cannot be read, even if installed into another computer. Floppy disks can be cut apart. Thus, while information may still reside on the drive, that information is essentially destroyed. Disks and CDs can even be melted down.

A number of vendors offer data destruction services to those having concerns about the sensitivity and vulnerability of their data. Government agencies usually have in-house staff and facilities, so that sensitive information does not pass into unauthorized hands, even during the destruction process.

FURTHER READING:

BOOKS:

Bosworth, Seymour and Michael E. Kabay. *Computer Security Handbook.* New York: John Wiley & Sons, 2002.

Eoghan, Casey. *Digital Evidence and Computer Crime.* New York: Academic Press, 2000.

Kruse, Warren G., II., and Jay G. Heiser. *Computer Forensics: Incident Response Essentials.*Boston: Addison Wesley Professional, 2001.

SEE ALSO

Computer Virus
Electronic Communication Intercepts, Legal Issues
Information Security

Computer Fraud and Abuse Act of 1986

ADRIENNE WILMOTH LERNER

The United States Computer Fraud and Abuse Act of 1986 served to define criminal fraud and abuse for computer crimes on the federal level. The act specified a misdemeanor crime for the trafficking and misuse of passwords, and two felony offenses for unauthorized access to federal information systems and private computers deemed to have a "federal interest." The act removed several legal ambiguities that surrounded computer information theft, such as the lack of specific legislation mentioning computers and the slightness of legal precedence in such cases.

Computer data systems of varying sorts had been used by the United States government since the 1960s. In the early 1980s, the first computers for business and home use were available in the marketplace. This expanse of the computer-owning and software-literate population forced the government to begin finding ways to protect data, either through encryption or protective barrier mechanisms around certain files. With the advent of intranets and computer-to-computer communication through telephone lines, hacking, or the breaking into other computer systems, became more commonplace. In 1981, a computer-savvy 24-year-old named Ian Murphy hacked into several government systems, including the White House switchboard. Murphy used the switchboard to order various products before turning his attention to cracking the codes protecting sensitive military files. Murphy was arrested, but prosecutors did not have the legal recourse to try him for computer crimes, as no such laws existed. Murphy was eventually convicted of theft and knowingly receiving stolen goods.

By 1982, Congress began collecting data on computer crime, and gathering testimony from computer fraud victims. Most of the victims were major corporations who did not want their security breeches and vulnerability to become public knowledge. Not only was it easy for random hackers to crack a system, but also corporations could hack into the data systems of rival companies, engaging in corporate espionage. After five years, Congress introduced the Computer Fraud and Abuse Act of 1986. The bill

passed decisively. That same session, the Electronic Communication Privacy Act of 1986 was passed, criminalizing the seizure and interception of digital messages and communication signals.

In January of 1989, Herbert Zinn was the first person to be convicted under the Computer Fraud and Abuse Act. As a teenager, Zinn broke into computer systems at the Department of Defense, wreaking havoc with several hundred files. Zinn was sentenced to nine months in prison and fined; he would have possibly received a harsher judgment if he had been over eighteen years-old at the time of the crime.

Since its inception, the Computer Fraud and Abuse Act has weathered changing technology and the development of the Internet. However, computer crime is once again on the rise, and only a fraction of victims report these crimes. Subsequent court proceedings and legislation such as the Compute Abuse Amendments Act of 1994 have provided specific wording criminalizing the promulgation of computer viruses and other damaging code.

SEE ALSO

Computer Hackers
Information Security

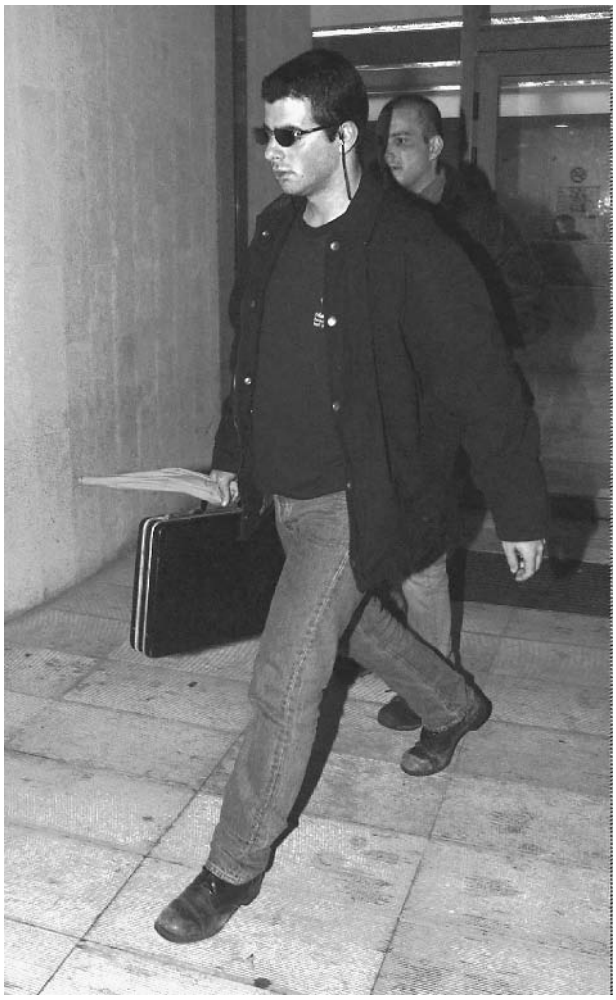
Computer Hackers

Computer hackers are people who gain remote access (typically unauthorized and unapproved) to files stored in another computer, or even to the operating system of the computer. In the 1950 and 1960s, hackers were motivated more by a desire to learn the operating characteristics of a computer than by any malicious intent. Indeed, in those days hackers were often legitimate computer programmers who were seeking ways of routing information more quickly through the then-cumbersome operating system of computers.

Since then, however, computer hacking has become much more sophisticated, organized, and, in many cases, illegal. Some hackers are motivated by a desire to cripple sensitive sites, make mischief, and to acquire restricted information.

In the late 1990s, several computer hackers attempted to gain access to files in the computer network at the Pentagon. The incidents, which were dubbed Solar Sunrise, were regarded as a dress rehearsal for a later and more malicious cyber-attack, and stimulated a revamping of the military's computer defenses. In another example, computer hackers were able to gain access to patient files at the Indiana University School of Medicine in February 2003.

The threats to civilian privacy and national security from computer hackers was deemed so urgent that the U.S. government enacted the Cyber-Security Enhancement Act in July 2002, as part of the Homeland Security measures in the wake of the terrorist attacks on September 11, 2001. Under this legislation, hackers can be regarded as terrorists, and can be imprisoned for up to 20 years.



Ehud Tenebaum leaves a police station near Tel Aviv, Israel, under house arrest with two other Israeli teenagers in 1998 pending charges for the most organized hacker attack ever perpetrated on the Pentagon's computer system. AP/WIDE WORLD PHOTOS.

One tool that a hacker can use to compromise an individual computer or a computer network is a virus. Depending on their design and intent, the consequences of a virus can range from the inconvenient (i.e., defacing of a Web site) to the catastrophic (i.e., disabling of a computer network). Within a few years during the 1990s, the number of known computer viruses increased to over 30,000. That number is now upwards of 100,000, with new viruses appearing virtually daily.

Despite the threat that they can pose, computer hackers can also be of benefit. By exposing the flaws in a computer network, hackers can aid in the redesign of the

Convicted computer hacker Kevin Mitnick, right, after being released from the Federal Correction Institute in Lompoc, California, in 2000, remained under a judge's order barring him from using a computer for a further three years. AP/WIDE WORLD PHOTOS.

system to make information more inaccessible to unauthorized access.

■ FURTHER READING:

BOOKS:

McClure, Stuart, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets and Solutions,* 4th ed. Emeryville, CA: McGraw-Hill Osborne Media, 2003.

Spitzner, Lance. *Honeypots: Tracking Hackers.* Boston: Addison Wesley Professional, 2002.

Wang, Wallace. *Steal This Computer Book 3: What They Won't Tell You About the Internet.* San Francisco: No Starch Press, 2003.

Warren, Henry S., Jr. *Hacker's Delight.* Boston: Addison Wesley Professional, 2002.

SEE ALSO

Computer Fraud and Abuse Act of 1986
Cyber Security
Internet Tracking and Tracing

Computer Hardware Security

■ BRIAN HOYLE

A phenomenal amount of information now resides on computers. Individual computers as well as computers that communicate with each other in geographically-restricted local networks as well as globally, via the Internet, contain billions of pages of text, graphics, and other sources of information. Without safeguards, this information is vulnerable to misuse or theft.

Computer security can takes two forms. Software security provides barriers and other cyber-tools that protect programs, files, and the information flow to and from a computer. Hardware security protects the machine and peripheral hardware from theft and from electronic intrusion and damage.

Physical on-site security can be as easy as confining mission-critical computers to a locked room, and restricting access to only those who are authorized. This also holds for servers, which are computers that function as a central routing point for information to and from the

networked computers and the Internet. Many personal computer users pay to have this service provided by an Internet service provider (ISP). However, having an outside provider can generate security threats and can be disruptive if the ISP ceases operation. Nowadays, many corporations opt to establish an in-house ISP. In this way the security of the corporate server is under direct control.

Computers also have an internal form of a lock and key. A security password that is needed to gain access to all of a computer's functions can be stored on a chip known as the BIOS chip. Unfortunately, a dedicated thief can easily circumvent this hardware security feature, by removing the hard drive and putting it into another computer with a different BIOS chip.

With the exploding popularity of the Internet, hardware security has been extended to this electronic realm. Computers that are connected to the Internet are vulnerable to remote access, sabotage, and eavesdropping unless security measures are in place to buffer the computer from the outside electronic world.

Many corporations whose computers are linked to one another, employ a local version of the Internet. An Intranet or Local Area Network allows the exchange of information between the linked computers, while at the same time enabling the erection of hardware and software (i.e., firewalls) that screen information flowing to and from the Internet. Remote users of the internal network, such as telecommuting employees, can be protected through what is known as a virtual private network (VPN). A VPN establishes a protected communications link across a public network between the remote computer and the computers physically linked in the local network.

The individual computers that are linked in a network, and the dedicated devices that route information back and forth, are also known as nodes. The security measures that have been discussed above also function to safeguard nodes.

At the core of a network is a device called the hub. The hub exchanges the information between all of the connected computers. As such, it is key to a network. A hub should be kept away from high traffic areas, and preferably in a secure room. This restricts tampering.

While a hub relays information indiscriminately from computer to computer, a device called a switch is more selective. Information can be sent to one user computer but not to another. The use of a switch allows a network administrator to control the information flow to authorized viewers, which can be a security issue.

Fluctuations in the power supply can play havoc with computers. For example, a blackout or brownout can cause a computer to shut down abruptly. Information that is stored only in short-term memory will be lost. As well, the fluctuation can physically damage computer components. The use of a surge protector guards against electrical spikes and drops. An uninterruptible power supply (UPS) can also be hooked up to a computer. A UPS is essentially a battery that will power the computer in the event of a power outage. This can provide time for information to be saved and for a computer to be shut down correctly.

FURTHER READING:

BOOKS:

Bentley, Tom, and Jon Hastings. *Safe Computing: How to Protect Your Computer, Your Body, Your Data, Your Money and Your Privacy in the Information Age.* Concord, CA: Untechnical Press, 2000.

Bishop, Matt. *Computer Security: Art and Science.* Boston: Addison Wesley Professional, 2002.

Luber, Alan D. *PC Fear Factor: The Ultimate PC Disaster Prevention Guide.* Indianapolis: Que, 2002.

SEE ALSO

Computer Keystroke Recorder
Cyber Security

Computer Keystroke Recorder

A computer keystroke recorder, as its name suggests, is simply a device for sequentially recording all the keys pressed on a computer keyboard. Keystroke recorders are available commercially, but much more sophisticated devices are used by government agencies such as the Federal Bureau of Investigation (FBI).

Also called a keystroke logger, key logger, or keylogger, a computer keystroke recorder is a program that runs in the background as the computer operates, recording all key depressions or strokes. Some such devices are plugged in manually, but the more effective kind operate through means of a computer program. The latter may be introduced to the computer by means of a trojan horse, a remotely inserted program that operates much like a virus.

An example of an FBI keystroke-recording trojan is Magic Lantern, which made it possible to log keystrokes by means of a computer virus sent to a remote user's machine. The revelation of the device's use, reported by MSNBC News on December 12, 2001, invoked the ire of civil libertarians, as well as computer companies whose assistance the government sought. According to the MSNBC report, vendors of anti-virus software refused to cooperate with FBI requests to bypass special government-created trojans and viruses used for security purposes.

The FBI and its computer keystroke recording technology also made the news in late 2001 due to its involvement in *United States v. Scarfo.* The first known case of its kind, *Scarfo* involved a request by the defense to allow analysis of the keystroke recording technique used to gather evidence against the defendant. The government

claimed protection of classified information under the Classified Information Procedures Act (CIPA), and the court granted the government's motion.

FURTHER READING:

PERIODICALS:

Hentoff, Nat. "The FBI's Magic Lantern." *Village Voice.* 47, no. 22 (June 4, 2002): p. 35.

Huleatt, Richard S. "EPIC May Never Learn Details of Government Keystroke Monitor." *Information Intelligence Online Newsletter* 22, no. 10 (October 2001): 5–6.

ELECTRONIC:

FBI Confirms "Magic Lantern" Exists. MSNBC. <http://www.msnbc.com/news/671981.asp> (January 27, 2003).

SEE ALSO

Classified Information
Computer Hardware Security

Computer Modeling

JUDSON KNIGHT

Modeling, in the technical use of the term, refers to the translation of objects or phenomena from the real world into mathematical equations. Computer modeling is the representation of three-dimensional objects on a computer, using some form of software designed for the purpose. Among the uses of computer modeling are war games and disaster simulations, situations in which computers offer a safe, relatively inexpensive means of creating or re-creating events without the attendant loss of life or property.

Mathematics, Computers, and Modeling Software

Mathematical modeling dates to advances in geometry and other disciplines during the late eighteenth century. Among these was the descriptive geometry of French mathematician Gaspard Monge, whose technique was so valuable to Napoleon's artillery that it remained a classified defense secret for many years. Nearly one and a half centuries later, at the end of World War II, mathematicians and scientists working for the United States war effort developed a machine for readily translating mathematical models into forms easily grasped by non-mathematicians.

That machine was the computer, and during the last two decades of the twentieth century, varieties of three-dimensional modeling software proliferated. These included any number of computer animation and gaming packages, as well as varieties of computer-aided design/computer-aided manufacturing (CAD/CAM) systems. CAD allowed engineers and architects, for instance, to create elaborate models that allowed them to "see into" unbuilt structures, and to test the vulnerabilities of those structures without risking lives or dollars.

One notable variety of three-dimensional software is virtual reality modeling language, abbreviated VRML and pronounced "ver-mal." Necessary for representing three-dimensional objects on the World Wide Web (that portion of the Internet to which general users are most accustomed), VRML creates a virtual world, or hyperspace, that can be viewed through the two-dimensional computer screen. By pressing designated keys, the user is able to move not only up, down, right, and left, but forward and backward, within this virtual world.

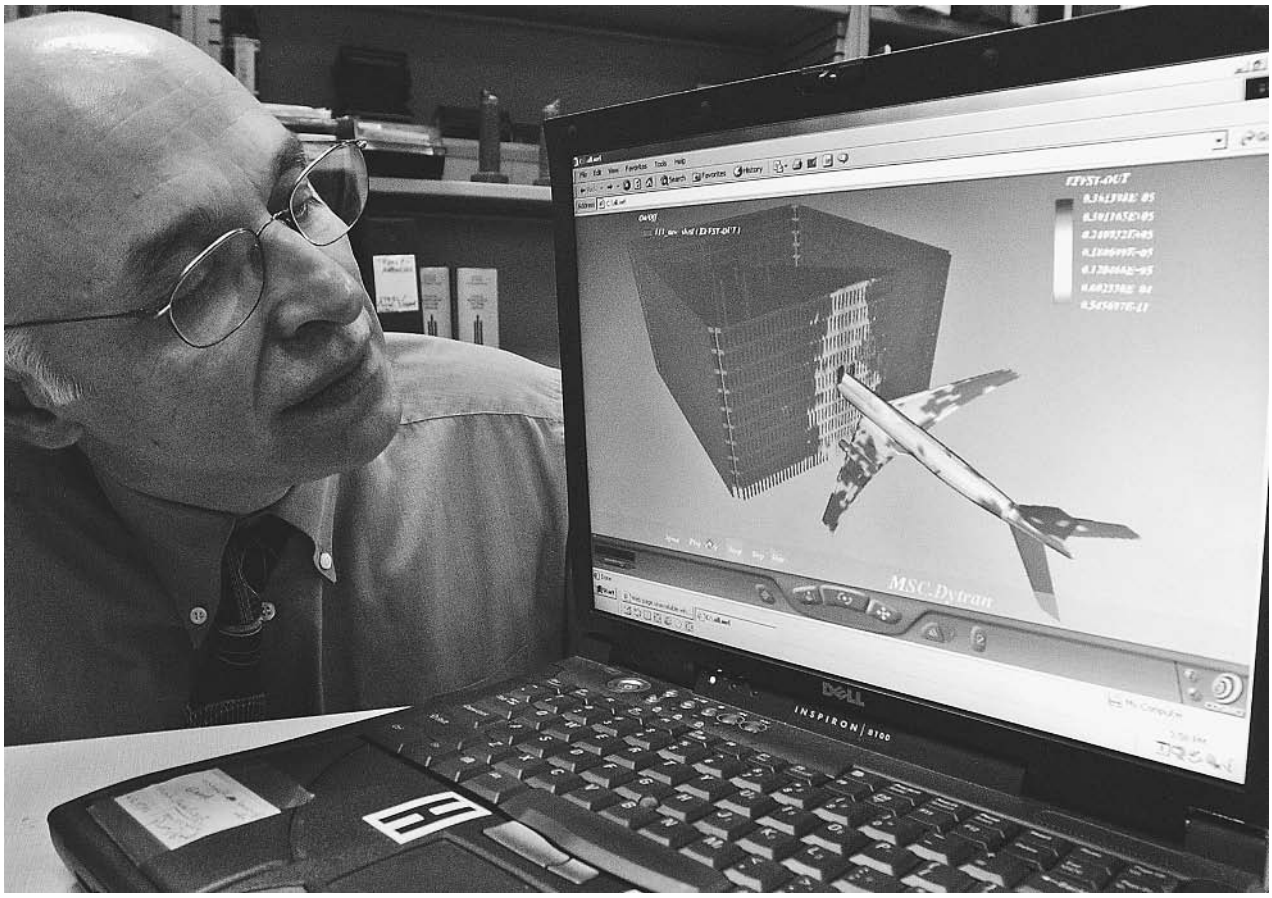
Disasters, Wars, and Other Simulations

After the space shuttle *Columbia* crashed on February 1, 2003, analysts at the National Aeronautics and Space Administration (NASA) used modeling software applied by the National Transportation Safety Board (NTSB) for studying crashes. In applications such as those for the NASA and NTSB studies, the purpose is to understand not only what happened, but how and why it happened, and what caused it.

The more data available on a disaster, the better the model, and this in turn gives investigators more accurate tools for analysis. In the end, however, there is no substitute for human reasoning. For example, an NTSB simulation of the Swissair Flight 111 crash in September 1998 tracked the course of a fire from the cockpit that eventually brought down the plane, but it did not explain what caused the fire.

Still, the simulation is invaluable inasmuch as it provides human minds with an extraordinarily accurate and vivid source of information as to the exact sequence of events that took place during a disaster. NASA analysts used computer modeling to study the first great shuttle disaster, that of *Challenger* in 1986, but the technology of 2003 was vastly superior. Not only was a $2,000 computer capable of running simulations that required a $75,000 machine 17 years earlier, but advances in graphics—spurred, ironically, by the seemingly frivolous demands of gaming and the movies—had resulted in a vastly more accurate picture of what happened.

War games and terror simulations. The connection between entertainment and simulation in general, as well as computer modeling technology in particular, has not been lost on the U.S. security and defense leadership. In the immediate aftermath of the September 11, 2001, terrorist attack, federal officials brought together a team that included David Fincher, director of *Seven* and *Fight Club;* Steven E.



A steel structure expert at the University of California, Berkeley, studies a three-dimensional computer model of the airliner hitting the 96th floor of the World Trade Center. AP/WIDE WORLD PHOTOS.

De Souza, screenwriter for *Die Hard;* and Spike Jonze, director of *Being John Malkovich.* The assignment placed before these creative minds was one ideally suited to Hollywood: to imagine scenarios in which terrorists attacked the United States.

These scenarios, along with other forms of input, have helped form the basis for simulations by groups such as the Institute for Creative Technologies (ICT), a research center at the University of Southern California at Los Angeles. ICT is one of many entities in which the federal government invests nearly $100 million a year for the purpose of developing military simulations—studies that, unlike the disaster models for NTSB or NASA, are concerned not so much with what has happened as with what *could* happen. The Department of Defense also has its own simulation think tanks, including the U.S. Army Simulation, Training, and Instrumentation Command, known as STRICOM.

Simulations developed by ICT are mind-boggling in their degree of verisimilitude. The "virtual humans" on screen are not automatons; rather, they have been programmed with personalities and emotions, like characters in a movie. Cutting-edge computer technology makes it possible to even simulate smells. In an unusual merger of public and private sectors, ICT has sold commercial versions of games it co-produced with the U.S. Army.

The purpose of simulations produced by ICT and others involved in computer modeling goes far beyond mere entertainment: at a fraction of the expense and risk involved in war games involving real troops and equipment, commanders and their subordinates can study and learn from battle. Computer modeling also makes it possible to study dozens of different terror, but without any human or financial cost. By providing laboratories for instruction, simulations may prevent losses in real situations.

FURTHER READING:

BOOKS:

Danby, J. M. A. *Computer Modeling: From Sports to Spaceflight—From Order to Chaos.* Richmond, VA: Willmann-Bell, 1997.

Emmer, Michele. *The Visual Mind: Art and Mathematics.* Cambridge, MA: MIT Press, 1993.

Modeling and Simulation: Linking Entertainment and Defense. Washington, D.C.: National Academy Press, 1997.

ELECTRONIC:

Lee, David B., Lt. Col., USAF. "War Gaming: Thinking for the Future." *Airpower Journal* <http://www.airpower.maxwell.af.mil/airchronicles/apj/3sum90.html> (March 14, 2003).

U.S. Air Force Wargaming Institute. <http://www.cadre.maxwell.af.mil/wargame/main.htm> (March 14, 2003).

U.S. Army Program Executive Office for Simulation, Training, and Instrumentation. <http://www.stricom.army.mil/> (March 14, 2003).

SEE ALSO

Internet
NASA (National Air and Space Administration)
NTSB (National Transportation Safety Board)
Supercomputers

Computer Security Act (1987)

The Computer Security Act of 1987 is the first major United States government effort to legislate protection and defense for unclassified information in government-related computer systems. The act mandates the National Bureau of Standards to develop and implement procedures that improve the security and privacy of sensitive material and creates a means for establishing minimum acceptable security practices.

The CSA arose out of congressional concerns about computer database vulnerability and executive branch over-zealousness on computer matters. While the Department of Defense argued that unclassified information could be pieced together to create a national security threat, President Ronald Reagan's 1984 National Security Decision Directive 145 set information safeguards at such a high level that private computer data companies loudly complained to legislators about federal scrutiny of their customers. Congress decided to assess the vulnerability of government computers, develop technical and management strategies against access to sensitive information, and establish mandatory training for employees in computer and communication security. The resulting CSA also designates the creation of a twelve-member advisory board that meets at least three times per year and reports to the Secretary of Commerce, the Office of Management and Budget, the National Security Council, and Congress.

While the CSA is designed to prevent the release of sensitive information, the law specifically forbids any federal agency to withhold information requested under the Freedom of Information Act (FOIA). It also does not authorize any agency to limit, restrict, or regulate the collection, disclosure, use, or sale of privately owned or public domain information. Despite this provision journalists have encountered increasing difficulty obtaining FOIA access to federal material stored in computer databases. Librarians have also observed that the Department of Defense, Department of Energy, and NASA release fewer documents to the public than in the years prior to CSA.

In light of the George W. Bush administration's concern with secrecy as an element of national security, the CSA will likely continue to be used to limit public access to government information.

■ FURTHER READING:

BOOKS:

Blyth, Andrew and Gerald L. Kovacich. *Information Assurance: Surviving in the Information Environment.* London: Springer, 2001.

Martin, Shannon E. *Bits, Bytes, and Big Brother: Federal Information Control in the Technological Age.* Westport, CT: Praeger, 1995.

SEE ALSO

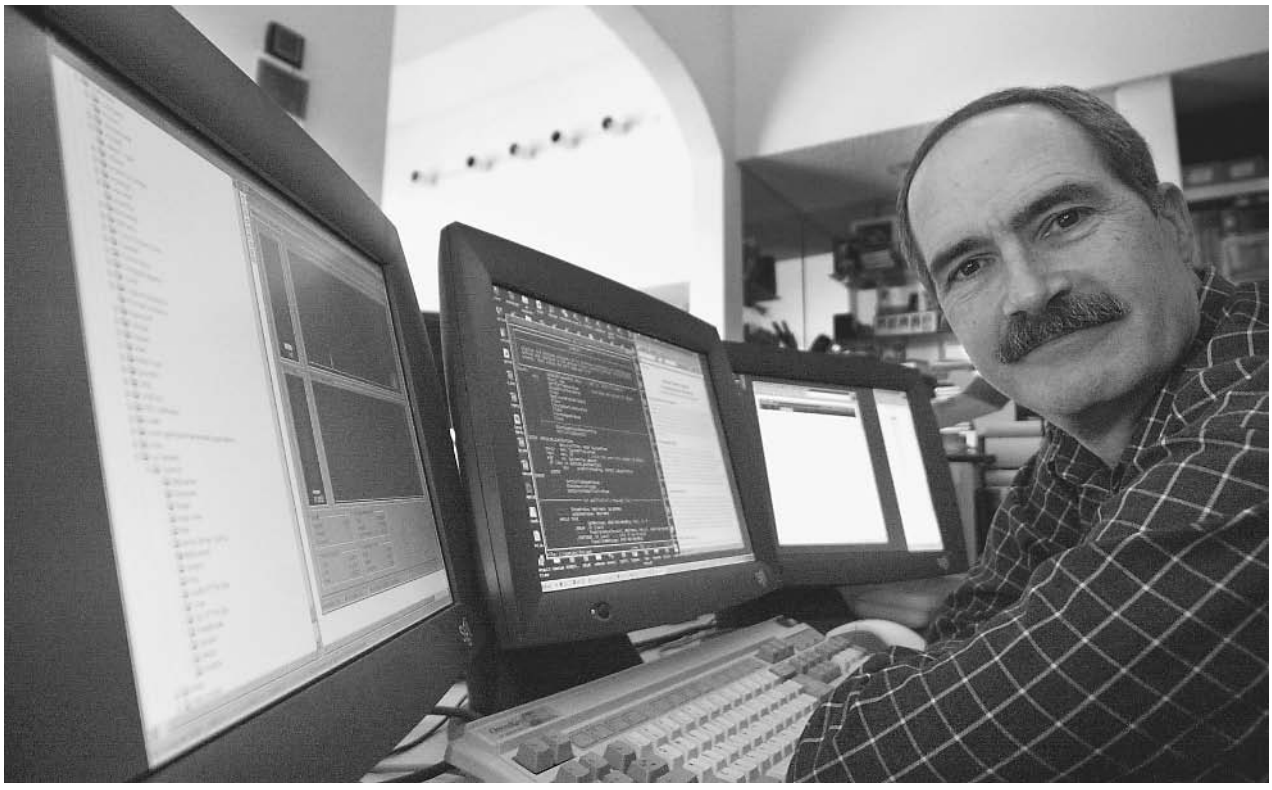
Bush Administration (2001–), United States National Security Policy
Classified Information
Commerce Department Intelligence and Security Responsibilities, United States
Computer Fraud and Abuse Act of 1986
Computer Hackers
Computer Hardware Security
DOD (United States Department of Defense)
DOE (United States Department of Energy)
FOIA (Freedom of Information Act)
Information Security
NSC (National Security Council)
Reagan Administration (1981–1989), United States National Security Policy

Computer Software Security

■ BRIAN HOYLE

Computer software security refers to the use of software to prevent damage to computer files, programs, and operating systems, as well as to monitor a personal computer (PC) or laptop for theft.

Anti-virus software. A recommended feature for any computer that is connected to the Internet is software that protects the computer from viruses. Like biological viruses, computer viruses need the machinery of another host, in this case a computer, to make new copies of themselves and infect another host computer. There are upwards of



Computer security researcher Steve Gibson is seen in his home office in Laguna Hills, California, in April, 2002. Two years prior, Gibson was testing intrusion-detection software when he suddenly found a program running on his computer that he had unknowingly installed. The hidden program secretly tagged along with another program and monitored his Internet habits. AP/WIDE WORLD PHOTOS.

100,000 known viruses, with new viruses being detected literally every day.

Viruses can enter computers via different routes. A common route is as an attachment to an email. When the email is opened the virus is triggered to disrupt whatever computer code it has been targeted towards. Viruses that target email addresses can distribute themselves to other computer very quickly. An infamous example is the "Love" virus, which infected millions of computers worldwide within hours of its release in May 2000.

There are a wide variety of anti-virus software programs available that will recognize, quarantine and destroy many of these viruses. Anti-virus programs need to be updated frequently (often accomplished automatically "on-line" with some vendors products) to keep pace with the appearance of new viruses.

Theft. Next to viruses, theft represents the biggest security issue for computer users. Various hardware options are designed to lessen the chance of theft. Anti-theft software is also available. There are several software programs that aim to lessen the usability, and so the appeal, of a stolen computer (particularly laptop computers). In one setup, a registered identifier number is beamed out when the stolen computer is hooked up to the Internet. Proprietary software can detect and even track the location of the sending computer. Another strategy uses motion-sensing software that is adjusted to the motion patterns of the normal user. A different range of motions that are uncharacteristic of the principle user can trigger an audio alarm. As well, the computer is triggered to shut down and reboot. The user then needs to supply a complicated password to use the computer and even to read the scrambled files (see below) from the hard drive. This protection occurs even when the computer is shut off.

Data encryption and ownership. Encryption is the scrambling of the data so as to make the data undecipherable. Encryption programs can scramble the data that is resident in the computer as well as data sent to another computer via email. The message can be reassembled to the original format if the receiving computer has an encryption program installed.

With contracts being sent over the Internet, the ownership and legal status of such information has become an important issue. Digital signatures can be affixed to a document sent via the Internet to establish ownership, in the same way that a signature on a paper contract is legally binding. Countries including the United States have sanctioned the use of digital signatures.

Authorization and intrusion. Software programs allow a hierarchy of approvals to be established for access to data. In a company, for example, senior managers can be authorized to view and even manipulate data that more junior personnel do not have access to. Other programs act as guardians of the data, and detect any unauthorized or unusual actions on the computer (i.e., hacking).

Computers connected to the Internet are often equipped with software known as a firewall. The firewall functions to monitor incoming transmissions and to restrict those that are deemed suspicious. It is a controlled gateway that limits who and what can pass through. A number of vendors offer firewall programs. Like anti-virus software, these programs can and should be frequently updated, since those who seek to maliciously gain remote access to computers are constantly developing methods to thwart the firewall barrier.

FURTHER READING:

BOOKS:

Bentley, Tom, and Jon Hastings. *Safe Computing: How to Protect Your Computer, Your Body, Your Data, Your Money and Your Privacy in the Information Age.* Concord, CA: Untechnical Press, 2000.

Bishop, Matt. *Computer Security: Art and Science.* Boston: Addison Wesley Professional, 2002.

Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security: Repelling the Wiley Attacker, Second Edition.* Boston: Addison Wesley Professional, 2003.

Stoll, Clifford. *Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage.* New York: Simon and Schuster, 2000.

Whittaker, James A., and Herbert Thompson.*How to Break Software Security: Art and Science.* Boston: Addison Wesley Professional, 2002.

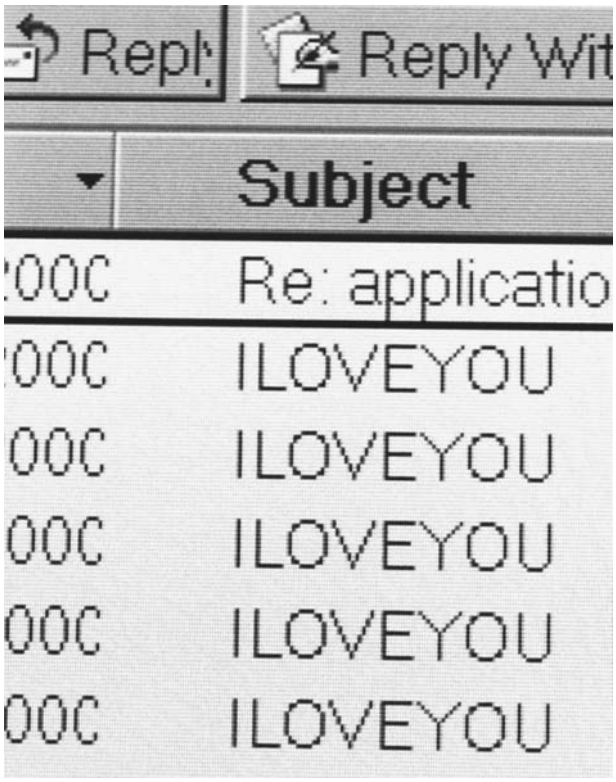
SEE ALSO

Computer Hardware Security
Computer Virus
Cyber Security

Computer Virus

LARRY GILMAN

A computer virus is a program or segment of executable computer code that is designed to reproduce itself in computer memory and, sometimes, to damage data. Viruses are generally short programs; they may either stand-alone or be embedded in larger bodies of code. The



A computer screen e-mail inbox showing subject names reading "ILOVEYOU," that contains a powerful computer virus that struck global communications systems and crippled government and corporate computer networks around the world in May, 2000. AP/WIDE WORLD PHOTOS.

term "virus" is applied to such code by analogy to biological viruses, microorganisms that force larger cells to manufacture new virus particles by inserting copies of their own genetic code into the larger cell's DNA. Because DNA can be viewed as a data-storage mechanism, the parallel between biological and computer viruses is remarkably exact.

Many viruses exploit computer networks to spread from computer to computer to computer, sending themselves either as e-mail messages over the Internet or directly over high-speed data links. Programs that spread copies of themselves over network connections of any kind are termed "worms," to distinguish them from programs that actively copy themselves only within the memory resources of a single computer. Some experts have sought to restrict the term "virus" to self-replicating code structures that embed themselves in larger programs and are executed only when a user runs the host program, and to restrict the term "worm" to stand-alone code that exploits network connections to spread (as opposed to, say, floppy disks or CD ROMs, which might spread a virus). However, virus terminology has shifted over the last decade, as computers that do not communicate over networks have become rare. So many worm/virus hybrids have appeared that any distinction between them is rapidly disappearing. In practice, any software that replicates itself may be termed a "virus," and most viruses are

designed to spread themselves over the Internet and are therefore "worms."

A program that appears to perform a legitimate or harmless function, but is in fact designed to propagate a virus is often termed a Trojan Horse, after the hollow, apparently-harmless, giant wooden horse supposedly used by the ancient Greeks to sneak inside the walls of Troy and overthrow that city from within. Another interesting subclass of viruses consists of chain letters that purport to warn the recipient of a frightening computer virus currently attacking the world. The letter urges its recipient to make copies and send them to friends and colleagues. Such hoax letters do not contain executable code, but do exploit computerized communications and legitimate concern over real, executable-code viruses to achieve self-replication, spread fear, and waste time. Chain letters have also been used as carriers for executable viruses, which are attached to the chain letter as a supposedly entertaining or harmless program (e.g., one that will draw a Christmas card on the screen).

The first "wild" computer viruses, that is, viruses not designed as computer-science experiments but spreading through computers in the real world, appeared in the early 1980s and were designed to afflict Apple II personal computers. In 1984, the science fiction book *Necromancer*, by William Gibson, appeared; this book romanticized the hacking of giant corporate computers by brilliant freelance rebels, and is thought by some experts to have increased interest among young programmers in writing real-world viruses. The first IBM PC computer viruses appeared in 1986, and by 1988 virus infestations on a global scale had become a regular event. An anti-virus infrastructure began to appear at that time, and anti-virus experts have carried on a sort of running battle with virus writers ever since. As anti-virus software increases in sophistication, however, so do viruses, which thrive on loopholes in software of ever-increasing complexity. As recently as January 28, 2003, a virus dubbed "SQL Slammer" (SQL Server 2000, targeted by the virus, is a large software package run by many businesses and governments) made headlines by suspending or drastically slowing Internet service for millions of users worldwide. In the United States alone, some 13,000 automatic teller machines were shut down for most of a day.

All viruses cause some degree of harm by wasting resources, that is, filling a computer's memory or, like SQL Slammer, clogging networks with copies of itself. These effects may cause data to be lost, but some viruses are designed specifically to delete files or issue a physically harmful series of instructions to hard drives. Such viruses are termed *destructive*. The number of destructive viruses has been rising for over a decade; in 1993 only about 10% of viruses were destructive, but by 2000 this number had risen to 35 percent.

Because even nonmalicious or nondestructive viruses may clog networks, shut down businesses or Web sites, and cause other computational harm (with possible real-world consequences, in some cases), both the private sector and governments are increasingly dedicating resources to the prevention, detection, and defeat of viruses. Twenty to 30 new viruses are identified every day, and over 50,000 viruses have been detected and named since the early 1980s, when computers first became integrated with the world economy in large numbers. Most viruses are written merely as egotistical pranks, but a successful virus can cause serious losses. The ILOVEYOU virus that afflicted computers globally in May, 2000 is a dramatic recent case that illustrates many of the properties of viruses and worms.

The ILOVEYOU virus was so named because in its most common form (among some 14 variants) it spread by looking up address-book files on each computer it infected and sending an e-mail to all the addresses it found, including a copy of itself as an attachment named LOVE-LETTER-FOR-YOU.TXT.VBS. ("VBS" stands for Visual Basic Script, a type of file readable by World Wide Web browsers.) If a recipient of the e-mail opened the attachment, the ILOVEYOU virus code would run on their computer, raiding the recipient's address book and sending out a fresh wave of e-mails to still other computers.

ILOVEYOU first appeared in Asia on May 4, 2000. Designed to run on PC-type desktop computers, it rapidly spread all over the world, infecting computers belonging to large corporations, media outlets, governments, banks, schools, and other groups. Many organizations were forced to take their networks off line, losing business or suspending services. The United States General Accounting Office later estimated that the losses inflicted by the ILOVEYOU virus may have totaled $10 billion worldwide. Monetary losses occurred because of lost productivity, diversion of staff to virus containment, lost business opportunities, loss of data, and loss of consumer confidence (with subsequent loss of business).

National security may also be threatened by computer viruses and similar software objects. During the ILOVEYOU incident, the U.S. Department of Health and Human Services was disrupted for many hours. An official of the department stated that if a biological outbreak had occurred simultaneously with this 'Love Bug' infestation, the health and stability of the nation would have been compromised with the lack of computer network communication. An official at the U.S. Department of Defense stated that so many personnel had to be shifted from their primary responsibilities to deal with ILOVEYOU that if the incident had continued much longer, reservists would have had to be called up. All this damage, and more, was accomplished by a virus not even especially designed to do so. Governments are, therefore, concerned that specially designed viruses and other forms of cyberattack may be used deliberately by hostile governments or terrorist groups to cripple the military or the economy. The U.S. National Security Agency has stated that at least 100 governments are developing viruses and other cyberweapons, as well as terrorist groups. To counter such threats, the U.S. government has established a

National Infrastructure Protection Center in the Federal Bureau of Investigation. Its mission is to serve as the central federal point for coordinating information on threats to infrastructure, including threats (such as viruses) to computers and telecommunications networks.

FURTHER READING:

BOOKS:

Ferbrache, David. *Pathology of Computer Viruses.* Germany: Springer-Verlag, 1992.

Fites, Philip, Peter Johnston, and Martin Kratz. *The Computer Virus Crisis.* New York: Van Nostrand Reinhold 1992.

PERIODICALS:

"Virus Hits A.T.M.s and Computers Across Globe." *New York Times.* January 28, 2003.

ELECTRONIC:

Brock, Jack L. "'ILOVEYOU' Computer Virus Highlights Need for Improved Alert and Coordination Capabilities." United States General Accounting Office. Testimony before the Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs, U.S. Senate. May 18, 2000. <nsi.org/library/virus/ai00181t.pdf> (Jan. 28, 2003).

SEE ALSO

Cyber Security

Concealment Devices

JUDSON KNIGHT

The need for concealment strikes at the heart of intelligence and covert operations work, as well as a number of military activities. Concealment devices have been used to disguise film, documents, and other items containing intelligence material, which of necessity must be transported from a dangerous location—in or around the spot where they were gathered—to a safe haven, namely the intelligence bureau that commissioned the activity. To achieve the objective of circumventing detection, intelligence agencies and operatives have developed a number of clever devices, ranging from hollow coins to fake batteries. Documents, cameras, and film had found secure hiding places in objects as innocuous as a statuette, a hairbrush, or a can of shaving cream.

Camouflage and Concealment: Passive Arts

All forms of concealment devices rely on the use of camouflage in the most general sense of the term. The word, from the French *camoufleur* ("to disguise"), entered the English language during World War I, when the development of military aircraft exposed troop positions to enemy reconnaissance planes. In the course of the war, all major military forces established camouflage units composed of soldiers trained in the art. This led to the development of camouflage uniforms, the use of foliage or other materials to disguise positions, and other measures.

Nature, of course, "discovered" camouflage long before humans did, and in a wide variety of plant and animal species, natural selection has favored those that developed protective coloration or other forms of natural camouflage. Concealment by camouflage, in its truest sense, is of necessity passive rather than active, and in this regard, the term does not encompass those species capable of imitating predators or otherwise "convincing" other plants or animals that they are something other than they are.

This point is an important one, because it is not the purpose of camouflage and concealment to persuade the enemy; rather, the purpose of camouflage is to render the enemy unaware. Disinformation, then, is not truly concealment, as its purpose is to convince the enemy that some (actually false) premise is the case. Likewise, codes and ciphers, while they certainly conceal information, are not a form of concealment in this sense because they are obviously codes.

Varieties of Concealment Devices

Effective concealment necessarily involves items that resemble everyday objects, coins being a good example. During the Cold War, KGB operatives often carried microfilm in a concealment device made from one of the more physically large coins commonly used in the country of their operation. Likewise, a Western intelligence service in the late 1970s used a hollow version of a United States Eisenhower dollar coin.

Inside the Soviet version was a cavity for hiding microfilm, which might contain ciphers, messages, or a communiqué providing the operative with date and time coordinates for a planned transmission. A special pin opened the interior. The Western version, in use during the late 1970s, could be opened by pressing the tip of the eagle's wing on the reverse side.

Long before the use of coins as concealment devices, intelligence operatives utilized an even more common disk-shaped object of small size: a button. In this case, the button itself was an ordinary one, but the back contained a carefully written coded or enciphered message in very small lettering. This technique dates back to World War I.

Hiding cameras. A number of concealment devices, particularly those used by Soviet and East German intelligence, were designed to hide cameras inside ordinary-looking

Concealed weapons that fell into western hands through the defection of Russian Intelligence Captain Nikolai E. Khokhlov in 1954 included cases of cigarettes that fired hollowpoint bullets and miniature pistols that fired while making a sound less than the snap of a finger. AP/WIDE WORLD PHOTOS.

items. When West German operatives of the counterintelligence service BfV apprehended one East German spy, they found in his apartment a decorative wooden carving of an elk. Inside the base, however, was a compartment for holding a Minox camera, a favorite piece of photographic equipment on both sides of the iron curtain.

One reason for the Minox's popularity was its size and shape, which was oblong and flat, and therefore made for easy concealment. Another East German favorite was a men's clothing brush or shoe brush, which could easily hold a Minox in the handle. Locking pins kept the compartment from opening when the operative was using the brush for its intended purpose, as he would most certainly have done so as not to arouse suspicion.

A particularly inventive East German device made use of a portable chessboard whose surface had sockets to secure the playing pieces. One of the 64 sockets, when a paper clip was inserted into it, opened the back of the chessboard to reveal a microdot camera. The chessboard—which, like many of these items, was probably one of a kind, created in a special East German workshop for espionage equipment. Security of intelligence operations required that no device become standard equipment; if one operative were detected, this could potentially blow the cover of other comrades using a similar item.

Film and other items. Cylindrical objects make a logical hiding place for rolls of film, and agencies of the Communist world used a number of such objects. One was a D-sized battery, about as large as a typical photographic film canister. So as to avoid suspicions arising from a non-working battery, inside the fake one was a much smaller battery, about the size of an AA, which provided voltage. This left the remainder of the inner compartment free to conceal any item small enough to fit.

For the same reason that the fake battery was made to work like a real one, a shaving-cream can device used by Western intelligence contained a small amount of shaving cream, with the remainder of the compartment set aside

for concealed items. A cigarette used by Polish intelligence likewise had real tobacco, but the operative would never knowingly light it: inside was a roll of extremely thin film. On the other hand, a soap case used by Czech intelligence to transport film did not have room for a real soap bar: inside was a battery and flashbulb, which would flash and ruin the film if it were opened improperly.

FURTHER READING:

BOOKS:

Breckenridge, Robert P. *Modern Camouflage, the New Science of Protective Concealment.* New York: Farrar & Rinehart, 1942.

Hartcup, Guy. *Camouflage: A History of Concealment and Deception in War.* New York: Scribner's, 1980.

Minnery, John. *CIA Catalog of Clandestine Weapons, Tools, and Gadgets.* Boulder, CO: Paladin Press, 1990.

ELECTRONIC:

CIA Museum. Central Intelligence Agency. <http://www.cia.gov/cia/information/artifacts/> (March 29, 2003).

International Spy Museum. <http://www.spymuseum.org/> (March 29, 2003).

SEE ALSO

Assassination Weapons, Mechanical
Cameras
Cameras, Miniature
CIA Directorate of Science and Technology (DS&T)
Covert Operations
Cryptology, History
Dead Drop Spike
Disinformation

Consumer Product Safety Commission (CPSC), United States

The United States Consumer Product Safety Commission (CPSC) is an independent federal agency designed to protect the public against unreasonable risks of injuries and deaths associated with consumer products. Congress established the commission in 1972, as part of the Consumer Product Safety Act. The CPSC regulates more than 15,000 types of consumer products, from coffee pots to toys. The commission's jurisdiction, however, is limited. Cars, trucks, and motorcycles are governed by the U.S. Department of Transportation; the U.S. Food and Drug Administration (USFDA) oversees cosmetics, food and drugs. Alcohol, tobacco, and firearms fall under the domain of the U.S. Treasury Department.

Since its inception, the CPSC has conducted research on potential product hazards and vigorously pursued and enforced mandatory standards on many consumer products. The Consumer Product Safety Act requires manufacturers to report serious product defects in a timely manner. Failure to do so can result in civil penalties. In 2001, the commission fined Fisher-Price $1.1 million on charges that it failed to disclose a fire hazard in a popular toy. The fine was the largest against a toy firm in CPSC's history.

Product recalls are one of the most familiar actions of the CPSC. Recall information is posted on the commission's Web site and circulated throughout the news media. One of the largest recalls in recent history involved 650,000 baby strollers that collapsed while in use. The CPSC and Ohio-based Century Products announced the historical recall after hundreds of children suffered injuries.

The backbone of the CPSC is the National Electronic Injury Surveillance System (NEISS). The system compiles data on consumer product-related injuries occurring in the U.S., as documented by hospital emergency departments. Such data allow the CPSC to make timely national estimates of the number of injuries associated with, although not necessarily caused by, specific consumer products. CPSC analysts study the data for important clues to the cause and potential prevention of injuries.

The Washington, D.C. headquartered agency has an operating budget of approximately $56 million and employs approximately 480 people. In 2002, President George W. Bush nominated attorney Hal Stratton as the eighth chairman of the agency.

FURTHER READING:

ELECTRONIC:

Consumer Product Safety Commission "Who We Are; What We Do For You." December 12, 2002 <http://www.cpsc.gov/cpscpub/pubs/103.html>(December 10, 2002).

SEE ALSO

ATF (United States Bureau of Alcohol, Tobacco, and Firearms)
FDA (United States Food and Drug Administration)
NTSB (National Transportation Safety Board)

Continuity Irish Republican Army (CIRA)

Continuity Irish Republican Army (CIRA) also operates as, or is known as, the Continuity Army Council.

A consumer information officer with the U.S. Consumer Product Safety Commission demonstrates the danger crib slats can pose to an infant during a press conference in 2002. AP/WIDE WORLD PHOTOS.

CIRA is a radical terrorist splinter group formed in 1994 as the clandestine armed wing of Republican Sinn Fein (RSF), which split from Sinn Fein in the mid-1980s. "Continuity" refers to the group's belief that it is carrying on the original IRA goal of forcing the British out of Northern Ireland, and CIRA actively seeks to recruit IRA members. CIRA has been active in the border areas of Northern Ireland where it has carried out bombings, assassinations, kidnappings, extortion, and robberies. Targets include British military and Northern Ireland security targets and Northern Ireland Loyalist paramilitary groups. CIRA does not have an established presence on the U.K. mainland. As of May, 2002, CIRA was not observing an established cease-fire and in October, 2001, CIRA officials stated that decommissioning weapons would be "an act of treachery."

CIRA is estimated to have fewer than 50 dedicated activists, but is said to have recruited new members in Belfast. CIRA is suspected of receiving funds and arms from sympathizers in the United States. CIRA may have acquired arms and materiel from the Balkans in cooperation with the Real IRA.

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual Reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Continuity of Government, United States

ADRIENNE WILMOTH LERNER

The Continuity of Government (COG) program ensures the survival of essential federal government leaders and agencies in the event of a severe crisis. Created at the height of 1960s public and government concern about the possibility of nuclear warfare, COG provides a network of disaster relief, emergency assistance, law enforcement, and information services to the general citizenry of the United States. COG also maintains underground facilities to protect the president, cabinet members, and essential government personnel in the event of attack or catastrophe.

President John F. Kennedy created the Continuity of Government program on February 12, 1962. The stated purpose of COG was to shield the essential infrastructure of the United States government from destruction, permitting its continued operation and authority in a time of crisis. Intended to preserve the American form of representative government, continuity of federal authority aided law enforcement, ensured general safety, and protected the government from the illegal assumption of power by rival foreign powers or anti-government organizations. The government acknowledged plans to construct secret facilities and implement a COG strategy, but the details and locations of COG operations were meant to remain secret.

The Kennedy administration incorporated existing emergency strategies into its COG plans. Executive Order 10346, issued by President Harry S. Truman in 1947, outlined emergency plans for federal departments. Truman created the Office of Emergency Planning to establish policies for continued operations in the event of a national crisis. Kennedy reorganized the Office of Emergency Planning as part of his wide-sweeping reform of national defense infrastructure. These reforms were dictated by Executive Order 10952, and the Office of Emergency Planning gained the authority to set policy for the continuity of all three main branches of government.

One of the first orders of the COG was to ensure the survival of the president, or executive authority. In 1947, the line of succession of to the presidency was expanded, and more firmly established. The line of succession moved first to the vice president, then to the Speaker of the House of Representatives, the president pro tem of the Senate, and then proceeds through nine members of the cabinet. Cabinet positions created after 1947 are not included in the line of presidential succession. COG used this established line of succession to determine its strategies for the preservation of executive function. According to COG policy, not all twelve people on the list of presidential succession can gather in the same location, at the same time. During large, pan-government events, such as the State of the Union Address, and presidential inaugurations, one member of the Cabinet is removed to a remote, safe, COG-designated location.

After securing the line of succession in the Executive branch, the COG program mandated that individual government departments create their own, internal lines of succession and continuity plans. COG officials check these lines and plans annually, and most are published in the Federal Register, so that other agencies can coordinate operations with continuity personnel.

One of the most clandestine operations of the COG program is the maintenance of the so-called Shadow Cabinet. The Shadow Cabinet is composed of trained personnel, appointed by the president and cabinet to serve as a reserve government in the unlikely event of a catastrophic disaster that destroys the government in Washington. The Shadow Cabinet operates at a secure COG location, and has never been utilized or played any role in Federal policy formation.

COG plans also included the physical protection of government entities. The preeminent COG safe facility was constructed in stages, beginning in the 1940s. An extensive series of underground bunkers that contain all of the necessities of a small city, was constructed in the mountains of Virginia. The facility, known as Mount Weather, is one of a series of regional Crisis Relocation Facilities. Command centers for the Federal Emergency Management Agency (FEMA) and the National Emergency Coordinating Center are located deep within the cavernous structure. Other facilities designated as COG safe sites include several military bases and *Air Force One,* the president's personal airplane.

In the 1980s, the White House National Program Office was responsible for COG operations. Operations were expanded to include the establishment of facilities responsible for the maintenance of critical information systems, including government and banking computer systems. Emergency management agencies decided to house reserve command centers at Mount Weather, providing a central, underground, and contained location for COG operations.

As the Cold War ended, and details of the government's COG operations garnered public attention, debate emerged over the usefulness and possible effectiveness of COG plans. Critics alleged that the system was outdated; others claimed it was insufficient to handle a crisis of great magnitude. As the frenzy about nuclear weapons ebbed, the COG strategy was evaluated to handle post-cold war threats, such as terrorist attacks. Indeed, some aspects of the COG plan went into effect during the September 11, 2001, terrorist attacks on New York and Washington, D.C.

The recent creation of the Department of Homeland Security (DHS) will possibly alter current, established COG

plans. The DHS gained the authority to administer COG plans, and assumed responsibility for many of its member agencies. To compliment the federal COG program, DHS officials encouraged state and local governments to implement or reform their own COG strategies. New guidelines and annual audits will aid in the supervision of sate and local COG plans, making sure that such plans provide an adequate guarantee of local law enforcement and government operation in the event of a crisis.

FURTHER READING:

ELECTRONIC:

Federal Emergency Management Agency. Mount Weather Emergency Assistance Center homepage. <http://www.fema.gov/pte/weather.htm> (20 April 2003).

SEE ALSO

Emergency Response Teams
FEMA (United States Federal Emergency Management Agency)

Continuous Assisted Performance (CAP)

In order to extend the physical capabilities of soldiers and the mental acuity of pilots and other operators of technical equipment, the Defense Advanced Research Projects Agency (DARPA) sponsors research into continuous assisted performance (CAP) technology and pharmacology.

CAP programs are designed to allow an increase in operation tempo by allowing soldiers to operate without sleep, or limited amounts of sleep, for at least seven days. In most combat operational systems, the fatigue of soldiers is the major limiting factor in operational readiness and ability to continue action. Because of the increasingly technical nature of warfare, the mere ability to go without sleep is not productive unless high levels of both cognitive and physical performance can be maintained.

The effects of sleep deprivation are well known to interrogators, and informal efforts to fight fatigue among troops have ranged from the soldier's historical use of strong coffee or tea to the condoned use of pharmacological fatigue management tools. U.S. Air Force pilots are routinely allowed to take dexamphetamine pills (also known as "go" pills), a prescription drug.

The use of go pills is controversial because the active ingredients can impair judgment. In fact, when used in other formulations, such drugs routinely carry warnings against operating heavy equipment under the influence of the drug. The impairment of judgment associated with dexamphetamine pills, further stimulates CAP research.

During the Flight of Apollo 13, as the crew entered the critical reentry orbit interface, the exhausted crew was reportedly ordered to take Dexedrine tablets to help keep their computer inputs precise and accurate.

Use of dexamphetamine by U.S. pilots, whose judgment might have been impaired by fatigue or the use of "go pills," was also argued to be a contributing factor in a 2002 "friendly fire" bombing accident in Afghanistan.

FURTHER READING:

ELECTRONIC:

DARPA, Defense Science Office. Continuous Assisted Performance (CAP). <http://www.darpa.mil/dso/thrust/biosci/cap.htm> (April 14, 2003).

SEE ALSO

Information Warfare
Interrogation: Torture Techniques and Technologies

Coordinator for Counterterrorism, United States Office

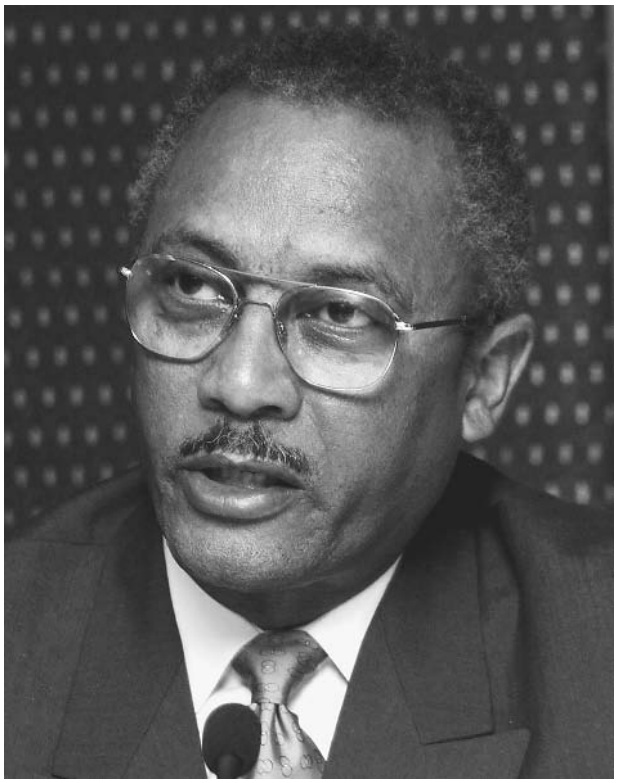
The Office of the Coordinator for Counterterrorism is a section of the United States Department of State charged with coordinating efforts to improve cooperation between the U.S. government and its foreign counterparts in battling terrorism. The coordinator, an ambassador, is the primary functionary of the federal government for developing and implementing America's counterterrorism policy.

Four Principles of U.S. Counterterrorism Policy

In forming specific policies for tactical purposes, the coordinator considers four strategic principles of U.S. counterterrorism policy:

1. The government makes no concessions to, or agreements with, terrorists;

2. Terrorists must be brought to justice for their crimes;



U.S. State Department Coordinator for Counterterrorism, Francis X. Taylor, answers questions at a news conference in New Delhi, India, during a 2001 meeting to finalize a U.S./India anti-terrorism project. AP/WIDE WORLD PHOTOS.

3. States that sponsor terrorists and terrorism must be isolated and pressured so as to force a change of behavior; and

4. The counterterrorism capabilities of countries allied with the United States, and those that require assistance in fighting terrorism, must be bolstered.

Under provisions of the U.S. Patriot Act of 2001 (8 U.S.C. 1182), Section 411, the secretary of state may, in consultation with the attorney general of the United States, designate certain terrorist organizations on a "terrorist exclusion list" (TEL). Organizations listed on the TEL may be prevented from entering the country, and in certain circumstances may be deported. Before the secretary of state places an organization on the TEL, he or she must find that its members commit or incite terrorist activity, gather information on potential targets for terrorist activity, or provide material support to further terrorist activity. Under the terms of the statute, "terrorist activity" means all unlawful activity that involves hijacking or sabotage of an aircraft, vessel, or vehicle; hostage-taking; a violent attack on a person protected under international law; assassination; or the use of firearms, biological or chemical agents, nuclear devices, or other weapons to endanger individuals or damage property for purposes other than mere personal gain.

On December 5, 2001, Secretary of State Colin Powell, in consultation with Attorney General John Ashcroft, placed more than three dozen groups on the TEL. These represented a range of ideologies and areas of operation, including the Libyan Islamic Fighting Group, the Army for the Liberation of Rwanda, the Continuing Irish Republican Army, and the Japanese Red Army. Included also were front organizations such as the al-Hamati Sweets Bakeries, a Yemeni company considered to have ties with the Islamist terror organization al-Qaeda.

FURTHER READING:

PERIODICALS:

Nelson, Scott Bernard. "U.S. Offers $5M in Financial War on Terrorism." *Boston Globe.* (November 14, 2002): C1.

ELECTRONIC:

Coordinator for Counterterrorism. United States Department of State. <http://www.state.gov/s/ct/> (February 22, 2003).

SEE ALSO

Department of State, United States
FEST (United States Foreign Emergency Support Team)
Terrorist Organization List, United States
United States, Counter-Terrorism Policy

Copyright Security

The term *copyright security* refers to the protection of, and measures taken to prevent the unauthorized duplication of, copyrighted materials. With the increasing digitization and computerization of society, efforts aimed at maintaining and protecting copyright security have likewise become increasingly high-tech. Software is routinely copyright-protected, and copyright holders often take extraordinary measures, including the retention of detective agencies, to police acts of copyright infringement.

Copyright law. Article I, Section 8, of the United States Constitution authorizes Congress to protect the writings of authors, and to this end, Congress passed the U.S. Copyright Act (17 USC 101–810), the principal set of statutes governing copyright in America. Because the law is written to be interpreted broadly, and because it contains provisions precluding any state laws inconsistent with it, copyright law is almost entirely a federal and not a state matter.

In order to be protected by copyright, a work must be original, and must be in a concrete medium—in other

A steam roller crushes pirated CDs and electronic games during a destruction ceremony at the customs office in Bangkok, Thailand. AP/WIDE WORLD PHOTOS.

words, it must be recorded, not existing solely in "live" form. A work need not carry a copyright notice to be copyrighted, nor is registration required. However, copyright holders wishing to obtain registration may do so through the federal agency charged with administering copyright, the Copyright Office of the Library of Congress in Washington, D.C.

The holder of a copyright has the exclusive right to reproduce, distribute, perform, display, or license his or her work, as well as derivatives of his or her work. This means that others, in order to use all or a portion of that work, must obtain permission and, if necessary, pay a fee for use. There are, however, limited exceptions for "fair use" of copyrighted works, as in a book review.

Works published before 1923 are now in the public domain, meaning that they no longer hold a copyright, though a particular translation, made more recently, may be copyrighted. For works published after 1923, there are specific provisions as to when the item becomes part of the public domain. Some of these provisions, and other aspects of U.S. copyright law, are governed by the Berne Convention for the Protection of Literary and Artistic Works, which the United States signed in 1989.

The Digital Millennium Copyright Act. As technology has changed, so has the definition of "writings" under U.S. copyright law. Today the Copyright Act encompasses not only those forms of expression traditionally understood as writings, but also architectural designs, works of graphic art, motion pictures, sound recordings, and computer software. Continued changes in the technology of copyrighted material prompted the 1998 passage of the Digital Millennium Copyright Act (DMCA), the most comprehensive overhaul of copyright law in a generation.

The DMCA endures criticism from detractors who consider it as squelching the free exchange of ideas through the Internet and electronic media. Although controversial, the DMCA remains law, and as such requires enforcement. Although federal authorities have sole power where enforcement is concerned, private firms such as BayTSP, a digital detective service, assist the federal government by interdicting lawbreakers. In addition to law enforcement agencies, Bay TSP's clientele includes private holders of intellectual property who pay the company to protect that property against infringements in cyberspace.

Using an Internet spider (a computer program that crawls over the World Wide Web and automatically fetches Web pages, for instance for a search engine), BayTSP searches the Web for lawbreakers. These include, for its federal clients, purveyors of child pornography, and for its private clients, users offering electronic files to share. These electronic files may include software, sound recordings in digital format, or other materials.

If BayTSP finds an IP or Internet Protocol address (equivalent to a neighborhood post office on the Internet) at which illegal activity is taking place, under the DMCA, it has the right to subpoena logs kept by the Internet service provider. These logs will enable it to connect IP addresses with user accounts. Arrest of lawbreakers may follow, depending on the seriousness of the crime and the degree of desire for enforcement on the part of the client. For companies interested in maintaining good public relations, that desire may be low, whereas for federal agencies investigating child pornography, enforcement is usually swift and severe.

FURTHER READING:

ELECTRONIC:

Cringely, Robert. "We Can Run, But We Can't Hide: How BayTSP Is Enforcing the Digital Millennium." Public Broadcasting System. <http://www.pbs.org/cringely/pulpit/pulpit20020919.html> (February 22, 2003).

Forno, Richard. Copyright, Security, and the Hollywood Hacking Bill. <http://online.securityfocus.com/columnists/99> (February 22, 2003).

SEE ALSO

Computer Software Security

Counterfeit Currency, Technology and the Manufacture

In the past, counterfeiters produced false banknotes with printing presses, and some of the more skillful counterfeiters went to great lengths to imitate the original. Today, sophisticated computer printers and copiers enable even unskilled would-be counterfeiters to produce notes that bear at least a superficial resemblance to real ones. However, the federal government continually works to stay a step or more ahead of counterfeiters, updating currency and making it ever more difficult to duplicate.

Two Waves of Counterfeiting

For virtually as long as there has been regular currency, there has also been false currency, which has provided a highly lucrative illegal trade to those who can successfully pass off false banknotes as the genuine article. The period since the middle of the twentieth century has seen two significant waves of counterfeiting. First, there was a surge in the illegal production of banknotes during the 1960s, when advances in printing and graphic arts technology enabled counterfeiters with the right equipment and skills to produce highly accurate copies of federal currency. By the 1990s, however, counterfeiting by means of the printing press had diminished in significance compared to a new variety of counterfeit currency manufacture, this one using computer printers.

The phenomenon of "P-notes," or "printer notes," first came to the attention of law enforcement in the early 1990s. In1995, authorities made a total of 37 arrests nationwide in connection with the production and distribution of currency produced on ink-jet or laser-jet printers. By 2000, this number had skyrocketed to 4,500 arrests, and officials estimated that P-notes accounted for as much as forty percent of the currency seized by the United States Secret Service (USSS) and other agencies annually.

Contrast of practitioners and techniques. The change in choice of technology also signaled a change in the profile of the average counterfeiter. The old variety of criminal operating in this field tended to be mature and skilled—a professional, highly trained practitioner who usually possessed, or at least had access to, printing equipment whose operation would require knowledge far beyond that of a novice.

A computer printout of counterfeit $20 bills removed from the home of a Massachusetts teenager by the U. S. Secret Service. AP/WIDE WORLD PHOTOS.

The 1990s variety of counterfeiter, by contrast, fit a quite different profile. Rather than being "professional counterfeiters," they were more likely to be drug dealers who used their P-notes in connection with other crimes, most notably the purchase of drugs. Typically youthful (many were juveniles), these new counterfeiters lacked skills for counterfeiting. Whereas the old model at least required some degree of human ingenuity, the new type of counterfeiting was primarily a matter of possessing the right equipment.

Equipment loomed large in the old counterfeiting technology as well, but practitioners had to know how to use it. Counterfeiters of that era carefully studied currency, and made numerous photographs of it with graphic-arts cameras using different filters so as to break down the various stages of the printing process. Only after considerable trial and error could a workable set of printing plates be produced.

In contrast to this painstaking process, the new counterfeiting process required only that one use a high-quality scanner to obtain an image of a bill, then print that bill on a printer with high resolution. Given the ease of production, counterfeiting again became a growth industry during the

1990s, and in 2001, the federal government seized a record $47 million in counterfeit currency. By the following year, the figure had dropped to $43 million.

Anti-counterfeiting Technology

The fact that the value of counterfeit currency seized in 2002 had dropped by almost 10 percent is not an indication of looser standards in interdiction; rather, after the September 11, 2001, terrorist attacks on the United States, the federal government was more likely to be aggressive in searching for counterfeiters, whose ranks could presumably include foreign operatives funding illegal operations while undermining the value of U.S. currency. The reduction in seizures is probably an indication of success in efforts by the federal government to make its currency more difficult to duplicate.

In 1996, partly as a response to the proliferation of P-bills, the U.S. currency underwent its first major redesign in 70 years. Already difficult to duplicate, the currency became much more so thanks to measures such as the use of optically variable ink (OVI). The latter contains tiny particles of special film such that it changes color depending on the angle from which it is viewed. Extremely expensive and therefore used in limited quantities, OVI is just one of several specialized varieties of ink used in producing currency. By 2004, additional changes included the introduction of new colors of inks. None is commercially available—another hurdle in the production of false currency.

A number of other features distinguish genuine currency from counterfeit. One of the most obvious ones is the paper itself. Every variety of national currency is made with a special type of paper (the Australian dollar is actually printed on very thin plastic), and U.S. currency uses a highly durable variety made from cotton pulp. Not only does it have a distinctive texture, it is far more resistant to tearing, deformation, moisture, or sunlight than most varieties of paper. Again, currency paper is not commercially available.

For the counterfeiter, a genuine banknote is a veritable minefield of potential pitfalls, and literally every square millimeter presents its own challenges. There are watermarks, embedded threads, see-through features, microprinting, holograms, latent images—even forms of embossing to facilitate recognition of various denominations by the blind and visually impaired. The printing of currency is also highly complicated, involving various processes at different stages. In addition to lithography, letterpress, and sometimes silkscreening, there is intaglio, an extremely expensive, technically difficult process in which the surface of the paper is deformed ever so slightly—another distinctive feature of official currency production.

Special safeguards against copiers. Aside from these challenges to the would-be counterfeiter, there is also the problem of producing a usable serial number. Given these challenges, a drug dealer with a computer printer or copier is unlikely to enjoy long-term success in this illicit trade. For those using a copier, the problem is rendered even greater by additional measures. Most modern forms of currency have anti-copy features, tiny designs that have words such as *VOID* or *FAKE* embedded in them in such a way that they will be visible if copied.

Manufacturers of color copy machines have also implemented a number of measures to circumvent the use of their equipment for illegal purposes. Most modern copy machines carry and embed unique codes, invisible in ordinary light, such that their products are traceable to a specific machine. There is also technology that detects specific design elements of currency, and will cause the copier to shut down if it is used for illegal purposes.

FURTHER READING:

BOOKS:

Optical Document Security. Boston: Artech House, 1998.

Sincerbox, Glenn T. *Counterfeit Deterrent Features for the Next-Generation Currency Design.* Washington, D.C.: National Academy Press, 1993.

U.S. Currency: Treasury's Plan to Study Genuine and Counterfeit U.S. Currency Abroad: Report to Congressional Requesters. Washington, D.C.: General Accounting Office, 1997.

ELECTRONIC:

"Counterfeit Detection: A Guide to Spotting Counterfeit Currency." <http://www.indigoimage.com/> (February 5, 2003).

"Technology Breeds New Counterfeiting." ABC News <http://abcnews.go.com/sections/Downtown/2020/Downtown_010601_counterfeitmoney_feature.html> (February 5, 2003).

SEE ALSO

Engraving and Printing, United States Bureau
Federal Reserve System, United States
Secret Service, United States

Counter-Intelligence

Counter-intelligence is the use of intelligence resources to identify, circumvent, and neutralize the intelligence activities of a foreign power. That foreign power may be an enemy nation or a putative ally. In the United States, counter-intelligence is overseen from the Counter-intelligence Center (CIC) of the Central Intelligence Agency

Counter-intelligence agents are sworn in before a joint congressional committee holding open hearings on events surrounding the September 11, 2001 terrorist attacks. Behind the screen at lower left, used to protect their identities, are CIA and FBI agents. ©REUTERS NEWMEDIA INC./CORBIS.

(CIA), although a number of intelligence and law enforcement agencies are concerned with counter-intelligence to some degree.

Not only has the United States faced spying by Soviet and Eastern Bloc, Chinese, and Cuban operatives, but also by semi-friendly nations such as France or Indonesia, and by outright allies such as South Korea and Israel. According to testimony given before the House Permanent Select Committee in 2000 by Paul Redmond, former CIA associate deputy director of operations for counter-intelligence, some 41 countries were at that time attempting to spy on the United States. Given the size of the threat posed by foreign intelligence—which seeks to gain information on the technology and activities of the U.S. government, its agencies, and the military—federal authorities have sought to keep in place an effective counter-intelligence network. This involves not only operators, or front-line personnel involved in direct contact with foreign intelligence agents, but also analysts, whose job it is to study wiretap transcripts, surveillance reports, and other materials on the activities of foreign agents.

While the CIA holds the principal role in counter-intelligence among U.S. agencies, even the Federal Bureau of Investigation (FBI), whose primary responsibility is law enforcement, has a counter-intelligence role. Sometimes this can be inadvertent; FBI agents, rather than their counterparts in the CIA, apprehended Soviet operative John Walker in 1985. Actual FBI counter-intelligence is concerned with investigating terrorist threats and other attempts to disrupt infrastructure or operations in the United States. (Ironically, an FBI counter-intelligence agent, Robert Hanssen, was exposed in 2001 as a spy of long standing for the Soviets and later Russia.)

Counter-intelligence may involve the employment of double agents, the planting of false information, or other efforts to undermine the intelligence-gathering activities of foreign nations. The agency conducting counter-intelligence may, when it has detected and identified foreign intelligence operatives, elect to keep those persons in place and not expose or arrest them—at least not for a time—in order to cause further detriment to the opposing intelligence agency by passing disinformation to the operative. This is a particularly likely option if the foreign agency represents a hostile power, rather than a friendly nation.

FURTHER READING:

Davis, James Kirkpatrick. *Spying on America: The FBI's Domestic Counter-intelligence Program.* New York: Praeger, 1992.

Godson, Roy. *Dirty Tricks or Trump Cards: U.S. Covert Action and Counter-intelligence.* Washington, D.C.: Brassey's, 1995.

Olson, James M. "The Ten Commandments of Counter-intelligence." *Studies in Intelligence* no. 11 (fall-winter 2001).

Parrish, Michael. *The Lesser Terror: Soviet State Security, 1939–1953.* Westport, CT: Praeger, 1996.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* third edition. Boulder, CO: Westview Press, 1995.

SEE ALSO

Domestic Intelligence
Intelligence and Counterespionage Careers

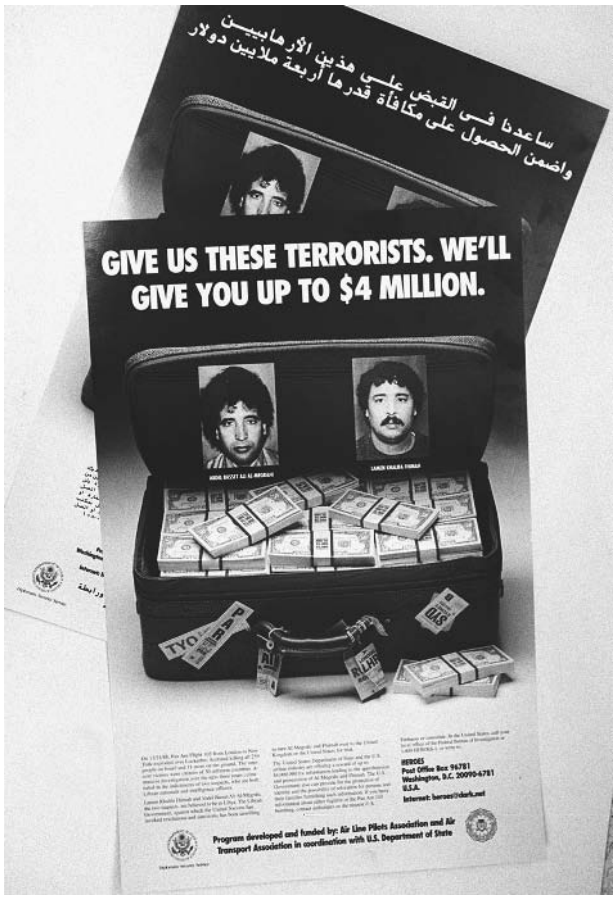
Counter-Terrorism Rewards Program

The Counter-Terrorism Rewards Program, administered by the United States Department of State offers monetary compensation for individuals who volunteer information that leads to the location, capture, and trial of suspected terrorists. The program also seeks information relevant to finances, assets, and plans of terrorist organizations. The Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA) work closely with the Department of State to investigate all information garnered through the Counter-Terrorism Rewards Program. In 1998, after the bombing of United States embassies in East Africa, the Department of State raised the maximum reward for information to $5 million.

The rewards program not only offers monetary rewards for information aiding anti-terrorism operations, but also promises confidentiality and anonymity for the informant. The United States government further promises to aid and relocate informants whose disclosure of information places themselves, and their family, in jeopardy.

The Counter-Terrorism Rewards Program is now a part of a larger anti-terrorism operation, the Rewards for Justice Program. The program pays for information relevant to the arrest and capture of wanted terrorists, both domestic and foreign. As part of the Patriot Act of 2001, the secretary of state can pay rewards greater than $5 million for information leading to the arrest of suspected terrorists. To date, the program has paid $9.75 million to 24 individuals who aided government anti-terror investigations.

The Counter-Terrorism Rewards Program, as part of Rewards for Justice, has had several key successes. Information received through the program led to the arrest and eventual conviction of the 1993 World Trade Center bomber, Ramzi Yousef. The highest current priority of the rewards program is information leading to the capture of al-Qaeda front man, Usama bin Laden, and others with suspected involvement in the 2001 attacks on the World Trade Center and the Pentagon.



Wanted posters, released in English and Arabic in 1995 by the FBI and State Department, show two suspects wanted in the bombing of Pan AM flight 103 which exploded over Lockerbie, Scotland in 1988. AP/WIDE WORLD PHOTOS.

■ FURTHER READING:

ELECTRONIC:

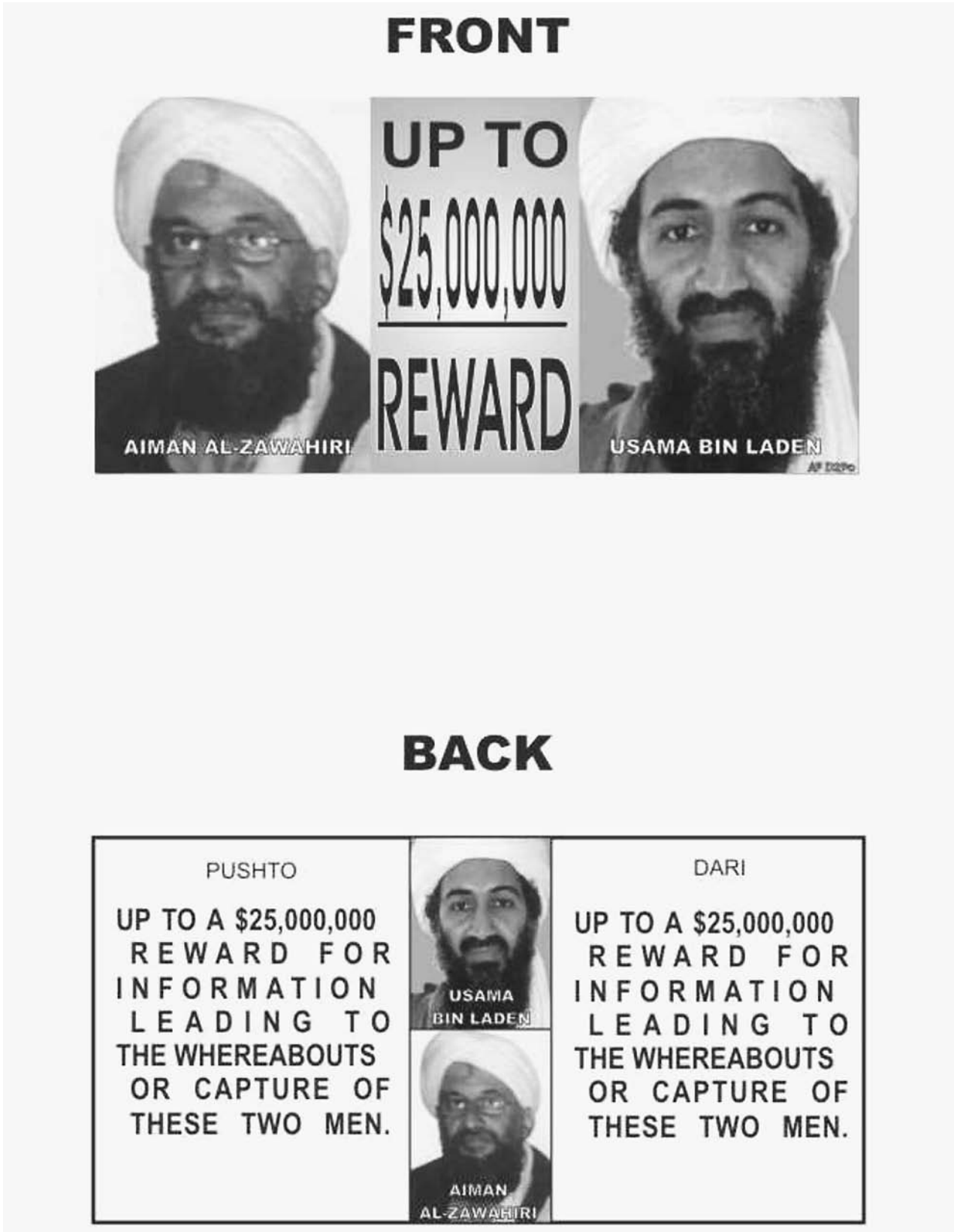
U.S. Department of State."Rewards for Justice" (April, 29, 2003)<http://www.rewardsforjustice.net/>.

SEE ALSO

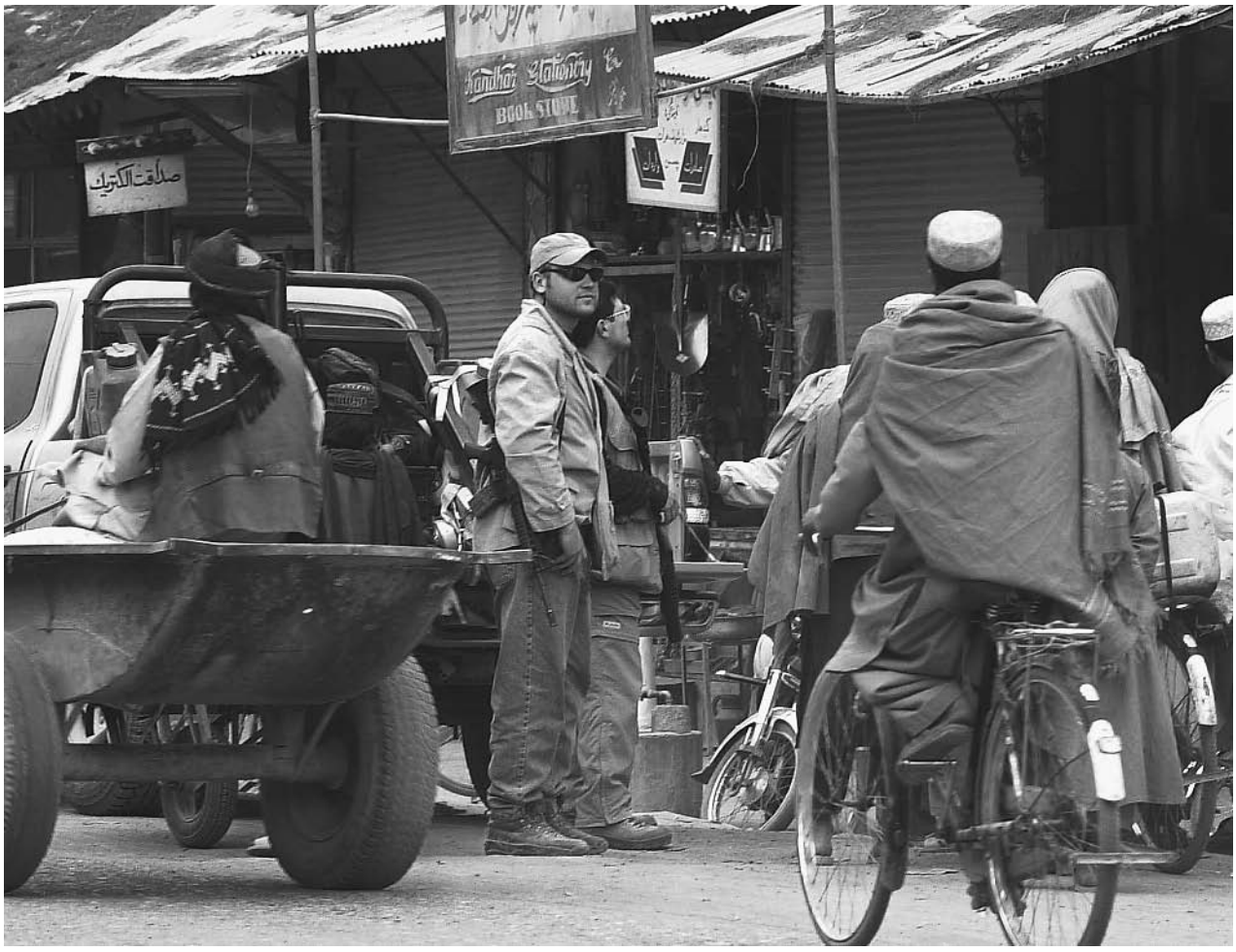
Counter-Intelligence
Homeland Security, United States Department
September 11 Terrorist Attacks on the United States

Covert Operations

Covert operations are activities carried out by an intelligence or security agency, usually in a foreign country, in such a way that it is difficult to connect that agency with its action. Laws requiring free access to government information and an assertive press have provided Americans



Leaflets dropped over Afganistan by the U.S. military advertising rewards of up to $25 million offered by the U.S. government for information leading to the capture of Usama bin Laden or his lieutenant Aiman al-Zawahiri. AP/WIDE WORLD PHOTOS.



Two members of a U.S.-led covert operations team stand in front of a downtown store in Kandahar, Afganistan in March, 2002. AP/WIDE WORLD PHOTOS.

with much knowledge about their country's participation in covert operations, particularly during the Cold War. Some scholars have interpreted this information about covert operations as evidence of an aggressive American hand played in foreign policy, while others regard the United States as the most effective nation to bear the burden of world security and political stability.

The Purpose of Covert Operations

For reasons that will be discussed below, most examinations of covert operations focus almost exclusively on U.S. covert operations, undertaken most prominently by the Central Intelligence Agency (CIA). Virtually every populated region has been the target of U.S. covert operations during the postwar era. This is particularly true of places in which the ruling regime is neither unreservedly hostile, nor unequivocally friendly, to the United States. Even a hostile regime that has failed to fully consolidate its power, such as Cuba in the period 1959–61 and Iran exactly 20 years later, may provide a promising area for covert operations.

Areas of focus in covert operations include the following: support, training and indoctrination, manipulation (including "dirty tricks"), and other covert activities. Support includes political advice to friendly parties, intelligence-gathering operations, monetary disbursements to individuals working in the service of U.S. interests, financial and technical help for pro-American political parties, and assistance to other private organizations such as labor unions and companies whose interests align with those of the United States.

Training and indoctrination areas of activity may include the dissemination of propaganda, which often must be covert in order to be effective. (An example from the late 1970s is the proliferation of editorial pieces in western European dailies that favorably compared the U.S. neutron bomb with the Soviet SS-20.) Also under this heading is the training of individuals, groups, and forces in a variety of techniques and areas of expertize.

Covert manipulation activities include economic operations, which can be designed either to destabilize the economy of a hostile power—in which case the action would qualify as a "dirty trick"—or to bolster the economy

of a friendly, but unstable nation. In the same way, paramilitary or political-action groups can be used to destabilize or overthrow a regime (a "dirty trick"), or they can help to support a pro-American government.

A Brief History of U.S. Covert Operations

During the immediate post World War II years, the focus of covert operations was Europe—primarily in the East, but also in western nations such as France or Italy, where Communists threatened to take power, and where covert operations focused on supporting anti-Communist labor unions and parties. In the East, the focus was on destabilizing Soviet-backed regimes. CIA also backed hundreds of propaganda assets, most notably Radio Free Europe, Radio Liberty, Voice of America, and Radio Free Asia, which broadcast from the Philippines to Communist China.

During the 1950s and 1960s, attention shifted to the newly emergent Third World, including Cuba, the Dominican Republic, and several nations in Central America, where Communists either tried to gain control of governments (or, in the case of Cuba, succeeded); the Congo in Africa, where the rise of Patrice Lumumba threatened to destabilize the region; and several areas in southwest Asia, most notably Iran, whose Prime Minister Mohammed Mossadegh had nationalized the Anglo-Iranian Oil Company.

The Carter years. The CIA and other organizations undertook extensive covert operations during the war in Vietnam, but the late 1970s saw a sharp decline in these activities. A number of reasons influenced this change, not least among them the exposure of questionable CIA deeds that took place during the Church Committee hearings in the U.S. Senate. It could be argued that the hearings themselves were but one aspect of a larger and generalized distrust of government power that emerged in the aftermath of the 1960s, Vietnam, and Watergate.

In addition, the administration of President James Earl Carter publicly favored openness in government, and reductions in American adventurism overseas. Even so, during this time, the CIA still undertook or supported, covert operations in such arenas as Angola, South Yemen, and Afghanistan, but there was unquestionably a greater emphasis on propaganda as opposed to direct action during the Carter years.

Reagan and Bush years. During the 1960s and 1970s, Communists had either won control, were attempting to win control, or enjoyed the support of dozens of nations in Africa, Asia, and Latin America. At the same time, the overthrow of the Shah in Iran portended the rise of another anti-American force, that of Islamic fundamentalism. Such were the challenges facing the administration of President Ronald Reagan when it took power in 1981.

Reagan responded to this situation by undertaking an array of covert operations unparalleled by that of any preceding administration. Regan stepped up covert operations and support of anti-Communist forces in Afghanistan and Angola, as well as those in El Salvador. He sought to destabilize the Vietnamese-backed Communist regime in Cambodia, as well as the Communist Sandinistas in Nicaragua. Although Reagan was particularly active in the Middle East against Iraq, Libya, and Iran, the most notorious covert operation of the Reagan years involved collusion between the CIA and the Iranian government in an arms deal that would free U.S. hostages and fund the anti-Sandinista Contras.

Although the Iran-Contra scandal served to hamstring many of Reagan's more ambitious undertakings, his covert operations did not end after the scandal broke in 1987. In 1989, successor George H. W. Bush conducted military operations against Panama's dictator, General Manuel Noriega, who was captured and imprisoned. In this action, as in the Gulf War of 1991, the actual firing of shots followed a long period of covert operations.

As with Carter, the last Democrat in the White House, President William J. Clinton pledged openness, and presented his as an administration that was above the practice of covert operations. This was a relatively easy claim to make, since the end of the Cold War obviated many of Reagan's and Bush's undertakings. Furthermore, like the Church Committee hearings, the Iran-Contra affair served to bring the operations of the intelligence establishment under public scrutiny. Clinton's administration, however, was one characterized by virtually unprecedented military adventurism, under a variety guises: humanitarian support in Somalia, nation-building in Haiti, and countering an aggressive, genocidal force in Bosnia and Yugoslavia. In each case, military action would have been much more difficult and costly without covert operations providing advance intelligence.

Eight months into his administration, President George W. Bush declared war on terrorism soon after the terrorist attacks of September 11, 2001. The twentieth century was over, and with it both the Cold War and the post-Cold War era. The war on terror began with the bombing of Afghanistan on October 7, 2001, but by then, the CIA and other organizations had long since paved the way with extensive covert operations on the ground.

■ FURTHER READING:

BOOKS:

Borosage, Robert, and John D. Marks. *The CIA File.* New York: Grossman, 1976.

Knott, Stephen F. *Secret and Sanctioned: Covert Operations and the American Presidency.* New York: Oxford University Press, 1996.

Marshall, Jonathan, Peter Dale Scott, and Jane Haapiseva-Hunter. *The Iran-Contra Connection: Secret Teams and Covert Operations in the Reagan Era.* Boston: South End Press, 1987.

Prados, John. *President's Secret Wars: CIA and Pentagon Covert Operations since World War II.* New York: William Morrow, 1986.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* third edition. Boulder, CO: Westview Press, 1995.

SEE ALSO

Bay of Pigs
Church Committee
CIA (United States Central Intelligence Agency)
Vietnam War

CPNB (Chemical and Biological National Security Program).

SEE *NNSA (United States National Nuclear Security Administration).*

Crib

A crib is a section of an encoded or enciphered message that can easily be rendered into plain text, thus providing a tool whereby a skilled cryptanalyst can crack the entire code or message. A famous example of a "crib" from outside the world of espionage is the Rosetta Stone, used to translate Egyptian hieroglyphics.

Essentially a thank-you note from a group of priests to a magnanimous king, the stone was addressed to the second-century B.C. ruler Ptolemy V, who, like all the Ptolemies, spoke Greek rather than Egyptian. Therefore, the priests sent the note in Greek, as well as in hieroglyphics and demotic, a simplified version of hieroglyphic writing. Thus the French archaeologist Jean-François Champollion, who studied the Rosetta Stone in the early nineteenth century, was able to translate the Greek portion, and from this crack the code first of demotic, and then of hieroglyphics.

Any time a force sends out a message whose content is predictable to the enemy, this offers an opportunity for a resourceful cryptanalyst to find a crib. Thus, when the German high command in World War II sent greetings to Adolf Hitler every April 20—the Fuhrer's birthday—it was fairly easy for Allied cryptanalysts to guess the gist of the message. This would have been so no matter how carefully it had been enciphered or encoded, but the Germans sometimes made things even easier by sending the same message in plain text.

■ FURTHER READING:

BOOKS:

Kahn, David. *Kahn on Codes: Secrets of the New Cryptology.* New York: Macmillan, 1983.

Konheim, Alan G. *Cryptography: A Primer.* New York: Wiley, 1981.

Lubbe, J. C. A. van der. *Basic Methods of Cryptography.* New York: Cambridge University Press, 1998.

Newton, David E. *Encyclopedia of Cryptology.* Santa Barbara, CA: ABC-CLIO, 1997.

SEE ALSO

ADFGX Cipher
Cryptology, History

Crime Prevention, Intelligence Agencies

The relationship between law enforcement agencies such as the Federal Bureau of Investigation (FBI) and intelligence is straightforwardly recognized, as exemplified by the fact that the FBI is regularly involved in intelligence and counterintelligence activities. Less obvious, however, is the interaction between operations such as the Central Intelligence Agency (CIA) and crime prevention or law enforcement. Although most activities of intelligence organizations are by definition secret, it is at least possible to discern the outlines of a positive correlation between intelligence and crime prevention activities. In the case of police states and terrorist organizations, the relationship between intelligence and crime prevention—or, for covert operations in enemy countries, intelligence and the promotion of crime—is even easier to demonstrate.

Totalitarian societies and radical movements. One of the means to appreciate the interaction between intelligence and/or covert operations on the one hand, and crime prevention on the other, is to observe the example of totalitarian nations and the radical movements associated with them. In nations such as those of the Soviet bloc before the end of the Cold War, the presence of an intelligence-gathering entity such as the KGB was so pervasive that it had the side effect of virtually minimizing ordinary crime. While in the last two decades of the Soviet era, the

black market became an increasingly significant facet of daily life. In the centralized command economy that prevailed at that time, it was by definition a criminal enterprise to engage in the buying and selling of goods through channels other than those overseen by state authorities. Yet, as the Soviet economy declined, the black market became virtually the only means whereby individuals could obtain basic goods, let alone luxury items. This was true even of party apparatchiks other than the highest officials, and for this reason, the black market became the beneficiary of benign neglect on the part of Soviet authorities.

With the exception of the forms of commerce encompassed by the black market, however—and most such commerce would not be deemed criminal in a liberal democracy—the Soviet Union and its Eastern European satellites seem to have had a much lower crime rate than the United States and Western Europe over a comparable period. The obvious explanation for this difference, particularly when European countries are compared to make up for cultural differences, is the existence of a pervasive information-gathering apparatus. With spies, cameras, bugs, and tape recorders pervasive throughout society, criminal activity was unlikely to flourish unless it enjoyed official sanction.

Promoting crime in liberal democracies. Opposite to this obvious relationship between totalitarian societies, intelligence, and crime prevention is that between totalitarian or radical movements, intelligence, and the promotion of crime in liberal democracies. The founder of the Soviet state, V. I. Lenin, is credited as saying that "The enemy will sell us the rope with which we will hang him." Lenin's statement may have been too modest: based on the apparent relationship between the Soviet Union, allied movements and nations, and illegal activity in the West during the 1970s and 1980s, it appears in some cases that, to paraphrase Lenin, the enemy actually paid for the rope himself.

Although rumors of CIA involvement in the drug trade have long been fodder for conspiracy theories of various ideological stripes, a more well-established relationship has existed between communist nations, particularly Cuba, and the traffic in illegal drugs. The same is true of the Islamic fundamentalist regime of the Taliban in Afghanistan, who controlled much of the heroin trade prior to their overthrow in 2001. Some of this activity, especially that of nongovernmental entities, falls under the category of narcoterrorism, defined by the Drug Enforcement Administration (DEA) as terrorism undertaken by groups directly or indirectly involved in producing, transporting, or distributing illegal drugs.

Whereas authoritarian and totalitarian governments deal harshly with drug traffickers inside their borders, selling drugs to Western nations serves a number of purposes. On the most basic level, it funds the activities of revolutionary armies and terrorist groups such as al-Qaeda, or the Havana-aligned FARC rebels in Colombia. The drug trade also forces liberal democracies to allocate additional resources toward a "war on drugs," and, by encouraging the behaviors associated with drug use, ultimately exerts a deleterious effect on the fabric of society. In such a way, encouragement of crime in a liberal democracy is a form of covert operation on behalf of an enemy state or movement.

Intelligence and crime prevention in Democracies. Ironically, the relationship between intelligence and crime prevention in open societies is more difficult to demonstrate. In part, this is because CIA and other organizations have far less influence on daily life in the United States than do intelligence organizations within a highly controlled political system. Still, the link between hostile governments or movements on the one hand, and crime on the other, has led U.S. authorities to increasingly link crime prevention and intelligence.

This is particularly so in the post-September 2001 world, in which the relationship between Islamist fundamentalist terrorism and the heroin trade has been clearly established. Even before that time, however, the CIA and FBI were working together and expanding operations overseas, in an effort to battle narcoterrorism. According to an April 1995 report in the *New York Times,* both agencies, along with the federal government, had begun to treat global crime as a national security issue.

The CIA has also taken an interest in crime-prevention tactics of domestic law enforcement. This is true not just on a federal level, but even—in the case of a New York City program—on a municipal level. In November 1999, CIA director George Tenet visited police headquarters in lower Manhattan to observe the operations of Compstat, a computerized statistical program whereby the New York Police Department monitors crime block by block. According to the *New York Times,* the agency was considering use of such a system to monitor entire foreign nations as a means of predicting potential unrest.

FURTHER READING:

PERIODICALS:

Blair, Jayson. "C.I.A. Chief Slips in to Study Police Department Program." *New York Times.* (November 6, 1999): section B, p. 2.

Gedda, George. "CIA Probes Cuban Link to Drug Trade." *Associated Press.* August 16, 1999.

Johnston, David. "Strength Is Seen in a U.S. Export: Law Enforcement." *New York Times.* (April 17, 1995): A1.

Kushner, Harvey W. "Can Security Measures Stop Terrorism?" *Security Management* 40, no. 6 (June 1996): 132.

SEE ALSO

Customs Service, United States

DEA (Drug Enforcement Administration)
FBI (United States Federal Bureau of Investigation)

Critical Infrastructure

Critical infrastructure is a general term for physical and computer-based systems essential to the functions of the government and economy. Among these are telecommunications, energy, banking and finance, transportation, water systems, and emergency services. The expression *critical infrastructure* entered the language of policymakers in the mid-1990s, as it became increasingly apparent that the United States depended on a network of systems that collectively constituted its physical engine, and that these systems were potentially as vulnerable as they were valuable.

Components of critical infrastructure. Included under the heading of critical infrastructure are highways, airports and aircraft, trains and railways, bus lines, shipping and boat lines, transport, trucking systems, and supply networks for basic goods, electric power plants and lines, along with oil and gas lines and utilities of all kinds, including water and sewer systems, land and cell phone systems, computer networks, television, and radio (not only that which is publicly accessible, but that controlled by private or government entities in special networks or on special frequencies), banks and other financial institutions, and security, fire, hospital, and emergency services.

Each element of critical infrastructure is so vital that if it were removed from the equation, even temporarily, the entire nation would experience monumental repercussions. Even when the infrastructure of a particular area is threatened, the results can be disastrous. To this day, people alive at the time remember the northeastern electrical blackout of 1965, or the New York City blackout of 1977. Today, the critical systems that run the engine of America are far more interlinked than they were even in the 1970s, and this interdependence carries with it new vulnerabilities.

Responding to the challenge. Recognition of these vulnerabilities led to the creation of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office, as well as the integration of critical infrastructure elements of disparate departments and agencies at the federal level. It has also led to the creation of critical infrastructure protection offices by state and local governments, and by the U.S. private sector. In other parts of the industrialized world, such as Canada, concerns over critical infrastructure have led to the establishment of new departments and offices.

Protection of critical infrastructure in the United States became even more of an issue after the September 11, 2001, terrorist attacks. Though some of the measures taken have invoked the ire of civil libertarians who decry the loss of information access, and limitations on movement, faced by ordinary citizens, it is likely that the future will see even more stringent protections over the systems critical to the functioning of modern America.

FURTHER READING:

BOOKS:

Cordesman, Anthony H., and Justin G. Cordesman. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland.* Westport, CT: Praeger, 2002.

Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection. Washington, D.C.: The Commission, 1997.

Zukin, Sharon. *Landscapes of Power: From Detroit to Disney World.* Berkeley: University of California Press, 1991.

PERIODICALS:

Ingram, Gregory. "Roundtable Discussion: Critical Issues in Infrastructure in Developing Countries." *Work Bank Research Observer* (1993): 473.

Lukasik, S. J., J. T. Goldberg, and S. E. Goodman. "Protecting an Invaluable and Ever-Widening Infrastructure." *Association for Computing Machinery* 41, no. 6 (June 1998): 11–16.

Robinson, C. Paul, Joan B. Woodward, and Samuel G. Varnado. "Critical Infrastructure: Interlinked and Vulnerable." *Issues in Science and Technology* 15, no. 1 (fall 1998): 61–67.

ELECTRONIC:

Partnership for Critical Infrastructure Security. <http://www.pcis.org> (February 27, 2003).

SEE ALSO

Critical Infrastructure Assurance Office (CIAO), United States

Critical Infrastructure Assurance Office (CIAO), United States

Created by Presidential Decision Directive 63 (PDD 63) in 1998, the Critical Infrastructure Assurance Office (CIAO) of the United States Department of Commerce (DOC) has the responsibility of coordinating security for energy, financial services, transportation, telecommunications, and other

A view of chain-locked gates leading to an area of critical infrastructure, the underground Pentagon near Founatin Dale, Pennsylvania. The facility was built inside a mountain as a second central command structure if needed during wartime. AP/WIDE WORLD PHOTOS.

major systems at the federal level. After the terrorist attacks of September 11, 2001, its mission became even more critical to national security, and in early 2003 it was incorporated into the newly created Department of Homeland Security (DHS).

In May 1998, President William J. Clinton signed PDD 63. The latter called for new measures to protect critical infrastructures, which it defined as those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.

Among the specific policy measures of PDD 63 was the creation of CIAO, a section of DOC designed to have a life span of three years. During that time, CIAO would conduct a study of the federal government's dependence on, and vulnerabilities with regard to, critical infrastructures.

CIAO continued to exist beyond the term of its mandate, and three and a half years after its creation, its mission gained new impetus in the wake of the September 2001 terrorist attacks. On October 16, 2001, President George W. Bush signed Executive Order 13231, "On Critical Infrastructure Protection," which established the Critical Infrastructure Protection Board (CIPB), and appointed the director of CIAO as a member of both the board and its coordination committee. On March 1, 2003, CIAO was moved from DOC to the newly created DHS.

FURTHER READING:

PERIODICALS:

Frank, Diane. "Cybersecurity Center Takes Shape." *Federal Computer Week* 16, no. 4 (February 18, 2002): 10.

Piazza, Peter. "Sunset of the CIAO? Industry May Decide." *Security Management.* 44, no. 11 (November 2000): 36.

ELECTRONIC:

Critical Infrastructure Assurance Office. <http://www.ciao.gov> (January 28, 2003).

SEE ALSO

Commerce Department Intelligence and Security Responsibilities, United States
Critical Infrastructure Assurance Office (CIAO), United States
Infrastructure Protection Center (NIPC), United States National

Croatia, Intelligence and Security

Following World War I, the ethnic nations in the Balkan region were unified into a single state, known after 1929 as Yugoslavia. Tensions between the various ethnic populations remained high, and the government unstable. After World War II, Marshal Tito, who established a strong-handed communist dictatorship, seized the Yugoslav government. The Yugoslavian governmental intelligence was dominated by secret police forces and government-backed political espionage. Modeled after intelligence and security forces in the Soviet Union, Yugoslav intelligence focused on protecting the ruling regime under the direct control of the Communist Central Committee.

In the 1990s, Yugoslavia broke apart following the fall of the Soviet Union. Croatia was the first province to declare its independence in 1991. Border disputes and ethnic tensions flared in the region, sparking intense warfare. When fighting eased after the intervention of UN peacekeepers, Croatia began its struggle to overcome the legacy of decades of communist dictatorship. The intelligence community was a primary target of initial reforms. Though the old secret police were disbanded, and new agencies sought to distance themselves from the legacy of their predecessors, the process of rebuilding intelligence and security services continues to be problematic in Croatia.

Between 1990 and 2003, the Croatian intelligence community altered its structure several times. As of 2003, twelve departments, in two government ministries, comprise the Croatian intelligence services. The main civilian agency, under the direction of the Ministry of the Interior, is the Croatian Intelligence Service (HIS). HIS operations deal exclusively with the collection and analysis of foreign intelligence. However, the agency also performs the bureaucratic function of coordinating the efforts of all civilian intelligence operations, and processing information gathered by various agencies for dissemination to government officials.

Aiding the HIS with coordination of intelligence operations is the National Security Office (UNS). The UNS also distributed necessary intelligence information to the government and oversees the operations of various intelligence agencies in Croatia. The UNS further coordinates joint efforts between the intelligence and law enforcement communities to act neutralize potential threats to national security. Many of Croatia's specific intelligence units, such as Communications Intelligence and Counter- intelligence force, are subsidiaries of the UNS.

A small agency, the Security Intelligence Service (OBS), conducts intelligence operations against neighboring Balkan nations, most especially Serbia and Montenegro. The agency constantly provides other intelligence and security forces with information on regional ethnic tensions, arms trafficking and stockpiling by various groups, and the strength and operations of other regional intelligence services.

The Croatian military, under the direction of the Ministry of Defense, also maintains specially trained intelligence forces, embedded in the each service branch. The small Croatian Navy collects signals, communications, and remote intelligence. The significantly larger Army Intelligence Force aids civilian intelligence operations, as well as collects information on foreign militaries. Both military and civilian intelligence forces are chard with the preservation of national security and the protection of Croatian government officials at home and abroad.

Even after U.N. intervention in the Balkan Peninsula, sporadic fighting between rival ethnic interests, and diplomatic disagreements between Croatia and neighboring states, remain endemic. Croatian government and economic reforms have made the nation the strongest in the region, with increasing participation in international organizations.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. The World Factbook, 2002. "Croatia" <http://www.cia.gov/cia/publications/factbook/geos/hr.html; (March 30, 2003).

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
World War I
World War II

Cruise Missile

Cruise missiles come in several varieties, the most well known being the Tomahawk. Operating rather like a

The destroyer USS *Porter* (DDG78) launches a Tomahawk Land Attack Missile toward Iraq on March 22, 2003, during Operation Iraqi Freedom; the missile struck a government communications site in Baghdad. AP/WIDE WORLD PHOTOS.

pilotless airplane, these missiles have powerful guidance systems that make them capable of hitting precise targets from a great distance. Operated by the United States Air Force and Navy, cruise missiles can be deployed from aircraft, submarines, and destroyers.

Of the two most notable types of cruise missile, the Tomahawk, most often used by the Navy, is 18 feet, 3 inches (5.56 m) long and weighs 2,900 pounds (1,315 kg). The Air Force AGM-86B/C weighs 3,150 pounds (1,429 kg) and measures 20 feet, 9 inches (6.3 m). The AGM, first deployed (as an 86B) in December 1982, is an air-to-ground strategic cruise missile, while the Tomahawk, which first saw service in 1986, is a long-range subsonic cruise missile for striking high-value or heavily defended land targets. Both have gone through several changes, including the introduction of the Tactical Tomahawk, to be launched from forward-deployed ships and submarines, in 2004.

A cruise missile includes a solid rocket booster, which makes up approximately fifteen percent of its weight at launch. Once it has burned its fuel, the booster falls away and the missile's wings, tail fins, and air inlet unfold. From that point until it reaches its target, the missile is powered by its turbofan engine. In flight, the cruise missile has a speed of about 550 miles per hour (880 kph).

Neither size nor speed nor rocket booster systems define the cruise missile as much as its accuracy. The Tomahawk has a range of 870 nautical miles (1,000 statute miles, or 1,609 km), and the AGM more than 1,500 miles (2,400 km) or more—the exact figure is classified—yet both are capable of hitting a target the size of a truck. Guiding these missiles are four different systems: the inertial guidance system, which detects changes in the missile's motion; terrain contour matching, which applies a three-dimensional database of the terrain over which the missile flies; global positioning system (GPS), which includes both military satellites and an onboard GPS receiver; and digital scene matching area correlation, which switches on once the missile nears its target, using an image correlator and a camera to locate the target.

■ FURTHER READING:

BOOKS:

Gormley, Dennis. *Dealing with the Threat of Cruise Missiles.* New York: Oxford University Press for the International Institute for Strategic Studies, 2001.

Huisken, Ronald. *The Origin of the Strategic Cruise Missile.* New York: Praeger Publishers, 1981.

Werrell, Kenneth P. *The Evolution of the Cruise Missile.* Maxwell Air Force Base, AL: Air University Press, 1985.

ELECTRONIC:

Fact Sheet: AGM-86B/C Missiles. U.S. Air Force. <http://www.af.mil/news/factsheets/AGM_86B_C_Missiles.html> (April 7, 2003).

How Cruise Missiles Work. Howstuffworks.com. <http://www.howstuffworks.com/cruise-missile.htm> (April 7, 2003).

Navy Facts: Tomahawk Cruise Missile. U.S. Navy Office of Information. <http://www.chinfo.navy.mil/navpalib/factfile/missiles/wep-toma.html> (April 7, 2003).

SEE ALSO

Ballistic Missiles
Ballistic Missile Defense Organization, United States
GPS
Patriot Missile System
Strategic Defense Initiative and National Missile Defense
Undersea Espionage: Nuclear vs. Fast Attack Subs

Cryo3 Detector.

SEE *Lawrence Berkeley National Laboratory.*

Cryptology and Number Theory

■ K. LEE LERNER

Cryptography is a division of applied mathematics concerned with developing schemes and formula to enhance the privacy of communications through the use of codes. More specifically, cryptography is the study of procedures that allow messages or information to be encoded (obscured) in such a way that it is extremely difficult to read or understand encoded information without having a specific key (i.e., procedures to decode) that can be used to reverse the encoding procedure.

Cryptography allows its users, whether governments, military, businesses or individuals, to maintain privacy and confidentiality in their communications. The goal of every cryptographic scheme is to be "crack proof" (i.e, only able to be decoded and understood by authorized recipients). Cryptography is also a means to ensure the integrity and preservation of data from tampering. Modern cryptographic systems rely on functions associated with advanced mathematics, number theory that explores the properties of numbers and the relationships between numbers.

Encryption systems can involve the simplistic replacement of letters with numbers, or they can involve the use of highly secure "one-time pads" (also known as Vernam ciphers). Because one-time pads are based upon codes and keys that can only be used once, they offer the only "crack proof" method of cryptography known. The vast number of codes and keys required, however, makes one-time pads impractical for general use.

Many wars and diplomatic negotiations have turned in the ability of one combatant or country to read the supposedly secret messages of its enemies. The use of cryptography has broadened from its core diplomatic and military users to become of routine use by companies and individuals seeking privacy in their communications. Governments, companies and individuals required more secure systems to protect their databases and email.

In addition to improvements made to cryptologic systems based on information made public from classified government research programs, international scientific research organizations devoted exclusively to the advancement of cryptography (e.g., the International Association for Cryptologic Research (IACR)), began to apply applications of mathematical number theory to enhance privacy, confidentiality, and the security of data. Applications of number theory were used to develop increasingly involved algorithms (i.e., step-by-step procedures for solving a mathematical problems). In addition, as commercial and personal use of the Internet grew, it became increasingly important, not only to keep information secret, but also to be able to verify the identity of message sender. Cryptographic use of certain types of algorithms called "keys" allow information to be restricted to a specific and limited audiences whose identities can be authenticated.

Mathematical Operations

In some cryptologic systems, encryption is accomplished, for example, by choosing certain prime numbers and then products of those prime numbers as a basis for further mathematical operations. In addition to developing such mathematical keys, the data itself is divided into blocks of specific and limited length so that the information that can be obtained even from the form of the message is limited. Decryption is usually accomplished by following an elaborate reconstruction process that itself involves unique mathematical operations. In other cases, decryption is accomplished by performing the inverse mathematical operations performed during encryption.

In the late 1970s, government intelligence agencies and Ronald Rivest, Adi Shamir, and Leonard Adleman published an algorithm (the RSA algorithm) destined to become a major advancement in cryptology. The RSA

algorithm underlying the system derives its security from the difficulty in factoring very large composite numbers. The RSA algorithm was the mathematical foundation for the development of a public two-key cryptographic system called Pretty Good Privacy (PGP).

Applications of number theory allow the development of mathematical algorithms which can make information (data) unintelligible to everyone except for intended users. In addition, mathematical algorithms can provide real physical security to data—allowing only authorized users to delete or update data. One of the problems in developing tools to crack encryption codes involves finding ways to factor very large numbers. Advances in applications of number theory, along with significant improvements in the power of computers, have made factoring large numbers less daunting.

In general, the larger the key size used in a system systems, the longer it will take computers to factor the composite numbers used in the keys.

Specialized mathematical derivations of number theory such as theory and equations dealing with elliptical curves are also making an increasing impact on cryptology. Although, in general, larger keys provide increasing security, applications of number theory and elliptical curves to cryptological algorithms allow the use smaller keys with any loss of security.

Advancements in number theory are also used to crack important cryptologic systems. Attempting to crack encryoption codes (the encryption procedures) often requires use of advanced number theories that allow, for instance, an unauthorized user to determine the product of the prime numbers used to start the encryption process. Factoring this product is, at best, a time consuming process to determine the underlying prime numbers. An unsophisticated approach, for example, might be to simply attempt or apply all prime numbers. Other more elegant attempts involve algorithms termed quadratic sieves, a method of factoring integers, developed by Carl Pomerance, that is used to attack smaller numbers, and field sieves algorithms that are used in attempts to determine larger integers. Advances in number theory allowed factoring of large numbers to move from procedures that, by manual manipulation, could take billions of years, to procedures that—with the use of advanced computing—can be accomplished in weeks or months. Further advances in numbertheory may lead to the discovery of a polynomial time factoring algorithm that can accomplish in hours what now takes months or years of computer time.

Advances in factoring techniques and the expanding availability of computing hardware (both in terms of speed and low cost) make the security of the algorithms underlying cryptologic systems increasingly vulnerable.

These threats to the security of cryptologic systems are, in some regard, offset by continuing advances in design of powerful computers that have the ability to generate larger keys by multiplying very large primes. Despite the advances in number theory, it remains easier to generate larger composite numbers than it is to factor those numbers.

Other improvements related to applications of number theory involve the development of "non-reputable" transactions. Non-reputable means that parties can not later deny involvement in authorizing certain transactions (e.g., entering into a contract or agreement). Many cryptologists and communication specialists assert that a global electronic economy is dependent on the development of verifiable and non-reputable transactions that carry the legal weight of paper contracts. Legal courts around the world are increasingly faced with cases based on disputes regarding electronic communications.

FURTHER READING:

BOOKS:

Burn R. P. *A Pathway into Number Theory,* 2nd. ed. New York: Cambridge University Press, 1997 .

Niederreiter, Harald. *Mathematical Foundations of Coding and Cryptology.* Singapore: World Scientific Press, 2003 .

Wagstaff, Samuel S., Jr., *Cryptanalysis of Number Theoretic Cyphers* Boca Raton, FL: CRC Press, 2002 .

SEE ALSO

Cryptology, History
Cryptonym

Cryptology, History

JUDSON KNIGHT

Cryptology is the study of both cryptography, the use of messages concealed by codes or ciphers, and cryptanalysis, or the breaking of coded messages. It is nearly as old as civilization itself, although ciphers and codes prior to the late medieval period in western Europe tended to be extremely simple by today's standards. Advances in mathematics made possible the development of ever more sophisticated systems. Further improvements in cryptology accompanied the creation of modern standing armies and intelligence services during the nineteenth century. Following the world wars and the creation of the computer, cryptology entered a far more advanced stage, resulting in the creation of codes and ciphers so sophisticated that virtually no amount of human genius unaided by computer technology can break them.

Ancient Cryptology

Early examples of cryptology can be found in the work of Mesopotamian, Egyptian, Chinese, and Indian scribes. In those four cradles of civilization, which emerged during

Cryptography on display at the National Cryptologic Museum in Ft. Meade, Maryland. ©RUBIN STEVEN/CORBIS SYGMA.

the period between 3500 and 2000 B.C., few people could read and write, therefore, written language was a secret code in itself. Further concealment of meaning behind opaque hieroglyphs, cuneiform, or ideograms served to narrow the intended audience even further.

The specialization of writing skills served, in two cases, to prevent the transmission of these skills to later generations. Knowledge of hieroglyphic writing in Egypt died out, and without the discovery and deciphering of the Rosetta Stone in the early nineteenth century, translation of Egyptian texts would probably have not occurred until the computer age—if at all. The fact that the written language of the Indus River valley civilizations in ancient India remains to be translated serves as proof that computers cannot solve all cryptologic questions without a crib or key.

Greece and Rome. Modern scholars know a great deal more about cryptologic systems in Greece and Rome than in earlier civilizations. The Spartans in about 400 B.C. used a cryptographic system called a *scytale,* whereby a sheet of papyrus was wrapped around a staff, a message was written down the length of the staff, and then the papyrus was unwrapped. In order to read the message properly, the recipient had to have a staff of exactly the same diameter.

Two centuries later, the Greek historian Polybius introduced what became known as the Polybius square, a 5 x 5 grid that used the 24 letters of the Greek alphabet—a model for the ADFGX cipher used by the Germans in World War I. Julius Caesar in the first century B.C. employed one of the first known ciphers, a system that involved a shift three letters to the right: for example, a plain text *Z* would become a *C,* an *A* a *D,* and so on.

Medieval Cryptology

Progress in cryptology—as with most other areas of study—came to a virtual standstill between the decline of the Roman Empire in the third century and the rise of Islam in the seventh. Arab scholars pioneered cryptanalysis, the solving of ciphers or codes without the aid of a key, from the eighth century onward. In 1412, al-Kalka-shandi published a treatise in which he introduced the technique, later made famous to popular audiences by Edgar Allan Poe in "The Gold Bug," of solving a cipher based on the relative frequency of letters in the language.

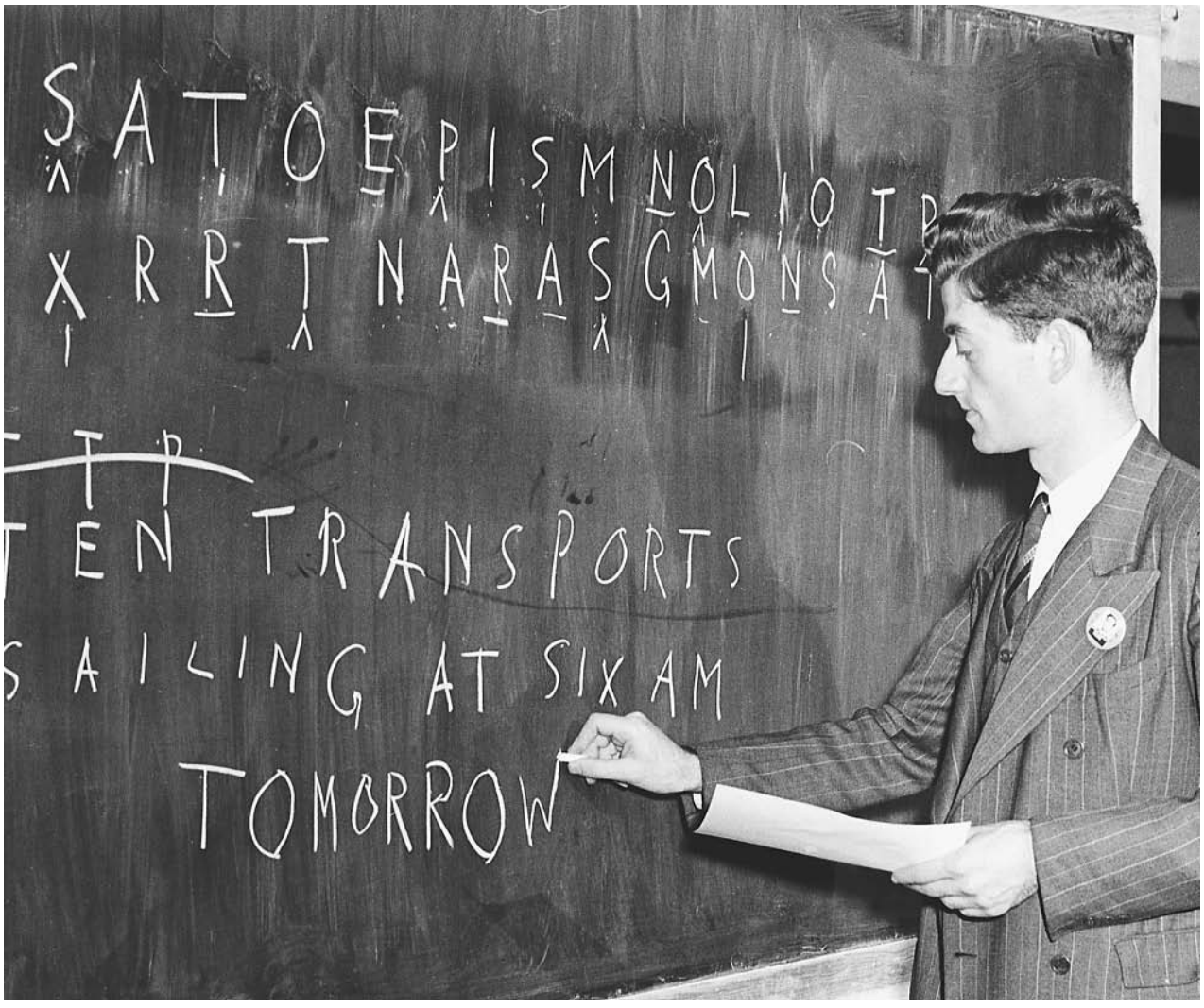
By that time, cryptology had begun to advance again in Europe, where the Italian city states used secret codes for their diplomatic messages in the fourteenth century. Messages were carried on horseback, and even in peacetime, the roads of Europe were plagued with highway robbers, so secrecy in communication was of the utmost importance.

Progress in mathematical learning from the twelfth century onward aided these advances. In the early thirteenth century, Italian mathematician Leonardo Fibonacci introduced the Fibonacci sequence, wherein each number is the sum of the previous two: 1, 1, 2, 3, 5, 8, and so on. Fibonacci's sequence would prove highly influential in cryptology: even in the late twentieth century, some cryptologic systems relied on an electronic machine called a Fibonacci generator, which produced numbers in a Fibonacci sequence.

In the late fifteenth century, another influential Italian mathematician, Leon Battista Alberti, published a work in which he introduced the idea of a cipher disk. The latter is a device for encoding and decoding messages by use of concentric wheels imprinted with alphabetic and numeric characters. Even in the late nineteenth century, cryptographers were using cipher disks based on the model pioneered by Alberti.

The Early Modern Era (1500–1900)

Due to its secret nature, cryptography—a word based on Greek roots meaning "secret writing"—had long been



This worker in the office of postal censorship in New York City, in 1942, deciphers a coded message found in a letter. ©BETTMANN/CORBIS.

associated with the occult, and one occultist who advanced the art was the early sixteenth-century German monk Trithemius. Trithemius developed a table in which each row contained all the letters of the alphabet, but each successive row was shifted over by one letter. The first letter of plain text would be encrypted using the first line, the second letter using the second line, and so on. Late in the 1500s, French cryptographer Blaise de Vigenère adapted the Trithemius table for his own Vigenère table, which in the twentieth century became the basis for the widely used data encryption standard, or DES.

By the eighteenth and early nineteenth centuries, cryptography had become widely used in Europe, where governments employed special offices called "black chambers" to decipher intercepted communications. In America, Thomas Jefferson developed an early cipher wheel, and in the 1840s, Samuel F. B. Morse introduced a machine that would have a vast impact on cryptology: the telegraph. Up to this time, all encoded or enciphered communication had been written and carried by hand, and the telegraph marked the first means of remote transmission. It also employed one of the most famous codes in the world, the Morse code, and helped influence widespread popular interest in cryptography. (It is no accident that Poe's fictional writing on cryptology coincided with this era.)

In the 1850s, Charles Wheatstone and Lyon Playfair introduced the Playfair system, which used a Polybius square and encrypted letters in pairs. This pairing made deciphering more difficult, since it was less easy to see how frequently certain letters appeared. The Playfair system proved so effective that the Allies used it in limited form against the Japanese during World War II. Despite these advances of the era, cryptography was still far from advanced during the American Civil War. The Confederacy was so disadvantaged in the realm of cryptanalysis that its government sometimes published undeciphered Union messages in newspapers with a request for readers' help in deciphering them.

A Korean War veteran examines a display explaining how cryptology was used to intercept North Korean radio transmissions during the Korean War at the National Cryptologic Museum in Ft. Meade, Maryland. AP/WIDE WORLD PHOTOS.

The Twentieth Century

In the early twentieth century, another invention, the radio, had a profound effect on cryptography by greatly improving the capacity of senders to transmit messages to remote areas. World War I marked a watershed in cryptography. Not only was it the first major conflict in which radio was used, it was the last in which a great power failed to employ cryptographic communications. On the Eastern Front, the Russians sent uncoded messages that were easily interpreted by Russian-speaking intelligence officers on the German and Austrian side, leading to a massive victory for the Central Powers at Tannenberg in 1914.

The war also marked the debut of the Germans' ADFGX cipher, which was so sophisticated that French cryptanalysts only deciphered it for one day, after which the Germans again changed the key. But the cryptographic dimension of the war did not belong entirely to the Central Powers. British signal intelligence cracked the German cipher, and intercepted a message from German foreign minister Arthur Zimmermann to the Mexican president, promising to return territories Mexico had lost to the

United States in the Mexican War if the country attacked the United States. Informed of the Zimmermann telegram, President Woodrow Wilson declared war on Germany.

Also in 1917, American engineer Gilbert S. Vernam developed the first significant automated encryption and decryption device when he brought together an electromagnetic ciphering machine with a teletypewriter. A year later, Major Joseph O. Mauborgne of the U.S. Army devised the one-time pad, whereby sender and received possess identical pads of cipher sheets that are used once and then destroyed—a virtually unbreakable system. World War I also saw the development of a cipher machine by Edward Hebern, who tried to sell his idea to the U.S. Navy. The Navy rejected Hebern's system, which was later taken by the Japanese and used in World War II. By the time of that war, Hebern had developed Mark II (SIGABA), which became the most secure U.S. cipher system during the conflict.

Allied cryptologic victories against the Axis in World War II have long been celebrated in the intelligence community, and few have received more acclaim that the cracking of the German Enigma code. The Germans' Enigma machine, invented by German electrical engineer Arthur Scherbius around the same time Hebern introduced his device, was a complex creation in which the variable settings of rotors and plugs determined the keys. Solving it was a major victory for the Allies, who kept secret the fact that they had cracked the system so as to keep exploiting it. Cracking of codes also aided victories in North Africa and the Pacific. At the same time, American use of codetalkers transmitting enciphered messages in the Navajo Indian language made their transmissions indecipherable to the Japanese.

The computer age. American cryptologic work during World War II had contributed to the development of a machine, the computer, which would revolutionize cryptology to an even greater extent than the telegraph or radio had previously. Most cryptologic advances since the war have involved, or made use of, computers. A quarter-century after the war's end, in the early 1970s, American electrical engineers Martin Hellman and Whitfield Diffie introduced the idea of asymmetric or public-key ciphers, which are extremely hard to crack. This led to the development of the RSA algorithm (named for its creators, Rivest, Shamir, and Adelman) at the Massachusetts Institute of Technology in 1977.

Also in 1977, the U.S. federal government introduced DES, a transposition-substitution algorithm so complex that it seemed a safe means of guarding computer data. Given the fact that DES had some 2^{56} possible keys (a number roughly equivalent to a 1 followed by 17 zeroes), it had seemed unbreakable at the time. By the early 1990s, however, vast increases in the processing speed of computers had made it possible for hackers to break DES using "brute-force" means—that is, trying every possible value for a given cipher until finding a solution. To guard against these attacks, new Advanced Encryption Standard (AES) algorithms were developed to replace DES.

Advances in computers, and in communication by electronic means over the Internet, have both enabled and necessitated progress in cryptology. For example, electronic commerce requires sophisticated encryption systems to protect users' credit card information. Similarly, digital communication via cellular telephones requires encryption to prevent easy interception of phone calls. Developments of the 1990s include Phil Zimmermann's PGP (Pretty Good Privacy) to protect e-mail communications.

FURTHER READING:

BOOKS:

Beutelspacher, Albrecht. *Cryptology: An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding, and Safeguarding Described Without Any Arcane Skullduggery But Not Without Cunning Waggery for the Delectation and Instruction of the General Public.* Washington, D.C.: Mathematical Association of America, 1994.

Haldane, Robert A. *The Hidden War.* New York: St. Martin's Press, 1978.

Kahn, David. *Kahn on Codes: Secrets of the New Cryptology.* New York: Macmillan, 1983.

Konheim, Alan G. *Cryptography, a Primer.* New York: Wiley, 1981.

Lubbe, J. C. A. van der. *Basic Methods of Cryptography.* New York: Cambridge University Press, 1995.

Melton, H. Keith. *The Ultimate Spy Book.* New York: DK Publishing, 1996.

SEE ALSO

ADFGX Cipher
Cryptology and Number Theory
GSM Encryption
Pretty Good Privacy (PGP)

Cryptonym

Cryptonym, or code names, are words, symbols, or numbers used in place of the actual name of a person, item, or planned event. The term is derived from two Latin roots, *crypto* meaning secret, and *nym*, meaning name. A security and counterintelligence measure, code names facilitate covert communication and enhance secrecy.

Cryptonym have long existed in many forms, each tailored to fit the circumstance in which they are used. To preserve security, military and intelligence operation code

names most often have littler or no relationship to the classified item, person, or event that they represent. Sometimes, such cryptonym are intentionally misleading. During World War II, the American military used the code name "Husky" to refer to a planned 1943 invasion of North Africa.

Intelligence and military agents working in the field often use cryptonym to disguise their identity. As means of protecting both volunteer operatives and the organizations, members of partisan groups in the French Resistance referred to each other by code names. Names of French villages, historical persons, and professional titles were commonly used cryptonym. Resistance volunteers adhered to the codename system to minimize the chance of Gestapo infiltrators, or with captured partisans under duress, easily identifying organization members.

Other types of cryptonym include number series, now commonly used in reference to military and computer technology, and symbols. Though used extensively throughout history as a means of maintaining a secret identity, the practice of substituting secret symbols for proper names has fallen out of favor. In medieval France and England, knights and nobles wishing to send secret communications often signed their messages with secretive wax seals different in color and design from their family crests or signature seals.

Although assigning intelligence matters of great importance a cryptonym is one of the oldest espionage and enciphering technologies, the practice remains commonplace today. Code names are no longer the exclusive domain of governments, military, or intelligence agencies. With the advent of the Internet, the ever-present user name, or handle, has become the most popularly used from of cryptonym.

SEE ALSO

Code Word

CT Scanners.

SEE *Scanning Technologies.*

Cuba, Intelligence and Security

Cuba has a security and intelligence apparatus that, when considered in light of the nation's size and its weak economy, is on a scale many times larger than that of the United States. Whereas its poverty, lack of exports, and depressed economic conditions would normally make Cuba an irrelevant player on the international scene, its clandestine operations extend its influence throughout the globe.

Chief among Cuban intelligence agencies is the Dirección General de Inteligencia (DGI), or General Intelligence Directorate. Established within the Ministry of the Interior in 1961, DGI initially took an aggressive role in fomenting third-world Communist revolutions. By the late 1960s, however, Cuba's Soviet sponsors had grown wary of this adventurism, and pressured Castro to purge DGI leadership. Thereafter the agency focused on intelligence collection.

Operations against the United States. Today DGI collects a wide variety of data through its operatives in Europe, the Third World, and North America—especially the last of these, because the United States is Cuba's self-declared number-one foe. The Cuban delegation to the United Nations in New York City is the third-largest in the world, and it has been estimated that nearly half of its personnel are DGI officers. In 1982, United States authorities convicted four Castro aides of smuggling drugs into the United States, and subsequently uncovered a vast drug-smuggling ring that operated in cooperation with General Manuel Noriega's Panama, as well as with Colombian drug lords.

Over a period of five years beginning in 1998, the Federal Bureau of Investigation (FBI) uncovered a Florida spy ring consisting of at least 16 Cuban operatives. They functioned on a shoestring budget, and had to account to Havana for money spent, but in the realm of spying at least, Castro's regime often manifests what analysts contend is a certain economic genius. In some cases, Havana receives intelligence free of cost. Ana B. Montes, a senior intelligence analyst at the Pentagon arrested in September 2002, received no money for activities on behalf of Cuba. Referring to the United States economic embargo against Cuba, in force since 1961, Montes claimed her actions reflected her concern over allegations of Washington's alleged unfair treatment of the Castro regime.

After the DGI reorganization, responsibility for "national liberation movements" shifted to the National Liberation Directorate (DLN), that in 1974 became the America Department (DA) of the Communist Party of Cuba Central Committee. DA, which supported the Communist movements that gained control of Nicaragua and Grenada in the 1970s and 1980s, is reported to have trained and supported guerrillas and terrorists. Many of its operatives function in supposedly innocuous positions, including the diplomatic corps and Cuban-front corporations.

In addition to DGI and DA, there is the Military Counterintelligence Department of the Ministry of Revolutionary Armed Forces, which conducts counterintelligence, signals intelligence, and electronic warfare activities against the United States.

The *New York Times* called "Cuba's intelligence apparatus the "Little Spy Engine That Could." Despite a stagnant economy crippled by Castro's policies—and sustained almost entirely by foreign aid and tourism—the Cubans have managed to maintain a security apparatus unequalled by that of any similarly small country other than perhaps Israel. And whereas, by comparison, Israel has a prosperous economy, Cuba has had to weather the loss of considerable aid following the collapse of the Soviet Union in the late 1908s and early 1990s. The post-Soviet Russian government has continued to offer support to its old ally, but on a much smaller scale than did its communist predecessor at the height of the Cold War.

The administration of President George W. Bush has accused Cuba of aligning itself with worldwide terrorist networks. Indeed, Castro has maintained friendly relations with all three members of what President Bush has publicly labeled the "axis of evil": Iran, Iraq, and North Korea.

FURTHER READING:

BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

PERIODICALS:

Golden, Tim. "White House Wary of Cuba's Little Spy Engine That Could." *New York Times.* (January 5, 2003): p. 1.3.

ELECTRONIC:

Cuban American National Foundation. <http://www.canfnet.org/> (January 22, 2003).

Cuban Intelligence Agencies. Fellowship of American Scientists. <http://www.fas.org/irp/world/cuba/index.html> (January 22, 2003).

SEE ALSO

*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*

Cuban Missile Crisis

LARRY GILMAN

The Cuban missile crisis of October 1962 was triggered by the Soviet deployment to Cuba of medium-range, nuclear-armed ballistic missiles. The United States demanded that the Soviet Union remove these missiles and imposed a naval blockade on Cuba, threatening to sink any Soviet ships that approached the island without permitting their cargoes to be inspected. Eventually, the Soviet Union (U.S.S.R.) announced that it would remove the missiles, and the crisis ended. Most historians affirm that the world has never been closer to global nuclear war than during the 13 days of the Cuban missile crisis (Oct. 14–Oct. 28, 1962).

The roots of the Cuban missile crisis go back, in part, to an earlier crisis—the failed Bay of Pigs invasion of Cuba by Cuban expatriates trained, supplied, and directed by the U.S. Central Intelligence Agency. The purpose of the failed invasion was to overthrow Fidel Castro's leftist rule of Cuba, but had two unintended effects. First, it frightened Castro, causing him to make concessions to the U.S.S.R, which wanted to place military bases on the island of Cuba, in exchange for protection against further U.S. invasion attempts. Second, it heightened tensions between the U.S. and U.S.S.R. Khrushchev, the Soviet leader, read U.S. weakness in the Bay of Pigs fiasco, and blustered publicly that he might retaliate by driving the U.S. out of West Berlin. U.S. President John Kennedy, in return, openly boasted that the U.S. possessed many more (and more accurate and deliverable) nuclear missiles and warheads than the U.S.S.R., and would consider striking first with them if it ever found itself at a military disadvantage. Kennedy's claim was true; in 1962, the U.S.S.R. had at most 20 or 30—perhaps as few as *four*—functional, deployed intercontinental ballistic missiles (ICBMs); the U.S. had several hundred. Nevertheless, Kennedy had claimed, during his presidential campaign, that the incumbent Eisenhower's administration had allowed the Soviets to get *ahead* of the U.S. in missiles, causing a "missile gap." A missile gap did exist, as Kennedy knew, but in reverse; it had always been the U.S. that was far ahead of the U.S.S.R. in such weapons. Once in office, Kennedy dropped the old story about the "missile gap" and brandished the United States's nuclear superiority openly against Khrushchev.

Khruschev's response was to secretly build missile bases on Cuban soil to compensate for Soviet inferiority in ICBMs. These missiles were medium-range and intermediate-range, rather than intercontinental, but from Cuba could reach the entire continental U.S. except its northwest corner. Similar missiles had been by stationed the United States for years in Turkey, which borders southern Russia. Castro gave permission to the Soviets to build Cuban missile bases in trade for a promise of protection against U.S. invasion and for cancellation of Cuban monetary debts.

Construction of the Cuban bases proceeded throughout the summer of 1962. The U.S. was aware, from various intelligence sources, that the Soviets were building up military forces on the island, but did not realize that intermediate-range nuclear weapons were part of the plan. Kennedy issued warnings to Khrushchev that the U.S. would not tolerate a major military buildup in Cuba, but would do "whatever must be done" to guarantee U.S. security; Kennedy and his advisors believed that Khrushchev would take these grave warnings seriously, and were

A low-level photograph taken November 1, 1962, of a medium range ballistic missile site at Sagua La Grande, Cuba, showing launch erectors removed and the launchpads bulldozed over. AP/WIDE WORLD PHOTOS.

also aware that the U.S.S.R. had never yet placed nuclear weapons outside Russian territory; these factors made it seem unlikely that nuclear weapons were part of the Cuban buildup. Nevertheless, they were.

U-2 spy planes (aircraft designed to take reconnaissance photographs from very high altitudes) were making regular flights over Cuba, observing the military buildup. On October 14, a U-2 spy plane photographed an area near San Cristóbal, Cuba, revealing launch pads, missile erectors, and transport trucks for medium-range missiles. Four of the launchers were already in firing position. Khrushchev had decided to deploy launchers for at least 16 intermediate-range missiles (capable of reaching most of the continental U.S.) and 24 medium-range missiles (capable of reaching the southeastern U.S., including Washington, D.C.).

The U-2 pictures were shown to Kennedy on the morning of October 16. Much like the Kennedy administration's claims during the Bay of Pigs crisis that the U.S. had no illegal intentions in Cuba, Khrushchev's claims to have no desire to base missiles in Cuba had proved to be untrue. Kennedy hastily assembled an ad hoc executive committee of the National Security Council, which helped him come up with two alternative plans: (1) Immediate attack on the Soviet missiles sites in Cuba, followed by a full invasion of the island using 180,000 U.S. troops. (2) A naval blockade of Cuba, to be lifted only if the Soviets removed its missiles. If the blockade did not work—and it was a risky plan, as such a blockade is, by international law, an act of war—the invasion plan would be carried out.

On October 22, 1962, Kennedy addressed the American people by television. He stated:

"This sudden, clandestine decision to station strategic weapons for the first time outside of Soviet soil is a deliberately provocative and unjustified change in the status quo which cannot be accepted by this country if our courage and our commitments are ever to be trusted again. . .To halt this offensive buildup, a strict quarantine on all offensive military equipment under shipment to Cuba is being initiated. All ships of any kind bound for

Cuba from whatever nation or port will, if found to contain cargoes of offensive weapons, be turned back."

Over the next four days, ships carrying Russian goods were searched at sea, and several Soviet vessels carrying missiles were turned back by U.S. naval vessels. The U.S. Strategic Air Command placed all its B-52 intercontinental bombers on 15-minute takeoff alert on October 20; on October 22, it placed them on a revolving airborne alert, with a percentage of bombers airborne at all times, ready to head over the North Pole toward the Soviet Union. ICBM crews were also placed on highest alert, ready to launch, and nuclear-armed Polaris submarines moved to their pre-assigned war stations at sea. The Soviet Union already had over 45,000 of its own troops on Cuba (though the U.S. estimated only 16,000), armed with 90 short-range nuclear warheads that would have been used against a U.S. invasion force. (The U.S. did not know of these short-range nuclear weapons.)

A U.S. invasion of Cuba, had it occurred, could have escalated rapidly to nuclear war, first in Cuba and then globally. The entire world, including Kennedy and Khrushchev and their advisors, feared throughout the crisis that global nuclear war was extremely probable. If nuclear war had occurred, it could have caused hundreds of millions of deaths, and significantly destroyed the U.S., the U.S.S.R., and many other nations as functioning societies.

On October 26, Khrushchev sent a private message to Kennedy indicating that he would be willing to remove the missiles if the U.S. would promise not to invade Cuba. The following day, a more formal message said that Soviet Union would remove its missiles only if the U.S. would remove its Jupiter-class intermediate-range missiles from Turkey. In secret negotiations between Soviet ambassador Anatoly Dobrynin and U.S. attorney general Robert Kennedy (brother of President Kennedy), the U.S. did promise not to invade Cuba in exchange for withdrawal of the Soviet missiles; it did not, however, promise to remove its missiles from Turkey. These missiles were considered largely symbolic by U.S. strategists, and were technically unreliable and obsolete. Additionally, their threat to the U.S.S.R. could have been replaced by deployment of a Poseidon submarine carrying nuclear missiles to the eastern Mediterranean. In secret, therefore, Kennedy seriously considered trading the missiles in Turkey for the missiles in Cuba, although in public he refused to do. On October 28—one day before the deadline urged by the U.S. Joint Chiefs of Staff for launching a Cuban invasion—the Soviets stated that they would remove their missiles from Cuba. The crisis abated.

Many historians have viewed Kennedy's handling of the Cuban missile crisis as a masterpiece of statesmanship. The Soviet Union backed down; its missiles were removed; U.S. goals were fully met; American geomilitary prestige was preserved. Other historians argue that the Kennedy administration was not as deft in reality as it seemed publicly. Kennedy and his advisors were badly frightened; Secretary of State Dean Rusk began to weep when told, at the height of the crisis, that a U-2 plane had been shot down over Cuba. Robert Kennedy said later that his brother had put events in motion that he could not control.

What is certain is that Khrushchev and Kennedy were both willing to risk global nuclear war for dubious gains. The Soviets were soon to achieve strategic nuclear parity with the U.S. simply by building more and better ICBMs; any strategic advantage to be gained by placing missiles in Cuba would, therefore, be short-term. By the same token, no long-term U.S. interests were at stake in the deployment of Soviet intermediate-range missiles to Cuba, as within a few years every city in the continental U.S. would be vulnerable to Soviet ICBMs and submarine-launched ballistic missiles anyway. Kennedy administration officials knew that the Soviet buildup in Cuba would, at worst, decrease the United States's massive strategic advantage, or *appear* to do so—in Kennedy's words, make the Soviets "look like they're coequal with the U.S." Kennedy was thus, willing to gamble the world's future not to save the U.S. from an imminent military threat, but because to tolerate the Soviet buildup in Cuba would, in his words, "have politically changed the balance of power. It would have appeared to, and appearances contribute to reality."

The U.S. emerged from the Cuban missile crisis with greatly expanded confidence in its own geopolitical skill. Its policymakers had verified, as they believed, that "showing resolve" (threatening to use military force) was more effective than diplomacy, the United Nations, or international law—with the proviso that the U.S. should be more willing to commit conventional (non-nuclear) military forces in a crisis, in order to keep back from the nuclear abyss. Today, many historians argue that U.S. willingness to invade Vietnam is directly attributable to its success during the Cuban missile crisis.

FURTHER READING:

BOOKS:

Nathan, James. *Anatomy of the Cuban Missile Crisis.* Westport, CT: Greenwood Press. 2001.

PERIODICALS:

Frankel, Max. "Learning from the Missile Crisis." *Smithsonian.* October, 2002: 53–64.

SEE ALSO

Bay of Pigs

Culper Ring.

SEE *Revolutionary War, Espionage and Intelligence.*

Cultural Resource Protection.

SEE *Archeology and Artifacts, Protection of during War.*

Customs Service, United States

JUDSON KNIGHT

One of the oldest bureaus of the federal government, the United States Customs Service was founded in the first year of George Washington's presidency, and for decades the tariffs it collected funded virtually all government activities. Today, Customs is a vast border security force that yearly interdicts hundreds of millions of dollars' worth of illegal goods. Following the terrorist attacks of September 11, 2001, Customs became a significant component in homeland security operations, and in March, 2003, it moved from the Department of the Treasury to the newly created Department of Homeland Security (DHS). Among the post-September, 2001, measures it has adopted is a port security program that requires shippers to provide advance notification of cargo arriving on American shores.

Background

Soon after Washington took office as the nation's first president, Congress passed the Tariff Act, which Washington signed on July 4, 1789. Four weeks later, on July 31—in only the fifth act of congressional history—Customs was established to protect American ports of entry. Newspapers of the day called the Tariff Act the "second Declaration of Independence," an appellation based on something more than the date on which the act was signed: for the next 125 years, the revenue provided by import tariffs funded nearly the entire federal government.

Over the course of its long existence, Customs has administered programs that eventually passed to other departments. These included the supervision of revenue cutters, ships that patrolled the coastline—a service that ultimately became the U.S. Guard. Additionally, Customs collected hospital dues to assist sick and disabled seamen, a program now handled by the Public Health Service; collected import and export statistics before the Bureau of the Census was founded to undertake this responsibility; established standard weights and measures prior to the founding of the now-defunct National Bureau of Standards (now the National Institute of Standards and Technology); and administered military pensions many decades before the founding of the Department of Veterans Affairs.

Customs activities. Customs is responsible for ensuring that all imports and exports comply with U.S. laws and regulations; collecting and protecting revenue; and guarding against smuggling. Its specific duties include assessing and collecting duties, excise taxes, and penalties on imported goods; interdicting and seizing illegal items; processing persons, baggage, cargo, and mail; administering certain navigation laws; detecting and apprehending persons engaged in activities designed to circumvent Customs regulations; protecting American industry, as well as intellectual property rights, by enforcing laws to prevent illegal trade practices; enforcing import and export restrictions on dangerous items; and collecting import and export data for the compilation of international trade statistics. In addition to enforcing its own laws, Customs enforces some 400 other laws on behalf of more than 40 government agencies.

In fiscal year 2002, Customs processed some 415 million passengers and pedestrians entering or leaving U.S. territory. Additionally, it processed a total of 130 million boats, ships, passenger vehicles, trucks, buses, and aircraft, both private and commercial. In the course of these efforts, it arrested nearly 13,000 people and seized a wide array of contraband, including $204 million in illicit proceeds, $60 million in counterfeit goods, and $1.3 million in merchandise; almost 4 million pounds (1.8 million kg) of marijuana, nearly 168,000 pounds (76,200 kg) of cocaine, over 4,000 pounds (1,814 kg) of heroin, 7.5 million tablets of ecstasy, and more than 3,000 pounds (1,361 kg) of methamphetamine; as well as nearly 40,000 firearms and 6.4 million rounds of ammunition.

Protecting Homeland Security

With a mission that already made it alert to the protection of U.S. borders and ports, Customs was a key component of homeland security even before the phrase gained widespread currency in the wake of the 2001 terrorist attacks. Following those attacks, Customs undertook new measures designed to tighten points of entry and protect the borders against suspicions persons and items.

One such measure was Operation Green Quest, in which Customs teamed with multiple federal agencies to target systems used by terrorist organizations to acquire and transfer funds. Established on October 25, 2001, Operation Green Quest issued 177 search warrants, and made 79 arrests and 70 indictments within a little more than a year. The program also netted $33 million in terrorist funds, some $21 million of it in the form of currency and monetary instruments seized as part of the Operation Green Quest bulk cash initiative.

On December 4, 2001, Customs partnered with U.S. industry in Project Shield America, established for the purpose of protecting against the acquisition and exploitation of technological products by terrorists and terror-sponsoring nations. (Among the latter, the federal government has identified seven governments: Cuba, Iran, Iraq,

A supervisor with the Bosnia-Herzegovina State Border Service Agency uses a fiberscope to examine the gastank of a pickup truck during the International Border Interdiction Training conducted by the U.S. Customs Service at the Hidalgo port of entry in Hidalgo, Texas. AP/WIDE WORLD PHOTOS.

Libya, North Korea, Syria, and Sudan.) Of specific interest are U.S. munitions list items, and strategic dual-use technology.

Challenges. Post-September 2001 security measures also include several programs requiring advance notice of shipments. Through its Container Security Initiative, Customs places personnel at major foreign ports to prescreen cargo bound for the United States. The 24-Hour Ruling, instituted in December, 2002, requires ocean carriers bringing goods to the United States to provide manifest information at least 24 hours prior to taking on cargo at the foreign port.

Additionally, in January 2003, Customs proposed new restrictions whereby it would receive four hours' advance electronic notification before imports are loaded into a truck. According to a report in *Transport Topics,* a number of truckers and shippers complained that this measure would cripple business, and one industry executive predicted that "These regulations will essentially eliminate same-day and next-day shipping." Similar restrictions imposed on deliveries by air and rail provoked protests from a wide array of shipping-related companies.

Disagreements with shippers may not be the only challenges Customs faces in its intensified mission of homeland security. By 2003, the service ran the danger of being overtaxed, with numerous activities across a broad spectrum, including counter-narcotics programs, new border security initiatives, financial investigations, and even child pornography stings. Additionally, in January, 2003, Customs deployed two Blackhawk helicopters and two Cessna Citation jets equipped with sensors to conduct 24-hour-a-day patrols over the skies of Washington, D.C., replacing military jets that had performed that role since September, 2001.

Further complicating the picture for Customs was its transition to DHS, which would require the separation of its border inspectors from its investigators under two different branches of the new department. As of March, 2003, as DHS began operations, Customs operatives faced the problem of developing a suitable technological interface with the department, and with each other.

FURTHER READING:

PERIODICALS:

Johnson, Jeff. "Truckers, Shippers Blast Customs Security Plan." *Transport Topics* no. 3521 (January 27, 2003): 1.

Mintz, John, and Spencer Hsu. "Customs Takes over Monitoring Local Skies." *Washington Post.* (January 28, 2003): A6.

Skrzycki, Cindy. "Security in Mind, Customs Says Cargo Can Wait." *Washington Post.* (February 11, 2003): E1.

Weiner, Tim. "Along Borders, Tension and Uncertainty Prevail." *New York Times.* (March 1, 2003): A11.

ELECTRONIC:

U.S. Customs Service. <http://www.customs.ustreas.gov/> (March 29, 2003).

SEE ALSO

Homeland Security, United States Department
IBIS (Interagency Border Inspection System)
Treasury Department, United States

Cyanide

JUDSON KNIGHT

The prospects for an intelligence operative captured by enemy forces are grim. Soldiers and other war fighters have recourse to Geneva Convention protocols concerning treatment, but personnel working in intelligence and covert operations are effectively denied such protection by virtue of their mission's clandestine nature. The best hope is to be released in a prisoner exchange, sometimes after years. Even then, imprisonment in many countries is likely to include lengthy and exposure to coercive methods, including beatings and/or torture whose intention is to induce the operative to divulge sensitive information. For some, the risk is too great, and therefore, intelligence operatives and agents have often gone into dangerous situations equipped with suicide devices. Most of these employ one form of disguise or another to hide a deadly compound of nitrogen, carbon, and other elements known as cyanide.

The chemistry and biological effects of cyanide. When an atom of carbon bonds with an atom of nitrogen, that is cyanide, an ionic compound designated as CN—hence the name cyanide. The bonding of these atoms with other elements produces various forms: hydrogen cyanide (HCN), cyanogen chloride (CNCl), sodium cyanide (NaCN), or potassium cyanide (KCN). The first two are colorless gases, while the second two appear in crystal form. In addition to these chemical formulas, cyanide is sometimes referred to by military organizations as AN (hydrogen cyanide) or CK (cyanogen chloride).

Applied in materials for exterminating rats and other pests, removing artificial nails, or developing photographs, cyanide has a number of practical uses. It is found in some foods, most notably cassava, and when combined with another chemical, it produces a life-sustaining substance, vitamin B^{12}. Yet even in small quantities, cyanide is harmful, a fact illustrated by poisoning deaths in parts of Africa where the diet is heavy in cassava. Cyanide is also one of the most dangerous toxins in cigarette smoke, which is the form of cyanide to which the average person is most likely to be exposed.

Cyanide prevents the body's cells from receiving oxygen, and particularly effects the heart and brain because those two vital organs are particularly dependent on the body's oxygen supply. Within minutes, the victim of cyanide poisoning in very small quantities will begin breathing rapidly and display signs of restlessness. Other symptoms include dizziness, weakness, headache, nausea and vomiting, and a rapid heart rate. Exposure to larger amounts causes rapid convulsions, severe lowering of blood pressure and heart rate, loss of consciousness, lung injury, and ultimately respiratory failure that leads to death.

Cyanide in history. Because cyanide is an effective killer, Iraqi dictator Saddam Hussein included hydrogen cyanide among the chemical weapons he used against the Kurds in the Iran-Iraq war of the 1980s. Forty years earlier, during World War II, Nazi Germany used hydrogen cyanide—in the form of Zyklon B—as an even more efficient agent of genocide in its death camps, where it killed millions of Jews and others. Ironically, in the same war, the Nazis' enemies carried cyanide pills on their persons for a very different reason, to eliminate themselves if captured.

Personnel working for the Special Operations Executive (SOE) in the war were often equipped with "L" pills (*L* for *lethal*) containing cyanide in crystal form. In some cases, cyanide could be hidden in the earpiece of a pair of glasses. When cornered, the operative could take off his glasses and pretend to thoughtfully bite the end of the earpiece while thinking about what he would say next. But there would not be any next statement: within seconds of consuming this deadly toxin, the operative would be dead.

A similar situation happened in 1977, when Soviet diplomat Aleksandr Ogorodnik found that he had reached the end of the line. He had been secretly working for the U.S. Central Intelligence Agency, who knew him by the code name TRIGON. When the Soviets discovered they had a traitor in their midst, they presented him with a confession to sign. Ogorodnik, well aware of what lay in store for him, asked to use his own pen, and when it was given to him, he bit off the end, ingesting a dose of cyanide hidden there. Within seconds, he was dead.

In order to keep this means of escape handy, operatives have gone to extraordinary lengths. Among the items used for concealing cyanide pills in the past is a container shaped like a cigarette lighter and made to fit in the rectum. In 1960, U-2 pilot Francis Gary Powers carried a

cyanide capsule on his person. Instead of committing suicide, when the Soviets shot down his plane, Powers parachuted to earth, and was taken prisoner. Later, after his captors had reaped enormous propaganda benefits from the incident, he was traded for a Soviet spy in a prisoner exchange.

FURTHER READING:

BOOKS:

Melton, H. Keith. *The Ultimate Spy Book.* New York: DK Publishing, 1996.

Minnery, John. *CIA Catalog of Clandestine Weapons, Tools, and Gadgets.* Boulder, CO: Paladin Press, 1990.

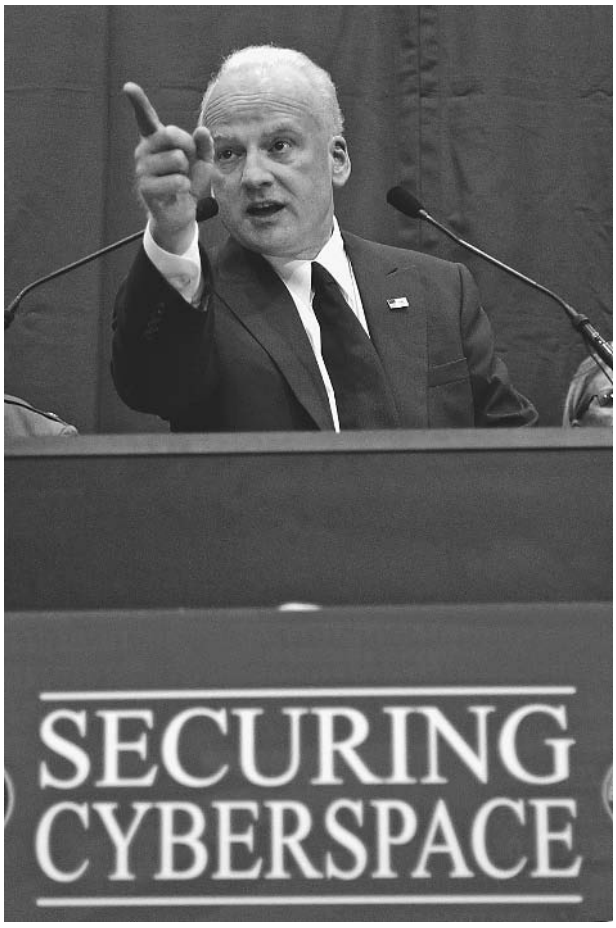
ELECTRONIC:

Facts About Suicide. Centers for Disease Control. <http://www.bt.cdc.gov/agent/cyanide/index.asp> (March 19, 2003).

International Spy Museum. <http://www.spymuseum.org> (March 19, 2003).

SEE ALSO

Assassination
Assassination Weapons, Mechanical
Biochemical Assassination Weapons
Chemical Warfare
Intelligence Agent
U-2 Incident



Richard Clarke, the White House's senior security advisor, outlines the administration's 2002 cyberspace security recommendations that include educating users and urging market forces, not government mandates, to fix cybersecurity problems. AP/WIDE WORLD PHOTOS.

Cyber Security

BRIAN HOYLE

Cyber security—measures taken to protect computers and computer networks from accidental or malicious harm—is an ongoing process. The security of a system is only as strong as its weakest link. When a fault is identified and corrected, the system tends to be stronger. This state is often transient, as other faults are eventually be detected and exploited.

The very nature of the Internet makes cyberspace vulnerable to attack. The vast majority of computers connected to the Internet are IBM compatible, as are the few operating systems that control their function. An attacker who can find a security flaw in even one computer could gain access to many computers that are not protected from intrusion.

An attack can be circuitous, involving many computers. Some computers are used surreptitiously in the attack; thus, the source of an attack becomes difficult to trace, especially if the attack has disguised the source address. While in the past, most breaches of computer security were mischief caused by computer hackers, increasingly, the information contained within computer databanks is probed and in some cases, altered.

Such disabling of computer networks can be crippling to business or infrastructure. The 1997 Presidential Commission on Critical Infrastructure concluded that cyber security was as essential to the functioning of the United States as water supplies, and declared cyber security vital to U.S. national interests. In November 2002, the U.S. government passed the Cyber Security Research and Development Act, which dedicates almost one billion dollars to the establishment of cyber security research and training centers.

Cyber Security Threats

A practice dubbed "dumpster diving" involves routing through the trash to recover paperwork or even used computer components that have been discarded. Even in

the computer age, many people print information and then discard it. A diligent search of a person's trash can sometimes obtain a great deal of sensitive information.

Intelligence personnel masquerading as janitors or other staff can gain access to computers in off-hours, and, utilizing deciphered user names and passwords, can delve into databases for information.

Cyber security also focuses on equipment. Computers that are linked via electrical wire (i.e., Ethernet networks) typically have many wall jacks ("network drops"), by which computers are connected to the network. A vacant network drop that has not been disabled can be surreptitiously used to connect with the network. Software is available that enables the connected computer to capture all data that is flowing through the network.

Wireless networks carry other security risks, as a rogue computer does not need to be physically connected to a network drop in order to acquire information. Furthermore, if the signal from a wireless network extends beyond the boundaries of a building, intelligence can be gathered even from someone parked outside.

Usernames and passwords are another vulnerable aspect of a computer network. The tendency of people to trust someone making a request for user information, and to use the same easy-to-decipher identifiers repeatedly can allow an intruder to gain access to a network.

Email is especially prone to breaches in security. The information in most emails, including the username, is in plain text. Applications are available (i.e., MailSnarf) that allow email transiting from sender to receiver to be retrieved and read by a third party. Thus, an attacker can read sensitive information contained in an email and as well, can hijack an email account to send and receive messages. Emails often have documents attached to them. This route is used to deliver malicious codes (i.e., viruses, worms, Trojan Horses) to computers.

Viruses are small programs that become embedded in files. Once a file is infected, the virus can execute its function. Depending on the intent of the virus designer, the result can be merely inconvenient to extremely destructive. Thousands of viruses exist, with new ones appearing daily. Thus, viral cyber security requires constant updating of viral protection software.

Trojan Horses are applications that are disguised as useful programs. Once activated, Trojan Horses permit a remote user to have access to the host computer, via the activated program. This aspect is especially relevant in espionage and the subterfuge can be difficult to detect.

Attackers sometimes utilize authorized network connections, in effect assuming the identity of the authorized user. Another attack strategy is called man-in-the-middle. Here, a third party—the attacker or intelligence-gatherer—impersonates both ends of a connection. The real sender and receiver are unaware that their communications are not proceeding directly to the destination. A third strategy is called the replay attack. In the replay attack, transmissions are intercepted, read, and passed along to the rightful final destination.

Cyber security Measures

The perimeter security model is the most popular type of cyber security model. The defenses are set to prevent intrusion while allowing authorized user activities to proceed unimpeded.

Typical perimeter defenses include firewalls (which filter incoming information according to set criteria for acceptance, such as IP address, domain name, protocol of sender-receiver communication, key words or phrases), intrusion detection systems, and virtual private network servers (where data is encrypted at the sending end and decrypted at the receiving end). When all the components are operating properly, a perimeter defense allows only those authorized activities to proceed from the 'outside' (i.e., the Internet) to the individual computer or computer network. However, improperly configured perimeter devices can create an illusion of security while offering little security at all.

Administrative scrutiny. Data are often backed up onto tapes. Being portable, the tapes are liable to theft. If the tape data are not encrypted, the information can be transferred or copied to another computer.

Another aspect of cyber security is the identification and approval of all hardware. The unapproved installation of a piece of hardware such as a modem or a firewall can compromise an entire network, if the installed item is not properly configured. For example, an improperly configured firewall can allow access to the Internet when only receipt and transmission of email should be permitted. A dedicated systems administrator is the best guarantee of daily scrutiny of a network's performance and vulnerability. A key component of a cyber security plan is the presence of a fallback plan in case of misadventure or deliberate sabotage.

Evaluation of the performance of some security measures is a prudent precaution. This can only be accomplished by triggering the measures by a staged attack. For example, former computer hackers are now employed by companies and government agencies to probe the vulnerabilities of a computer system. This surreptitious testing, even of the security personnel, is known as red-teaming.

Breaching of cyber security. Computer and network security tends to be expensive and can require additional operations on the part of the user. The installation of safeguards does not increase the operational efficiency of a computer

system, and can often add more layers to the operation of the computers. Until an attack, the value of the cyber security will be invisible. Thus, users and administrators can resist the implementation of cyber security measures. Without dedicated scrutiny, the cyber security measures that are in place can lapse over time, creating opportunities for breaching of the system.

FURTHER READING:

BOOKS:

Bosworth, Seymour (ed.) and Michel E. Kabay. *Computer Security Handbook.* New York: John Wiley & Sons, 2002.

National Research Council, Computer Science and Telecommunications Board. *Cyber Security Today and Tomorrow: Pay Now or Pay Later.* Washington, DC: The National Academies Press, 2002.

Northcutt, Stephen, Lenny Zeltser, Scott Winters, et al. *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs) Routers, and Intrusion Detection Systems.* Indianapolis: New Riders Publishing, 2002.

ELECTRONIC:

How Stuff Works. "How Firewalls Work." Jeff Tyson. <http://www.howstuffworks.com/firewall.htm> (15 December 2002).

SEE ALSO

Codes and Ciphers
Electromagnetic Pulse
Internet Spider

Cyber Security Warning Network

JOSEPH PATTERSON HYDER

Communication is critical during a time of national crisis. Emergency personnel need the ability to communicate quickly and effective with their colleagues in other parts of the country. In wartime, generals must remain in close contact with commanders and troops in the field. In the computer age, all communications systems—telephones, cellular phones, email, and others–are intertwined. A cyberattack that takes down the Internet by attacking root servers would also have a profound effect on all forms of communications, which rely on switches and routers to relay signals. Therefore, a cyberattack coordinated with other terrorist attacks or occurring during wartime could have catastrophic effects on national security and the economy.

In 2001, the George W. Bush administration and emergency response officials began studying what would have happened if an attack on America's communication infrastructure had coincided with the September 11, 2001 terrorist attacks. The more important question, however, was how to stop such an attack. The result was the Cyber Warning Information Network (CWIN), part of Bush's National Strategy to Secure Cyberspace.

Although the CWIN is not fully operational as of 2003, one proposed function of the CWIN is to prevent cyberattacks. The CWIN will accomplish this by creating several industry specific workgroups, or Information Sharing and Analysis Centers (ISACs). Each ISAC will monitor Internet activity and cyberattacks on Web sites and Internet infrastructure within its sector. The government agencies, companies, and network security firms involved in that ISAC will then communication with each other on cyberattacks and increase security to prevent future attacks. IF action is taken quickly enough, an ISAC will be able to stop the spread of computer viruses before they strike important systems.

The Clinton administration developed the ISAC concept. Currently, ISACs exist for each of the following sectors: information technology, banking and finance, telecommunications, chemical, and energy. The Bush administration worked with government agencies and the private sector to develop ISACs for public transportation infrastructure, water treatment, and agriculture and food.

While the idea of sharing information about particular network security vulnerabilities in order to increase security for all interested parties was considered favorable, many private sector members have been slow to volunteer network and software security problems. The Freedom of Information Act covers the CWIN, so these organizations have shown hesitancy that any information shared with fellow ISAC members might become public. Until these companies receive a privacy guarantee from the government, CWIN will not function as effectively as intended.

The second major function of the CWIN will be to allow each ISAC to operate as an individual network, even if the entire Internet is damaged in a cyberattack. This will allow ISAC members to continue to exchange critical information if all other communications systems are down. The CWIN will accomplish this by establishing an independent IP network for each ISAC.

Critics have found flaws with the CWIN on both conceptual and organizational grounds. Detractors argue that in order for the CWIN to be effective, the private sector and network security professionals will have to play a major role. So far, the government has offered few incentives for the private sector to invest the money and labor necessary to accomplish this objective. The Department of Homeland Security has also concerned some of the private

sector with a lack of commitment to the CWIN. Even after the unveiling of Bush's National Strategy to Secure Cyberspace program, which includes the CWIN, the DHS had not named a person to head the CWIN.

FURTHER READING:

ELECTRONIC:

MacMillan, Robert. "U.S. Heightens Cybersecurity Monitoring." *washingtonpost.com* <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A46583–2003Mar18¬Found=true> (18 March 2003).

SEE ALSO

Computer Fraud and Abuse Act of 1986
Computer Hackers
Computer Software Security
Computer Virus
Cyber Security
National Information Infrastructure Protection Act, United States

Czech Republic, Intelligence and Security

TIMOTHY G. BORDEN

Like all of the socialist governments of Eastern Europe, the Czechoslovakian regime used its intelligence and security services to clamp down on political dissent from the time it eliminated its opposition in 1948, until it was finally deposed in 1989. Although the scope and tactics of the Czech Statni Bezpecnost (StB) never reached the extent of its secret-police counterparts in East Germany or Romania, political repression was a feature of daily life in the country for its citizens. After the socialist regime fell in the peaceful Velvet Revolution of late 1989, the new, democratic government moved quickly to reorganize its security and intelligence operations and implemented a novel program to purge former high-level collaborators with the StB from retaining their public posts.

After assuming power in disputed elections in 1948, the Czechoslovakian Communist Party ruled the nation as a satellite of the Soviet Union. Its foreign and domestic policies closely followed that of its dominant partner and the Czechoslovak regime consistently passed intelligence information to the KGB. The brief period of reform in the Czechoslovakian Communist Party under Alexander Dubcek (1921–1992), known as the Prague Spring, came to an abrupt end with the Soviet-led Warsaw Pact invasion of August 1968. The government reverted to its former repression and maintained a network of informants working for the Statni Bezpecnost (StB), or secret police, which had its own staff of about 17,000 agents. The operatives were active in reporting and suppressing dissent among religious, academic, and political groups. The regime also maintained a higher standard of living compared to other Soviet-bloc nations, which further helped to diminish political opposition. The combination of repression and material incentives succeeded in stifling the once-restive Czechoslovakian people through the 1970s and well into the 1980s.

Domestic reform movements overturned the socialist regime with surprising swiftness and nonviolence during the Velvet Revolution of late 1989, when dissident writer Vaclav Havel emerged as the nation's president. In 1992, Havel also presided over the separation of Czechoslovakia into the independent entities of the Czech Republic and Slovakia. The government of the new Czech Republic maintained the four intelligence agencies that were established in May 1991. Two of the agencies, the Czech Security Information Service (Bezpecnostni Informacni Sluzba, or BIS) and Office for Foreign Relations and Information (Urad pro Zahranicni Styky a Informace, or USZI), gathered domestic and international information related to the protection of democracy, national interests, and human rights. The other two agencies, the Intelligence Service of the General Staff (Zpravodajska Sprava Generalniko Stab, or ZSGS) and the Military Defense Intelligence Agency, gathered information related to military interests. In contrast to the StB, the new civilian agencies did not retain executive powers of arrest and detention and were pledged to maintain the Constitutional rights of every citizen. The agencies also faced the challenge of training their new personnel in intelligence technology and surveillance and enlisted the aid of the United States, Great Britain, and the Netherlands in providing technical training in the 1990s.

Another major task of the new democratic government was implementing the lustration law passed in October 1991. Under the lustration process those who were found to have collaborated with the secret police during socialist rule were barred from a number of public posts, including the state's judicial system, central bank, and other high-level civil service, military, and academic posts. Through the expiration of the law at the end of 2000, over 300,000 lustration investigations took place under the Civic Forum, an independent commission. Less than five percent of the cases resulted in findings of collaboration with the StB and ultimately only about one hundred people were barred from their positions at the conclusion of their hearings. Other European countries adopted similar lustration laws during their transitions to democracy, including Hungary, Bulgaria, and Poland. The process went the furthest in the former German Democratic Republic (East Germany), where the Gauck Authority disseminated information from the Ministry for State Security (or Stasi) files.

During a 2002 ceremony, former Czech President Vaclav Havel, right, presents Vice Admiral Thomas R. Wilson, director of the U.S. Defense Intelligence Agency (DIA), with the Order of the White Lion for his contributions to Czech defense and intelligence in Prague. AP/WIDE WORLD PHOTOS.

FURTHER READING:

BOOKS:

Ulrich, Marybeth P. *Democratizing Communist Militaries: The Cases of the Czech and Russian Armed Forces.* Ann Arbor: University of Michigan Press, 2000.

Williams, Kieran and Dennis Deletant. *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania.* New York: Palgrave Macmillan, 2001.

ELECTRONIC:

Central Europe Review. "A Scorecard for Czech Lustration." Kieran Williams. November 1, 1999. <http://www.ce-review.org/99/19/williams19.html> (March 6, 2003).

Czech Security Information Service. "Intelligence Means." <http://www.bis.cz/eng/a_prostredky.html> (March 6, 2003).

———. "Terrorism, Extremism, and Organised Crime," <http://www.bis.cz/eng/a_ismy.html> (March 6, 2003).

Federation of American Scientists. "Czech Republic: Intelligence." John Pike. January 5, 2003. <http://www.fas.org/irp/world/czech/> (March 6, 2003).

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
Intelligence and Democracy: Issues and Conflicts
Slovakia, Intelligence and Security
Soviet Union (USSR), Intelligence and Security
STASI

This page intentionally left blank

D

D Notice

ADRIENNE WILMOTH LERNER

D Notice (defense notice) refers to an alert given by intelligence services or the armed forces to the media, alerting them of sensitive content that could damage national security or defense if reported in part or in whole. In Britain, the system is somewhat voluntary and various media corporations are not obliged to report or refrain from reporting, potentially sensitive issues.

The British D Notice system, the first of its kind, was established in 1912. Later the process was bolstered by the passage of the Official Secrets Act, which defined subjects that are not cleared for public broadcast. The act was intended to prevent information from falling into enemy hands. The notices then pertained to wire transfers, and have since evolved with the progression of technology. Today, D Notices cover media broadcast content via radio, films, television, and the Internet.

The parameters for information requiring a D Notice are straightforward. Defense plans, specific training regimens, and vital troop readiness statistics are discouraged from being broadcast. Reports on the specific operation of intelligence services, defense equipment, ciphers and data security systems are flagged for D Notices, as is the subject of civil defense, and nuclear weapons equipment and testing. The specificity and nature of a given journalistic piece, as well as the time and circumstance during which the report is broadcast, are all considered in the D Notice process. Perhaps the largest factor in the process is what type of media will be airing the piece. Television and film cameras, as well as still photographs, can often reveal more then words alone.

D Notices have again reentered the public consciousness, and are often called DA Notices (defense advisory notices). During the Persian Gulf War, several government and military officials from various nations complained that intense media coverage let Iraq prepare for every American strike. In late 2002, a new rash of D Notices were issued for information coming from military operations in the Middle East. Some journalists hold that D Notices are too often issued for subjects that are merely unflattering to government, rather than a matter of national defense., and thus are a from of soft censorship. On the whole, media companies and individual journalists are increasingly opting out of cooperating with D Notices advisories, when possible. However, there is always the possibility of professional disciplinary action, or legal punishment, such as suspension of broadcasting privileges or a steep fine, for refusal to heed some especially sensitive D Notice warnings.

FURTHER READING:

ELECTRONIC:

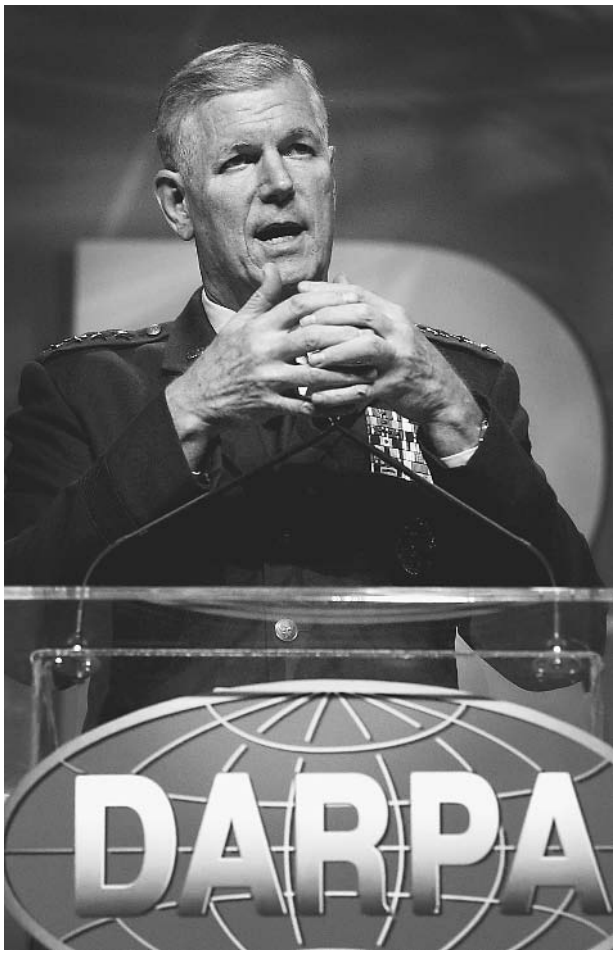
Wilkins, Gus. "The DA-Notice Web site-The Official Site of the Defence, Press and Broadcasting Advisory Committee." <http://www.dnotice.org.uk/index.htm> (December 1, 2002).

DARPA (Defense Advanced Research Projects Agency)

K. LEE LERNER

The Defense Advanced Research Projects Agency (DARPA) is the central United States Department of Defense agency dedicated to advancing research in areas of science and technology that may directly enhance military effectiveness.

DARPA's development of the TCP/IP network protocol architecture and packet switching and significantly



Air Force General Richard B. Myers, chairman of the Joint Chiefs of Staff, stresses the need for the different branches of the military, as well as the providers of weapons and technology, to work as a cohesive unit at a 2002 conference of the Defense Advanced Research Projects Agency (DARPA). AP/WIDE WORLD PHOTOS.

contributed to the development of the Internet during the 1960s-1970s (then known as ARPANet).

The launch of The Soviet satellite *Sputnik* in 1958 fueled the creation of DARPA. Eventually DARPA's programs related to utilization of space were transferred over to the National Aeronautics and Space Administration (NASA) or the National Reconnaissance Office (NRO). Currently, DARPA continues research in space programs related to rapid use of the near space environment. DARPAS space use programs include the Responsive Access, Small Cargo, Affordable Launch (RASCAL) program, Orbital Express program, and the Space Surveillance Telescope (SST) capable of detecting small satellites and other military hardware place in geosynchronous orbit.

During the Cold War, DARPA placed emphasis on developing technology related to ballistic missile defense. In 1968, DARPA programs became the foundation for the Army Ballistic Missile Defense Agency (ABMDA).

DARPA is specifically charged to maintain the technological superiority of U.S. military forces. Instead of funding projects based upon traditional criteria (i.e., expectations of anticipated results), DARPA strives for innovation in technology—including areas and projects with a low probability of success. This approach does not allow the direct development of technology but helps to prevent technological surprise by potential enemies.

As much as a governmental agency is able, DARPA has embraced an entrepreneurial oversight approach that facilitates rapid project start-up and strives to keep projects from becoming entrenched in traditional research funding mires. In some cases, DARPA can operate outside of traditional Civil Service rules and procure material support for projects outside of Federal regulations related to funding, bidding, and acquisition.

DARPA does not directly operate laboratories or facilities. DARPA is organized around a technology branch—a branch that encompasses DARPA's Defense Sciences Office, Information Processing Technology Office, and the Microsystems Technology Office—and system branch encompassing DARPA's Tactical Technology Office, Advanced Technology Office, Information Exploitation Office, Special Projects Office, and Information Awareness Office.

DARPA also encourages research by offering and awarding monetary prizes. For example, DARPA decided to offer a substantial monetary prize to the winner of a race of fully autonomous, unmanned ground vehicles from Los Angeles to Las Vegas set for April 2004. For the Army and Marines, DARPA's project AGILE led to the development of the modern M-16 rifle.

DARPA's HAVE BLUE and TACIT BLUE programs led to the development of the F-117 stealth fighter and B-2 stealth bomber used by the U.S. Air Force. Current DARPA programs seek to advance hypersonic flight capabilities. DARPA stealth programs include the SEA SHADOW program designed to apply stealth technology to naval vessels.

As of 2003, DARPA emphasized research in counterterrorism, assured use of the near space environment, networked manned and unmanned systems, self-forming robust networks, technologies to detect and destroy elusive surface targets; remote sensing and characterization of underground structures, biotechnology, and cognitive computing capabilities (i.e., computing systems that have the ability to reason and learn).

■ FURTHER READING:

ELECTRONIC:

DARPA Offices and programs. May, 2003. <www.DARPA.mil> (May 10, 2003).

SEE ALSO

Biological and Biomimetic Systems
Biological Input/Output Systems (BIOS)

Biological Warfare, Advanced Diagnostics
Bio-Magnetics
Bio-Optic Synthetic Systems (BOSS)
Bioshield Project
Bioterrorism
Brain-Machine Interfaces
Molecular Biology: Applications to Espionage, Intelligence and Security
Nanotechnology
NSF (National Science Foundation)
Pathogen Genomic Sequencing
Quantum Physics: Applications to Espionage, Intelligence, and Security Issues
Robotic vehicles
Tissue-Based Biosensors
Unmanned Aerial Vehicles (UAVs)

Data Mining

BRIAN HOYLE

Data mining refers to the statistical analysis techniques used to search through large amounts of data to discover trends or patterns.

Data mining is an especially powerful tool in the examination and analysis of huge databases. With the advent of the Internet, vast amounts of data are accumulating. As well, the amount of data that can be generated from a single scientific experiment where stretches of DNA are affixed to a glass chip can be staggering. Visual inspection of the data is no longer sufficient to make a meaningful interpretation of the information. Computer-driven solutions are required. For example, to analyze the DNA chip data, the discipline of bioinformatics—essentially a data mining exercise—emerged in the 1990s as a powerful melding of biology and computer science.

The collection of intelligence and the monitoring of the activities of a government or an organization also involves sifting through great amounts of data. Coded information can be inserted into data transmissions. If this information escapes detection, it can be used for undesirable purposes. The ability to extract the suspect information from the background of the other information is of tremendous benefit to security and intelligence agencies.

An example of data mining that is of relevance to espionage, intelligence and security is the use of computer programs—such as the Carnivore program of the United States Federal Bureau of Investigation—to screen thousands of email messages or Web pages for suspicious or incriminating data. Another example is the screening of radio transmissions and television broadcasts for codes.

The formulas used in data mining are known as algorithms. Two common data mining algorithms are regression analysis and classification analysis. Regression analysis is used with numerical data (quantitative data). This analysis constructs a mathematical formula that describes the pattern of the data. The formula can be used to predict future behavior of data, and so is known as the predictive model of data mining.

For example, from a database of terrorists who have corresponded using emails, predictions could be made as to who will send an email and to whom. This would aid efforts to intercept the transmission. This type of data mining is also referred to as text mining.

Data that is not numerical (i.e., colors, names, opinions) is called qualitative data. To analyze this information, classification analysis is best. This model of data mining is also known as the descriptive model.

The data mining process involves several steps:

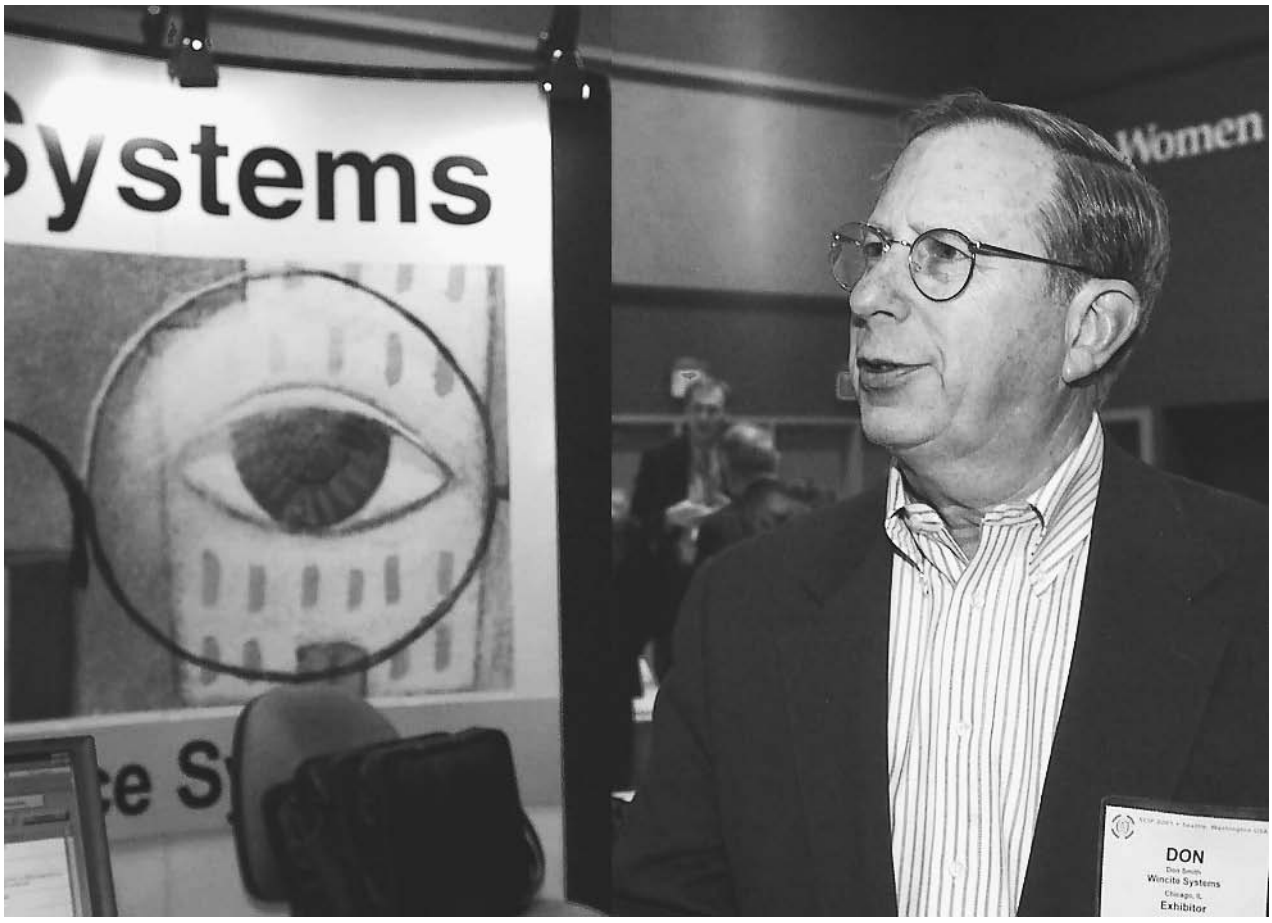
- Defining the problem.
- Building the database.
- Examining the data.
- Preparing a model to be used to probe the data.
- Testing the model.
- Using the model.
- Putting the results into action.

Database construction and model preparation—in essence the building of the framework for the mining exercise—requires about 90% of the data mining effort. If these fundamentals are done correctly, the use of the model will uncover the data that is of potential significance.

In July 2002, the Intelligence Technology Innovation Center, which is administered by the United States Central Intelligence Agency (CIA), pledged up to $8 million to the National Science Foundation, to bolster ongoing research into data mining techniques. United States intelligence officials suppose that terrorist organizations use Web pages and email to send encoded messages concerning future activities. Currently, unless a message is accidentally uncovered, only monitoring every Internet transmission from a region can reliably discover the covert information.

Also in 2002, the U.S. Federal Bureau of Investigation and the Central Intelligence Agency, under the direction of the Office for Homeland Security, have begun the joint development of a supercomputer data mining system. The system will create a database that can be used by federal, state, and local law enforcement agencies. Currently, the FBI and CIA have their own databases.

Another aspect of data mining is the linking together of data that resides in different databases, such as those maintained by the FBI and the CIA. Often, different databases cannot be searched by the same mechanism, as the language of computer-to-computer communication (protocol) differs from one database to another. This problem also hampers the development of bioinformatics (the computer-assisted examination of large amounts of biological



The Society of Competitive Intelligence Professionals convened in Seattle in 2001, where representatives of data-mining services such as Don Smith, shown here, gathered to exhibit new software and explain their data-mining techniques. AP/WIDE WORLD PHOTOS.

data). Increasingly, biological and computer scientists are advocating that databases be constructed using a similar template, or that they be amenable to analysis using the same search method.

FURTHER READING:

BOOKS:

Edelstein, Herbert A. *Introduction to Data Mining and Knowledge Discovery,* Third Editon. Potomac, MD: Two Crows Corporation, 1999.

Han, Jiawei and Micheline Kamber. *Data Mining: Concepts and Techniques.* New York: Morgan Kaufmann Publishers, 2000.

ELECTRONIC:

What You Need To Know About. "Data Mining: An Introduction." About.com. <http://databases.about.com/library/weekly/aa100700a.htm>(17 December 2002).

SEE ALSO

Cyber Security
Information Security

DCI (Director of the Central Intelligence Agency)

JUDSON KNIGHT

The director of Central Intelligence (DCI) is the head of the U.S. Central Intelligence Agency (CIA), principal intelligence advisor to the president, and leader of the U.S. Intelligence Community. The director oversees intelligence activities both on a broad scale, and through highly targeted operations such as the DCI Crime and Narcotics Center, the DCI Counterterrorist Center, and the DCI Center for Weapons Intelligence, Nonproliferation, and Arms Control. DCI also prepares the annual intelligence community budget, and chairs two advisory boards, the National Foreign Intelligence Board and the Intelligence Community Executive Committee. Notable DCIs of the past include Allen W. Dulles, the consummate 1950s cold warrior; Richard M. Helms, who led the CIA in the Vietnam and Watergate eras; Stansfield Turner, who sought to clean up the agency in the wake of scandals in the 1970s; and

CIA director George Tenet, right, huddles with CIA Assistant Director Dale Watson during testimony before the Senate Intelligence Committee in 2002, during which Tenet told the committee that Osama bin Laden's al-Qaeda terror group remained the most immediate threat facing the U.S. AP/WIDE WORLD PHOTOS.

William J. Casey, a key figure in the Iran-Contra affair. The list of DCIs also includes a man who went on to hold the nation's highest office: George H. W. Bush.

Directors of Central Intelligence: 1946–73

The title of the DCI is actually older than the CIA itself: President Harry S. Truman first used it in a January 22, 1946, presidential directive, when he designated it as the lead position in the Central Intelligence Group (CIG) within the National Intelligence Authority (NIA). It was in this capacity that the first DCI, Rear Admiral Sidney W. Souers, served during his brief tenure (January 23-June 10, 1946). Lieutenant General Hoyt S. Vandenberg (June 10, 1946-May 1, 1947) also served as DCI prior to the establishment of the CIA.

The latter was created under the National Security Act of July 26, 1947, which also created the National Security Council (NSC), and it began operation on September 18. On May 1, Rear Admiral Roscoe H. Hillenkoetter became DCI, and on December 19, the NSC gave him orders for the CIA to conduct its first covert operation intended to influence the general elections in Italy so as to prevent a Communist victory. So successful was this effort that the CIA's leadership became convinced of the efficacy of covert action.

Despite this success, Truman blamed Hillenkoetter for failing to predict the coming of the Korean War, and replaced him with General Walter Bedell Smith on October 7, 1950. Smith held the position throughout the entirety of the Korean War, and it was under his leadership that the CIA undertook one of its more notorious early covert actions by helping to bring about the overthrow of Iran's Premier Mohammed Mossadegh after the latter nationalized oil fields in his country. Smith resigned on February 9, 1953, after President Dwight D. Eisenhower—on whose staff he had served in World War II—appointed him under secretary of state.

Dulles and the 1950s. The accession of Allen W. Dulles to the position of DCI on February 26, 1953, marked the beginning of a new era. Whereas most of his predecessors had served in military intelligence units during the war, Dulles came from the organization of which the CIA was both a successor and an opposite: the Organization for Strategic Services (OSS). Having served as chief of OSS operations in Europe, Dulles brought expertise to the job. Dulles's grandfather, uncle, and brother all served as U.S. secretaries of state, but in contrast to his family's penchant for

diplomacy, he favored action. Under his direction, the CIA became highly energetic and enterprising, building both the Berlin Tunnel and the U-2 spy plane, and undertaking covert operations in Guatemala, Egypt, Indonesia, Chile, and the Congo.

Despite a number of successes, the CIA under Dulles also experienced several disasters, most notably the shootdown of U-2 pilot Francis Gary Powers over the Soviet Union in 1960, and the abortive invasion of Cuba at the Bay of Pigs in 1961. Though Richard Bissell, one of Dulles's lieutenants, was actually more involved with these two fiascoes, President John F. Kennedy blamed Dulles, and demanded his resignation.

The early 1960s. Under John A. McCone, who replaced Dulles on November 29, 1961, the CIA regained favor with Kennedy when it furnished spy plane photos showing Soviet missile emplacements in Cuba, evidence Kennedy used during the Cuban Missile Crisis.

Vice Admiral William F. Raborn, Jr. had little background in intelligence when fellow Texan Lyndon B. Johnson appointed him DCI on April 28, 1965. His lack of experience showed in his handling of the U.S. intervention in the Dominican Republic in 1965, when he passed directly to Johnson a great deal of data that had not been processed by CIA analysts. His deputy DCI (DDCI), Richard McGarrah Helms, put a stop to this indiscriminate flow of raw information, and on June 30, 1966, Helms took Raborn's place.

Helms: mid-1960s-early 1970s. Helms, who as DDCI had already put considerable CIA resources into the war in Vietnam, built up the CIA office in Saigon at the expense of stations around the world. He vigorously prosecuted the CIA's secret wars in Cambodia and Laos, and under his aegis the proprietary airline, Air America—actually established much earlier—flourished. Yet, for all his pragmatism, Helms maintained an idealism about intelligence work, and this would put him at odds with both Johnson and Richard M. Nixon.

First Johnson in the 1960s, then Nixon in the early 1970s, sought to involve Helms in domestic intelligence-gathering. The degree to which Helms willingly participated in these activities is a subject of some dispute, but it is clear that when Nixon sought to involve him more heavily in questionable activities, Helms objected. In particular, Nixon requested secret details involving Kennedy's debacles such as the Bay of Pigs. Nixon relieved Helms of his position on February 2, 1973.

Directors of Central Intelligence: 1973-Present

James R. Schlesinger had the shortest tenure of any DCI: exactly five months. During that short time, he set about revamping the agency, calling for the firing of some 1,000 employees and compiling a list of agency secrets that his successor would reveal to Congress. For two months after his July 2, 1973, departure, the DCI's position went unfilled; then, on September 4, William E. Colby took leadership. Colby's was an extremely difficult tenure, as the CIA came under intense scrutiny during this time.

In a feud with CIA counterintelligence chief James Jesus Angleton, Colby told *New York Times* reporter Seymour Hersh of a domestic intelligence campaign, Chaos, that he claimed was Angleton's brainchild. Colby did eventually relieve the CIA of Angleton, whose hunt for moles in the organization had become a preoccupation, but the revelations to Hersh set off a flurry of suspicions on Capitol Hill. During the latter part of Colby's tenure, the CIA would come under the scrutiny of multiple congressional committees, and Colby would reveal the details of the secrets compiled by Schlesinger—a list of misdeeds nicknamed "the Family Jewels".

The Late 1970s: Bush and Turner. Colby retired on January 30, 1976, and was replaced by George H. W. Bush. Despite the overall significance of Bush's career, his tenure as DCI was short—slightly less than one year. Bush did, however, put considerable support behind intelligence-gathering technology, and the Keyhole satellite program flourished under his leadership. In the midst of ongoing debates regarding proposals to transfer the Panama Canal to Panamanian oversight, Bush learned of an effort by a Panamanian lieutenant colonel to purchase U.S. intelligence secrets. Given the volatile atmosphere surrounding the Canal transfer debate, Bush opted not to act against the colonel. Twelve years later, as president, he would unseat the Panamanian, Manuel Noriega, who by then was a general and dictator of his nation.

Bush's tenure ended on the day James E. Carter became president, as Carter had his own choice for DCI: Admiral Stansfield Turner, who took office on March 9, 1977. Although Turner was an old Naval Academy classmate of Carter, the two men barely knew one another at the time of his appointment. In contrast to the early days of CIA when DCIs tended to be military officers, Turner, who retired from active duty in December 1978, had been the only military officer to serve in the position since 1966.

Turner continued Bush's emphasis on intelligence collection via satellite, and favored electronic intelligence over human intelligence. This preference had much to do with his desire to distance the agency from its old practices, and covert operations declined dramatically under his leadership. The value of those decisions came in to question, however, when the CIA was later in a poor position to gain and analyze intelligence from human sources that could help foresee or intervene in events such as the Soviet invasion of Afghanistan or the Islamic fundamentalist takeover in Iran.

The 1980s: Casey. Whereas Turner was an outsider—a military man whose methods sometimes clashed with the culture of CIA—William J. Casey, who replaced him on January 28, 1981, was an old-time spy. As the last of the former OSS men—a group that also included Helms and Colby—to serve as DCI, Casey ran the agency as a fiefdom, and kept as much secret from Congress as he could.

The CIA's budget, size, and influence grew enormously under Casey, who enjoyed strong support from President Ronald Reagan. Casey reportedly directed funds and arms to rebels fighting Communist regimes in both Afghanistan and Nicaragua, and became heavily involved in the Iran-Contra affair. How great that involvement was may never be known, in part because Casey's staff deceived Congress regarding their activities, and in part because Casey died on January 29, 1987, before he could testify.

From the mid-1980s to the present. William H. Webster has been the only man to serve both as FBI director (1978–87) and DCI (May 26, 1987-August 31, 1991). He sought to reform the abuses that had occurred under Casey, while strengthening counterintelligence. However, the degree to which counterintelligence was strengthened would be open to question after the revelation in 1994 that the CIA had long had a highly paid Soviet mole, Aldrich Ames, in its midst.

Before becoming DCI on November 6, 1991, Robert M. Gates had already served as DDCI for many years, and even served as acting DCI during Casey's illness. As DCI (a job to which Bush appointed him), he led the redirection of CIA efforts away from their Cold War orientation, and toward a focus on issues such as nonproliferation, terrorism, and drug trafficking. During an October, 1992 visit to Moscow, Gates did something inconceivable for a DCI in Dulles's time: he entered the Kremlin.

President William J. Clinton replaced Gates with R. James Woolsey, who served two years and resigned on January 10, 1995, amid criticism concerning CIA's handling of the Ames case. John M. Deutch, who took office on May 10, 1995, became the first DCI to serve on the president's cabinet. His tenure was a short one as well, ending on December 15, 1996. During that time, however, he had put considerable effort into reform of the organization. George J. Tenet, who became the fifth DCI in just six years when he assumed leadership on July 11, 1997, set the tone for his no-nonsense style of leadership in a statement of the CIA's purpose in the post-Cold War world:

"At the end of the day, this is an espionage organization. It must generate information that is unique . . . otherwise we don't know why we are here. We no longer are in search of a mission. We know what the mission is, we know what the targets are."

The DCI serves a triple function: head of CIA, principal intelligence advisor to the president, and director of the Intelligence Community. He reports to the president, both directly and through the national security advisor and/or the NSC, of which he is a member and intelligence advisor. DCI oversees the preparation of the annual CIA budget, which is in turn part of the Intelligence Community budget, a request he presents as a whole to the president.

DCI is also responsible for directing and coordinating national foreign intelligence activities, though he only exercises direct authority over the CIA, as well as some staff organizations outside the agency. The latter include the National Intelligence Council (NIC), which is responsible for preparing national intelligence estimates, and the Community Management Staff, which assists him in his executive functions as chief of the intelligence community. He also chairs two intelligence advisory boards, the National Foreign Intelligence Board and the Intelligence Community Executive Committee.

As head of the CIA, the DCI oversees a vast network of offices, and is involved in several offices within the directorate of intelligence that are concerned with issues that affect national security in the twenty-first century—namely, drug trafficking, terrorism, and weapons proliferation. These offices are the DCI Crime and Narcotics Center (CNC), the DCI Counterterrorist Center (CTC), and the DCI Center for Weapons Intelligence, Nonproliferation, and Arms Control (WINPAC).

Working on behalf of lawmakers and the law enforcement community, the CNC collects and analyzes information on international drug trafficking and organized crime. Its staff is made of a diverse array of personnel trained in areas ranging from international finance, to remote sensing, to foreign languages. Its strategic analysts prepare papers and briefings on both long-term trends and late-breaking events, while its targeting analysts conduct in-depth research of high-priority criminal and drug-trafficking organizations. Operating support specialists and program managers assist colleagues overseas with up-to-the-minute information on crime and narcotics issues, and remote sensing and geographic information specialists use cutting-edge technologies to detect narcotics crops and manufacturing facilities overseas.

The CTC is actually independent of the directorate of intelligence, although its Office of Terrorism Analysis (OTA) belongs to that directorate. Established by Casey in 1986 upon the recommendation of a task force chaired by then-Vice President Bush, CTC is designed to assist DCI in coordinating Intelligence Community antiterrorism efforts. OTA, its analytic component, monitors and assesses crosscutting issues and emerging trends in terrorism. Its responsibilities include tracking terrorists, analyzing worldwide terrorist threat warning information, assessing terrorist issues that cross national or regional boundaries, and producing intelligence to help interdict the flow of funds to terrorist organizations.

WINPAC provides intelligence support to U.S. policymakers the military with the aim of protecting the

United States and its interests from foreign weapons threats. Its staff includes mathematicians, engineers, physicists, economists, political scientists, chemists, biologists, and others. It studies the development of weapons across a broad spectrum, including weapons of mass destruction, advanced conventional weapons such as laser devices, and missiles. It monitors strategic arms control agreements, and supports military and diplomatic operations overseas.

FURTHER READING:

BOOKS:

Colby, William, and Peter Forbath. *Honorable Men: My Life in the CIA.* New York: Simon and Schuster, 1978.

Grose, Peter. *Gentleman Spy: The Life of Allen Dulles.* Boston: Houghton Mifflin, 1994.

Montague, Ludwell Lee. *General Walter Bedell Smith as Director of Central Intelligence, October 1950-February 1953.* University Park: Pennsylvania State University Press, 1992.

Persico, Joseph E. *Casey: From the OSS to the CIA.* New York: Viking, 1990.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

Powers, Thomas. *The Man who Kept the Secrets: Richard Helms and the CIA.* New York: Knopf, 1979.

Prados, John. *Lost Crusader: The Secret Wars of CIA Director William Colby.* New York: Oxford University Press, 2003.

Thomas, Evan. *The Very Best Men: Four Who Dared: The Early Years of the CIA.* New York: Simon & Schuster, 1995.

Turner, Stansfield. *Secrecy and Democracy: The CIA in Transition.* Boston: Houghton Mifflin, 1985.

ELECTRONIC:

Central Intelligence Agency. <http://www.cia.gov/> (April 24, 2003).

Central Intelligence Agency. Federation of American Scientists. <http://www.fas.org/irp/cia/index.html> (April 24, 2003).

SEE ALSO

Americas, Modern U.S. Security Policy and Interventions
Ames (Aldrich H.) Espionage Case
Bay of Pigs
CIA (United States Central Intelligence Agency)
CIA, Formation and History
CIA, Legal Restriction
Covert Operations
Cuban Missile Crisis
HUMINT (Human Intelligence)
Intelligence, United States Congressional Oversight
Intelligence Community
Moles
OSS (United States Office of Strategic Services
Satellites, Spy
U-2 Incident
Vietnam War
Watergate

DEA (Drug Enforcement Administration)

JUDSON KNIGHT

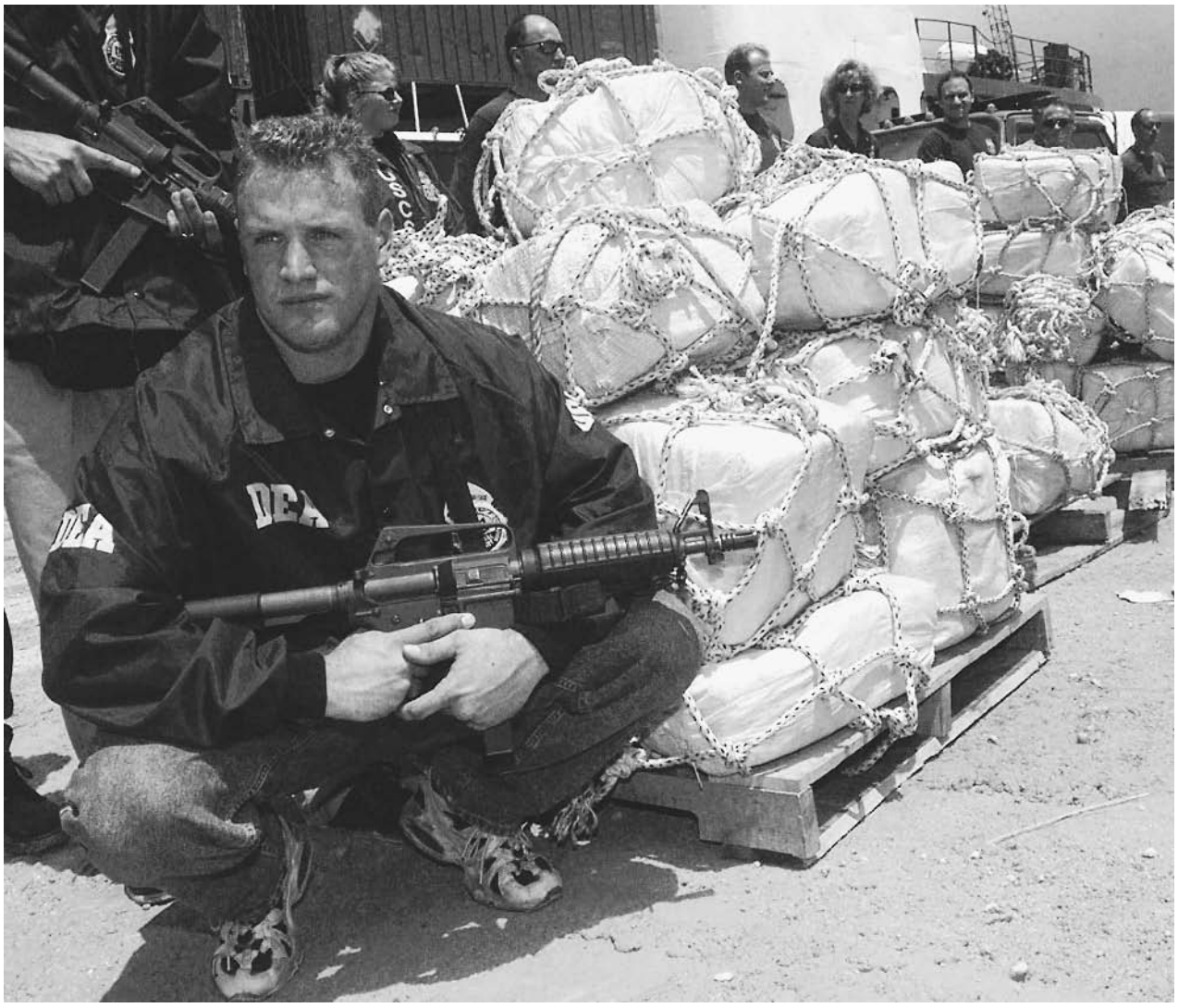
The Drug Enforcement Administration (DEA) is the lead agency of the United States government for the enforcement of federal statutes on narcotics and controlled substances. Created in 1973, it is a division of the Department of Justice with offices throughout the United States, and in 56 countries. DEA has numerous enforcement, education, and interdiction programs, an array as varied as the range of illegal drugs and the variety of groups to which they appeal. Of particular interest within the context of espionage is DEA's intelligence function, much of which is centered at the El Paso Intelligence Center (EPIC).

Historical Background

The genealogy of DEA involves entities, not only of the Justice Department, but also of Treasury and even the now-defunct Department of Health, Education, and Welfare (HEW). From 1915 to 1927, what traffic in illegal drugs there was in the United States was the purview of Treasury's Bureau of Internal Revenue, which in 1927 turned this responsibility over to the Bureau of Prohibition. In 1930, Treasury established the Bureau of Narcotics, the principal drug-fighting agency of the federal government for more than a generation.

When the government set out to fight illegal drugs during World War I, the use of marijuana and cocaine was a marginal activity, while some synthetic drugs, such as LSD, had yet to be invented. By the mid-1960s, however, the rising culture of psychedelia, closely tied with the antiwar movement and a generalized opposition to "the establishment," had catapulted drug use into the center of the youth culture. Recognizing these changes, HEW in 1966 established the Bureau of Drug Abuse Control within the Food and Drug Administration, and in 1968 this merged with the Bureau of Narcotics to become the Bureau of Narcotics and Dangerous Drugs, the first Justice Department incarnation of what was to become DEA.

DEA in the 1970s and 1980s. On July 1, 1973, the Bureau of Narcotics and Dangerous Drugs became DEA, which arrived on the scene as drug use was spreading from college



A Drug Enforcement Agency (DEA) agent stands guard next to 5,137 pounds of cocaine seized from a Panamanian vessel in Miami, Florida. AP/WIDE WORLD PHOTOS.

campuses to the mainstream of middle-class life. At no time before or since has drug use been as socially acceptable as it was in the 1970s, and DEA faced an uphill battle both culturally and operationally. The extraordinary growth in marijuana and cocaine use was coupled with a staggering rise in drug traffic from Colombia, Mexico, and other countries, and DEA greatly increased its interdiction efforts at borders, harbors, and airports.

Drug use in the United States reached an all-time high in 1979, and began to steadily decline thereafter. The change is one for which DEA rightly claims considerable credit, but a number of factors contributed. Some were at the level of policy, both public and private, including the "war of drugs" initiated by President Ronald Reagan, the "Just Say No" campaign of First Lady Nancy Reagan, and the efforts of companies who contributed airtime, advertising space, and creative talents to the Partnership for a Drug-Free America. But a societal change was also underway, closely tied with the 1980s emphasis on traditional values, health and fitness, and self-help. By the beginning of the 1990s, Alcoholics Anonymous and other addiction recovery groups were as popular as drugs and alcohol had been a decade earlier.

New drugs and new challenges. Even as drug use became less widespread, the level of commitment to drugs on the part of users deepened. This was accompanied by the rise of ever more dangerous drugs. In the mid-1980s, there was ecstacy, followed by an extraordinarily lethal cocaine derivative called crack. The underpinning of new criminal enterprises, crack spawned an attendant culture in America's inner cities, but the drug knew no ethnic barriers: users of all backgrounds joined the ranks of those addicted to this powerful narcotic.

Just as marijuana and even cocaine had once been mainstreamed among the youth culture as a whole, by the early 1990s one of the most powerful drugs of all, heroin, became a fixture among a much smaller youth segment of "Generation X." Pundits even spoke of "heroin chic," a gaunt look attended by a lackadaisical demeanor and unkempt clothing, which penetrated fashion and culture in general. This was followed a few years later by the surge in popularity of methampethamines and other synthetic stimulants, produced in illegal laboratories across the nation.

September 11, 2001, and narcoterrorism. The September 11, 2001, terrorist attacks heightened popular awareness regarding the connection between drugs and terrorism: the Taliban, Al Qaeda's fundamentalist Muslim hosts in Afghanistan, profited from the cultivation of poppies for making opium and heroin. But "narcoterrorism" was nothing new: for years, drug producers in Colombia, Peru, and elsewhere in Latin America had either been in league with, or even controlled by, radical or terrorist groups.

DEA analysts predicted that the connection between terrorism and drugs would only increase, inasmuch as former state sponsors of terrorism had either ceased to exist or had curtailed their activities. In the 1970s and early 1980s, Libya's Muammar Qaddafi had been a prominent sponsor of terrorist groups from Ireland to the Philippines, while the Soviet Union had its hand either directly or indirectly in terrorist activities throughout Western Europe and other regions. Qaddafi became much less involved in terrorism after the 1986 U.S. bombing of Libya, however, and the fall of Soviet Communism cut off millions of dollars in terrorist funding. Terrorists now turned to bank robbery, kidnapping, and drug trafficking to fund their activities.

Mission and Operations

Although it exists to enforce the drug laws of the United States, DEA operates on a worldwide basis. It presents materials to the U.S. civil and criminal justice system, or to any other competent jurisdiction, regarding those individuals and organizations involved in the cultivation, production, smuggling, distribution, or diversion of controlled substances appearing in or destined for illegal traffic in the United States.

DEA's job is to immobilize those organizations by arresting their members, confiscating their drugs, and seizing their assets. Among its responsibilities are investigation of major narcotics violators operating at the interstate or international levels; seizure of drug-related assets; management of a national narcotics intelligence system; coordination with federal, state, and local law enforcement authorities, as well with counterpart agencies abroad; and training, scientific research, and information exchange in support of prevention and control of drug traffic.

Liaison with other agencies and countries. The liaison between DEA and other agencies exists at all levels, from its relationship with law-enforcement in U.S. cities, towns, and counties to its interaction with the United Nations. DEA also works with INTERPOL and other organizations on matters relating to international narcotics control. Its agents operate throughout the world, with nations who seek to reduce the flow of drugs, and against those few rogue regimes—such as the Taliban in Afghanistan prior to the U.S. victory in late 2001—who profit from the sale of illegal drugs. Exemplary of DEA's worldwide sweep was an August 2002 *Washington Post* report that it was increasing its presence both along the Mexican border and on the other side of the planet, in Afghanistan, where it was sending 17 additional agents to help control the flow of chemicals used to process heroin.

Particularly significant is DEA's interaction with the Federal Bureau of Investigation (FBI). As part of a federal law enforcement reorganization by the Reagan administration, the FBI in January 1982 officially joined forces with DEA so as to greatly increase federal anti-drug efforts. Up to that point, DEA had reported to the associate attorney general—who at that time happened to be future New York City Mayor Rudolph Giuliani—but thereafter it would answer to the FBI director. At the same time, FBI gained concurrent jurisdiction with DEA where drug offenses were concerned. The result was the increase of the federal anti-drug force to some 10,000 FBI and DEA agents. Two decades later, DEA, a force much smaller than the FBI, was forced to reorganize some of its efforts in light of a post-September, 2001, FBI redirection of 400 agents from drug investigations to counterterrorism.

DEA intelligence. From its beginning, DEA was concerned with the collection, analysis, and dissemination of drug-related intelligence through its Operations Division, which supplied federal, state, local, and foreign officials with information. Originally, the agency had just a few intelligence analysts, but as the need grew, so did the staff, such that by the end of the twentieth century, DEA intelligence personnel—both analysts and special agents—numbered nearly 700.

Along the way, demand for drug-related intelligence became so great that the DEA leadership, recognizing how overtaxed the operations division was, in August, 1992, created the Intelligence Division. The latter consists of four entities: the Office of Intelligence Liaison and Policy, the Office of Investigative Intelligence, the Office of Intelligence Research, and EPIC. The last of these, located in El Paso, Texas, served as a clearinghouse for tactical intelligence (intelligence on which immediate enforcement action can be based) related to worldwide drug movement and smuggling. Eleven federal agencies participate at EPIC in the coordination of intelligence programs related to interdiction.

Other programs and the goals they serve. DEA also creates, manages, and supports domestic and international enforcement programs aimed at reducing the availability and demand for controlled substances. Among its dozens of programs is Demand Reduction, operated by 22 special agents at 21 domestic field divisions to educate youth and communities as a whole, to train law-enforcement personnel, and to encourage drug-free workplaces.

Demand Reduction falls under the heading of the first of three goals DEA established late in the twentieth century, and toward which it continued to work in the early twenty-first. That first goal is to educate and enable America's youth to reject illegal drugs as well as alcohol and tobacco. Among the programs in the service of the second goal—to increase the safety of America's citizens by substantially reducing drug-related crime—are the Mobile Enforcement Teams, which work to dismantle drug organizations.

The third goal, to break foreign and domestic drug sources of supply, places DEA in collaboration with foreign governments and agencies through programs such as the Northern Border Response Force. DEA also works with other federal agencies, including the Department of Justice National Drug Intelligence Center. DEA intelligence itself serves this third goal.

FURTHER READING:

BOOKS:

Levine, Michael. *Deep Cover: The Inside Story of How DEA Infighting, Incompetence, and Subterfuge Lost Us the Biggest Battle of the Drug War.* New York: Delacorte Press, 1990.

Ojeda, Auriana. *Drug Trafficking.* San Diego, CA: Greenhaven Press, 2002.

Stutman, Robert M., and Richard Esposito. *Dead on Delivery: Inside the Drug Wars, Straight from the Street.* New York: Warner Books, 1992.

PERIODICALS:

Lichtblau, Eric. "White House Report Stings Drug Agency on Abilities." *New York Times.* (February 5, 2003): A16.

Reddy, Anitha. "Terrorists Are Now Targets in Money-Laundering Fight." *Washington Post.* (July 25, 2002): E3.

Schmidt, Susan. "DEA to Bolster Presence along Mexican Border, in Central Asia." *Washington Post.* (August 10, 2002): A11.

ELECTRONIC:

Drug Enforcement Administration. <http://www.dea.gov> (March 13, 2003).

SEE ALSO

ATF (United States Bureau of Alcohol, Tobacco, and Firearms)
Drug Control Policy, United States Office of National
NDIC (Department of Justice National Drug Intelligence Center)

Dead Drop Spike

A dead drop spike is one of several types of equipment for concealing, and protecting from the elements, materials left at a dead drop. The latter term refers to the site at which an intelligence agent leaves materials—documents, film, etc.—for a handler or intelligence agent to retrieve at a later time. The handler may in turn leave money or other items for the agent to subsequently retrive. Obviously, it is important to both parties, as well as the agency sponsoring their activity, that these materials be safe from detection, theft, or harm by the elements or animals. Hence the need for the spike and similar devices.

Used since the late 1960s, a dead drop spike typically looks like a large, fat pencil. The blunt, "eraser" end has a lid that can be unscrewed, so as to insert materials and close them up in an air- and watertight chamber. The pointed end, or spike, makes the device easy to stick into the ground—safe from detection by interlopers, but easy enough for the agent or handler to retrieve.

Another device for making a dead drop is a wallet-like waterproof pouch. Sewn into the lining are ball bearings, which ensure that the pouch will sink to the bottom of a stream or ditch rather than float away. A "clam" dead drop is a tiny metal chamber attached to a magnet, such that it can be attached to an inconspicuous place on a car or any other large object with metallic parts.

FURTHER READING:

BOOKS:

Melton, H. Keith. *The Ultimate Spy Book.* New York: DK Publishing, 1996.

ELECTRONIC:

Dead Drop Spike. Central Intelligence Agency. <http://www.cia.gov/cia/information/artifacts/dead.htm> (February 1, 2003).

SEE ALSO

Drop

Dead-Letter Box

A dead-letter box is a covert location where messages or other items are deposited for retrieval by other intelligence operatives. Also called a dead drop, it is most often used as a means of transferring documents and messages, but can also be used to funnel equipment and money to agents in the field.

Dead-letter boxes can be highly clandestine or in obvious places such as public trash bins, nooks in buildings, and mailboxes that can be incorporated into normal activity. The only requirements are the ability to place items into the receptacle unseen, communication between the two parties regarding drop-off and pick-up, and the ability to elude surveillance.

Although they are one of the oldest tricks in espionage, dead drops remain a useful tool. A successful dead drop requires not only the transfer of items, but also careful attention to counter-surveillance measures. A dead drop is advantageous because it is accomplished without the two parties making contact, thereby rendering surveillance of suspected persons more difficult.

In February of 2001, Robert Philip Hanssen was arrested on charges of espionage after making a dead drop of classified documents in a public park in Vienna, Virginia. Days before his arrest, Federal Bureau of Investigations agents located Russian agents placing a parcel underneath an outdoor amphitheatre in Arlington, Virginia. They retrieved and photographed the package, which contained $50,000, the payment for the documents Hanssen was supposed to leave at the dead drop the day of his arrest. Over the course of 22 years, Hanssen, a veteran FBI counterintelligence officer, used various dead-letter boxes that he created in the New York and Washington, D.C. areas to smuggle information to Soviet (and later, Russian) agents. He was convicted of espionage and conspiracy to commit espionage and sentenced to life in prison. His final dead-letter box, code named Ellis, was underneath the supports of a park foot bridge.

SEE ALSO

Tradecraft

Decontamination Methods

BRIAN HOYLE

Decontamination refers to the efforts to safeguard property and people that have been exposed to chemical, nuclear, or biological agents. The intent of decontamination is twofold. The first objective is to make the individual free from the contaminant, or, if complete removal of the agent is impossible, to reduce the concentration of the contaminant to a level that is safe for survival. The second objective is to make property safe for habitation.

Human decontamination can involve removal of a contaminant from the skin. Usually such decontamination must be done quickly, since the contaminant may be absorbed through the skin where it can cause internal damage. In a setting such as the home, laboratory, or factory, permanent decontamination facilities can be present. For example, washrooms equipped with arm-activated water taps and antiseptic soap allow for the rapid removal of personal spills. Decontamination is also possible "in the field", courtesy of emergency response personal decontamination kits, which can be carried with workers or soldiers.

In April, 2003, military forces of the United States, Britain, and Australia faced the prospects of chemical and biological weapons attacks by forces in Iraq, as well as decontamination resulting from the deliberate destruction of oil installations and the discovery and destruction of stored biological and/or chemical weapons. For these forces, rapid response decontamination strategies are a prudent and vital precaution during the conflict.

Chemical Decontamination

There are a variety of decontamination methods and strategies that can be brought to bear on a chemical problem. Often, the method selected depends on the nature of the contaminant. For example, vacuuming up a spill of a powdery chemical can be a prudent step, while the same technique would be inappropriate for a liquid spill.

There are three general chemical decontamination methods. These methods involve physical, chemical, or thermal processes.

Physical methods. Liquid chemicals can be removed from inert surfaces or living surfaces (i.e., skin) by the use of sorbents. The sorbent can be a natural material, such as soil, diatomaceous earth, or activated charcoal, or can be synthetic (i.e., Amberlite XAD-2 and XAD-7 resins). In general, the natural materials absorb, or suck up, the liquid contaminants, while the synthetic materials adsorb contaminants. Adsorption involves the concentration of a substance from the liquid phase onto the surface of the adsorbent material due to the chemistry of the surface molecules.

The most recognizable solid absorbent is a clay material known as Fuller's Earth. This material is commonly found in kitty litter. When solid absorbent materials like Fuller's Earth, soil, or diatomaceous earth are used, the contaminant is usually not altered. For example, petroleum products are readily absorbed but are not changed in their character. Thus, the sorbent material becomes toxic and so must be collected and disposed of afterwards. Caution needs to be taken during the collection process, as fine dust or particles can be inhaled or stuck to exposed skin.

A different type of physical decontamination involves washing the contaminant away using another fluid like water, an alcohol, or freon. The aim here is to dilute the

A volunteer is scrubbed by hospital workers wearing biohazard suits during an Omaha, Nebraska, hospital bioterrorism decontamination drill in March 2002. AP/WIDE WORLD PHOTOS.

contaminant in the wash fluid, which should itself be collected for proper disposal. Washing is not a complete decontamination. Residual contaminant can remain behind in cracks or other hiding places. However, the use of high-pressure sprays can be an effective and rapid means of decontaminating surfaces like walls and floors.

Chemical methods. Chemical decontamination goes further than merely removing a contaminant from the environment. Rather, in chemical decontamination the adsorbing chemical neutralizes a contaminant. One example of chemical neutralization is the adsorption of a contaminant by material that is impregnated with an alkaline chemical. Another general example is the use of chemically reactive compounds that interact with the contaminant and change its structure into a form that is non-toxic.

A popular chemical decontamination strategy relies on the use of oxidizing agents. Bleach is a well-known example of an oxidizing agent. The use of oxidizing compounds such as calcium hypochlorite or sodium hypochlorite inactivates a variety of chemical compounds as well as dangerous microorganisms such as bacteria and viruses.

Oxidizing agents can be wiped onto a spill and collected in an absorbent material. As well, some oxidizing agents can be incorporated into topical lotions, which are smeared onto the skin to help inactivate a chemical or biological spill.

A recent innovative example of an oxidizing agent is L-Gel. Developed at Lawrence Livermore National Laboratory, L-Gel uses potassium peroxymonosulfate to deactivate a variety of biological agents, including anthrax spores and *Yersinia pestis* (the bacterium that causes plague). The thick gel is able to cling to surfaces better than water, especially to steeply sloping surfaces like walls, which keeps the decontaminant in contact with the target longer than using a straight water-based decontaminant. It is hoped that a powdered formulation of the product will soon be available for use in ventilation ducts, where clean up of chemical and biological agents is especially difficult.

During the fall of 2001, L-Gel was successfully used to decontaminate offices of Congress and at ABC News following the receipt of letters that were laced with anthrax spores.

Strong bases, such as hydroxide forms of calcium, sodium hydroxide, and potassium are other useful chemical decontaminants. These agents disrupt chemical bonds in the contaminant and so destroy the offending compounds' noxiousness.

Water is an ideal fluid for decontamination because a variety of chemically different detergents and soaps readily dissolve in water. These compounds can loosen or bind contaminants and so remove them from a surface. The friction of scrubbing also aids in decontamination of the skin during hand washing.

The different tendencies of chemicals to dissolve in water (a property known as solubility) affects the efficiency of a decontaminant. For example, a longer period of decontamination is needed when using a compound that is not readily soluble in water. This problem can be somewhat overcome by the use of microemulsions, which are essentially very small droplets of the decontaminant. The droplet coat is a material that is less water-soluble. The effect is best seen when oil is added to water. Then, a sheen of oil appears on the water, rather than a homogeneous oil-water mixture. If a contaminant is not water soluble, it will quickly partition into the hydrophobic ("water-hating") decontaminant portion of a microemulsion. This can speed up the action of a decontaminant. Microemulsions can be applied to a contaminated surface as a spray, which can be washed off later.

Thermal methods. Thermal decontamination is the use of heat to vaporize those chemical contaminants that will readily convert from a liquid to a gas in the presence of heat. Both water- and alcohol-based chemicals can exhibit this behavior.

Water can also be heated, even to the extent of being converted to steam. Hot water or steam treatment can be an efficient means of decontamination of greasy or oily contaminants. The use of moist heat, as in the laboratory sterilization unit called an autoclave, disrupts chemical bonds in many microorganisms, killing them. Unfortunately, certain noxious bacteria that form spores (i.e., *Bacillus anthracis*, *Clostridium* species) can, under some circumstances, survive autoclaving.

Hot air is another useful decontaminant for compounds that can be volatilized. This method is useful for situations where a spill can be isolated and treated over a longer period of time. In a battlefield situation, other more urgent methods are preferable.

Nuclear Decontamination

Nuclear decontamination in a battlefield site, to date only applicable in the Japanese cities of Hiroshima and Nagasaki in the waning days of World War II, necessitates the removal, burial, or storage of the contamination. However, in sites such as decommissioned nuclear power plants or weapons manufacturing facilities, the less concentrated amounts of radioisotopes that are encountered can be more systematically decontaminated.

Nuclear decontamination consists of the removal of the contaminating radioisotope. Removal can be accomplished by the use of water-soluble chemicals (i.e., alkaline permanganate, citric oxalic acid), fire-fighting foam, and even the electrochemical treatment of the contaminated surface.

Personal Decontamination

The specter of contamination with agents, in particular biological agents, was seared into the public consciousness in the latter months of 2001. Then, U.S. citizens were subjected to terrorist attacks as letters containing *Bacillus anthracis*, the bacterium that is the cause of anthrax were mailed through the U.S. Postal Service.

The concern over the use of biological weapons has not abated since that time. Indeed, the possibility of biological attack, and so the need for rapid decontamination, was one of the paramount concerns of U.S. troops and their allies involved in the war in Iraq in the winter and spring of 2003.

Suspected exposure to an aerosol of a dangerous microorganism should be dealt with promptly. The exposed clothing should be taken off and safely contained so as not to contaminate bystanders or medical personnel. It may be necessary to destroy clothing depending on the suspected contaminant. For example, spores of the anthrax bacteria can cling to clothing and retain their potential for infection for decades. Exposed skin should be decontaminated. The best strategy is to use soap and water with diligent scrubbing for at least 30 seconds. The use of diluted household bleach is acceptable.

Decontamination in the case of biological exposure is typically done in an isolated facility, where the access of personnel is tightly controlled, and the outgoing air can be filtered to prevent the spread of the biological agent. Such facilities are even used in the battlefield setting.

In battlefield settings such as Iraq, the military can use a dried resin known as M291. This resin is a dry black carbon containing material that decontaminates by absorption and physical removal of the chemical agents from the victim. M291 resin is particularly useful for localized ("spot") decontamination of exposed skin.

Organization of a military treatment area. Part of military strategy in conflicts where there is a potential for the use of biological or chemical weapons, as in the Iraq conflict of 2003, is the establishment of medical treatment facilities. In the battlefield a facility is divided into two zones. One zone (the "dirty" zone) is where contaminated personnel and equipment are segregated. The other, "clean" zone is

kept free from the contaminating agents. The transition area between these zones, which is called the hotline, keeps contaminated people (including casualties) and equipment out of the clean side until decontamination is completed.

Triage, emergency treatment, and decontamination are done in the dirty zone. The emergency treatment station essentially treats patients as best as possible and stabilizes them for movement to the clean zone operation theatre, or evacuation to a hospital. Any decontamination is done in the dirty zone, with more substantive medical procedures being done in the clean zone.

Civilian Decontamination

The National Pharmaceutical Stockpile Program in the U.S. has assembled large quantities of antibiotics, vaccines, and other medical treatment countermeasures that can be rapidly deployed. For example, in the aftermath of the anthrax attacks in the U.S. during 2001, federal and state agencies were able to quickly provide the antibiotic ciprofloxacin (Cipro) to those potentially exposed to *Bacillus anthracis*.

In the event of a large scale contamination, such as the "dusting" of anthrax spores over a metropolitan area, large numbers of causalities would likely result, as decontamination strategies for such masses of people are still in the planning stages.

Decontamination during the Iraq War of 2003

The past deployment of chemical and biological weapons by the government of Iraq under Saddam Hussein, and the inconclusive findings of the United Nations weapons inspectors who were present in Iraq in 2002–2003, heightened concerns for the possible use of such weapons during the 2003 war between Iraq and coalition forces of the United States and the United Kingdom.

In the 1980–88 war with Iran, Iraq deployed chemical weapons that affected an estimated 100,000 Iranians, killing about 10,000 people. Even today, some 1,000 people are considered to be moderately to severely ill because of these attacks.

Another decontamination effort will be necessary to deal with the oil wells that have been set ablaze by Iraqi soldiers in the 2003 conflict. The residue given off by the blazing wells in sufficient numbers could be an environmental disaster, and is unhealthy to breathe. Unfortunately, decontamination is virtually impossible, other than to extinguish the blazes and to clean up the terrain immediately surrounding the wells once they have been extinguished.

Contamination of the drinking water supplies of southern Iraqi towns such as Safwan and Zubayr makes the possibility of disease more immediate. Post-war decontamination efforts involved the isolation and treatment of the contaminated surface and ground waters.

FURTHER READING:

BOOKS:

Boss, Martha J., Dennis W. Day, and Roger F. Jones. *Biological Risk Engineering Handbook: Infection Control and Decontamination.* Boca Raton: Lewis Publishers, Inc., 2002.

Mauroni, Albert J. *America's Struggle with Chemical-Biological Warfare.* Westport, CN: Praeger Publishers, 2000.

ELECTRONIC:

United States Environmental Protection Agency. "Anthrax." EPAHome. January14, 2003. <http://www.epa.gov/epahome/hi-anthrax.htm>(04 March 2003).

SEE ALSO

Anthrax Weaponization
L-Gel decontamination reagent
Pathogens

Decryption

Decryption is simply the reverse of encryption, the process by which ordinary data, or plain text, is converted into a cipher. A cipher, often incorrectly identified as a code, is a system in which every letter of a plain text message is replaced with another letter so as to obscure its meaning. To decipher a message requires a key, an algorithm that provides the method by which the message was encrypted.

Ciphers, algorithms, and keys. In one of the earliest and simplest ciphers, Julius Caesar sent messages in which each letter was substituted by the letter three places after it in the alphabet. In place of *A,* then, one would use a *D.* The key for such a cipher would be simply, "Shift right by three," or something similar.

A key is an algorithm, or a method for solving a mathematical problem by using a finite number of computations, usually involving repetition of certain operations or steps. An excellent example of an algorithm is $f(x) = y$, a formula by which a relationship between two elements is shown on a Cartesian coordinate system. It is said that "y is a function of x," meaning that for every value of x, there is a corresponding value of y. Suppose it is established that $2x = y$; then the key for the function has been established, and all possible values of x and y can be mapped.

Brute force and weak and strong encryption. In a simplified form, this is what occurs in decryption. The example

shown is one that could easily be solved by what are called "brute-force" means. Brute force is a method of decryption in which a cryptanalyst, lacking a key, solves a cipher by testing all possible keys. This tends to be impractical for most ciphers without the use of a computer, and for the most sophisticated modern ciphers, brute force is all but impossible.

Suppose, however, one were shown a graph with the following coordinates for *x* and *y:* 1, 2; 2, 4; 3, 6, and so on. It would be fairly easy to determine from these values, using brute force, that $2x = y$, even if one did not have the key. This is an example of "weak" encryption. By contrast, some of the systems in use today for encryption of bank transactions or cellular phone communications and other purposes are extremely "strong". The ultimate example of strong encryption would be a situation in which decryption would be impossible without knowing the key.

Strong encryption is a controversial matter, due to the concerns of law-enforcement and intelligence authorities that such ciphers could be used by terrorists or other illegal groups. This has led to a move on the part of several governments, including that of the United States, to set up "key-escrow" arrangements, whereby all developers of ciphers would be required to give authorities a "back door" or key into the cipher. The government would maintain decryption keys in a secure location, and use them only when given a court order.

FURTHER READING:

BOOKS:

Kahn, David. *The Codebreakers: The Story of Secret Writing.* New York: Macmillan, 1967.

Kippenhahn, Rudolf. *Code Breaking: A History and Exploration.* Woodstock, NY: Overlook Press, 1999.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age.* New York: Viking, 2001.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World.* New York: John Wiley, 2000.

SEE ALSO

Encryption of Data
GSM Encryption
Pretty Good Privacy (PGP)

Defense Information Systems Agency, United States

The Defense Information Systems Agency (DISA) has the responsibility of planning, developing, and supporting the C4 (command, control, communications, and computers) and information systems that serve the president of the United States and other national leaders. DISA is also responsible for Department of Defense (DOD) telecommunications and information processing facilities and systems. Included among the latter are the Global Command and Control System, or GCCS.

DISA was established in 1960 as the Defense Communications Agency. Overseen directly by the assistant secretary of defense for Command, Control, Communications (C3) and Intelligence, the agency serves the needs of the president, the vice president, the secretary of defense, the joint chiefs of staff, combatant commanders, and other DOD components under all conditions of both peace and war. As the agency responsible for maintaining defense information infrastructure, DISA ensures that this infrastructure will be interoperable with theater and tactical command and control systems, with the C4 systems of allied nations, and with any other national or international systems relevant to the DISA mission. Furthermore, DISA supports the National Communications System (NCS) in its national security emergency preparedness telecommunications functions.

Among the information and communication systems DISA manages are the Defense Message System, the Defense Information Systems Network, the Global Combat Support Systems, the Common Operating Environment, and the Global Command and Control System (GCCS). GCCS is the nation's leading system for command and control of joint and coalition forces, and incorporates applications required by battlefield commanders to prepare and undertake military operations. Fielded at more than 625 sites globally, GCCS is networked through the highly secured private intranet of the DOD.

FURTHER READING:

BOOKS:

Communications Management and Control Activity (CMCA). Washington, D.C.: Defense Information Systems Agency, 1995.

The Defense Information Systems Agency (DISA): NAA, "The Three Sisters". Washington, D.C.: Defense Information Systems Agency, 1995.

Operation: DISA, A Continuing Evolution. Arlington, VA: Defense Information Systems Agency, 1996.

ELECTRONIC:

Defense Department Space Policy. Federation of American Scientists. <http://www.fas.org/spp/military/docops/defense/d5105_19.htm> (February 22, 2003).

Defense Information Systems Agency. <http://www.disa.mil/> (February 22, 2003).

SEE ALSO

Communications System, United States National
DOD (United States Department of Defense)

Defense Nuclear Facilities Safety Board, United States

The Defense Nuclear Facilities Safety Board (DNFSB) is an independent agency of the federal government charged with overseeing the disposition of defense nuclear materials controlled by the Department of Energy (DOE). Created by Congress in 1988, DNFSB as of 2003 consisted of three members responsible for advising, and providing recommendations to, the secretary of energy.

Today there are a dozen DOE defense nuclear sites around the nation, including facilities at Oak Ridge, Tennessee, and Los Alamos, New Mexico. From the time of the development of nuclear weapons by the United States in World War II until the 1980s, the operation of these facilities had taken place without benefit of external oversight, a situation that continued even as DOE replaced the old Atomic Energy Commission in the 1970s. By the late 1980s, public health and safety concerns raised by the accumulation of hazardous materials at the increasingly aged facilities of the defense nuclear complex prompted action on the part of Congress. The latter in 1988 passed the National Defense Authorization Act, which established DNFSB.

Activities and powers of DNFSB. An independent agency within the executive branch of government, DNFSB provides oversight with regard to all activities within DOE's nuclear weapons complex that affect, or potentially affect, public safety. Up until the end of the cold war, the nuclear weapons complex was concerned with designing and testing weapons, and with maintaining the nation's nuclear arsenal. With the end of the cold war, and hence of the arms race it spawned, the mission of the nuclear weapons complex changed. Thenceforth, its resources were committed to cleaning up contaminated sites, dismantling nuclear weapons, storing and disposing of excess materials, and maintaining the now-reduced nuclear stockpile.

To ensure that these activities are undertaken with the strictest concern for public health and safety, DNFSB continually reviews and evaluates activities at defense nuclear facilities. The board then makes recommendations to the secretary of energy regarding specific measures it deems necessary to protect the public. DNFSB also reviews, and if necessary recommends changes to, designs for new facilities, as well as modifications to old ones. The board also has the power to undertake investigations, issue subpoenas, hold public hearings, gather data, conduct studies, and establish requirements for DOE reporting. DNFSB is in turn required to report to Congress at least once a year.

FURTHER READING:

BOOKS:

Nuclear Safety: The Defense Nuclear Facilities Safety Board's First Year of Operation: Report to Congressional Requesters. Washington, D.C.: General Accounting Office, 1991.

Plans, Progress, and Experience to Date of the Defense Nuclear Facilities Safety Board: Hearings Before the Subcommittee on Strategic Forces and Nuclear Deterrence of the Committee on Armed Services, United States Senate, One Hundred First Congress, Second Session, March 28, 1990. Washington, D.C.: U.S. Government Printing Office, 1990.

ELECTRONIC:

Defense Nuclear Facilities Safety Board. <http://www.dnfsb.gov> (February 22, 2003).

SEE ALSO

DOE (United States Department of Energy)
Nuclear Power Plants, Security
Nuclear Reactors
Nuclear Regulatory Commission (NRC), United States

Defense Security Service, United States

The Defense Security Service (DSS) serves the Department of Defense (DOD) in a number of capacities, conducting personnel security investigations, providing industrial security products and services, and offering security training to DOD personnel, contractors, and employees of other government agencies. Its most significant undertakings are the Personnel Security Investigations (PSI) Program; the Industrial Security Program (ISP); and the Security Education, Training, and Awareness Program.

Established as the Defense Investigative Service on January 1, 1972, the service changed to its present name in November 1997 in order to more accurately reflect the breadth of its mission. Oversight comes from the assistant secretary of Defense for Command, Control, Communications, and Intelligence. As of 2003, DSS employed some 2,600 persons throughout the United States, with a much smaller contingent in Europe. About half of its personnel roster was comprised of special agents responsible for undertaking approximately half a million PSIs per year. Another 230 employees were involved in the ISP program, working with more than 11,000 contractors involved in research, development, and other classified projects outsourced to specially screened entities in the private sector.

Background investigations. The PSI program of the DSS oversees background investigations on military, civilian, and contractor personnel affiliated with DOD. PSIs are used to determine the suitability of an individual for entrance into the armed services, for access to classified information, and for appointment to sensitive positions within DOD. PSIs conducted by DSS special agents are submitted to the agency's Personnel Investigations Center at Fort Meade, Maryland, where they are processed. When completed, PSIs are sent to the appropriate DOD adjudicative facility, which makes the determination as to the individual's suitability. DSS is thus purely a reporting and screening agency, and has no power to choose or reject individuals for positions within DOD.

The work of processing security clearances, the most prominent service of DSS, has also provided the occasion for a number of frustrations. In July 2000, the agency experienced the breakdown of a $100 million computer system, thus temporarily bringing to a halt its background checks. Also in that month, a review panel that included representatives of DSS came under fire for approving an award to Loral Space & Communications Corporation "for outstanding security performance and practices." In 1996, Loral had forwarded a report on a Chinese rocket to the Chinese government without first obtaining State Department clearance, a situation that had led to a grand jury investigation. The backlog of security clearance investigations forced DSS to turn to civilian contractors for help. In June 2002, DOD investigators learned that one of the firms DSS had used, Government Business Services Group, may have submitted false reports to DSS and claimed to have completed work it had not done. As of fiscal year 2004, DOD had transferred responsibility for conducting most background checks from DSS to the Office of Personnel Management (OPM).

Other DSS programs. Under the ISP heading in DSS are three industrial security programs, the largest of which is the National Industrial Security Program, or NISP. DSS representatives working in the NISP oversee security at cleared contractor facilities, and assist the contractor's staff in formulating and maintaining security programs. The other two ISP sections are the Arms, Ammunition, and Explosives (AA&E) Program, which provides protection for munitions, and the Critical Infrastructure Program (CIP), which oversees systems vital to the operation of DOD. Additionally, the Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio, processes, issues, and maintains ISP facility and personnel clearances.

The Security, Education, Training, and Awareness Program includes instruction in counterintelligence and other areas. Training takes place at the DSS Academy, or DSSA, in Linthicum, Maryland, where some 10,000 students from DOD and the defense industry learn core security disciplines that integrate training in CI and information systems. Education is provided through combinations of formal classroom teaching, computer-based learning, and correspondence, distance, or tele-training.

In the realm of counterintelligence, the DSS Counterintelligence Office, established in May 1993, seeks to integrate an awareness of counterintelligence with DSS core mission areas. Its aims are to infuse the defense workforce with counterintelligence knowledge, to increase awareness of counterintelligence throughout DOD and the contractor base, and to assist those it trains in recognizing and reporting intelligence collection activities conducted by foreign powers or groups.

FURTHER READING:

PERIODICALS:

Barr, Stephen. "Defense Department Agrees to Have OPM Take Over Background Checks." *Washington Post.* (February 5, 2003): B2.

Pincus, Walter. "Computer Shutdown Hits Defense Security Service; Backlog of Background Checks Grows." *Washington Post.* (July 8, 2000): A10.

———. "A Pentagon 'Embarrassment': Loral Wins, Is Stripped of Award for Security Practices." *Washington Post.* (July 19, 2000): A21.

Pound, Edward T. "Keeping Secrets Secret." *U.S. News & World Report.* (June 3, 2002): 22.

ELECTRONIC:

Defense Security Service. <http://www.dss.mil/> (February 22, 2003).

SEE ALSO

Classified Information
Counter-Intelligence
DOD (United States Department of Defense)
Security Clearance Investigations

Delta Force

Delta Force is one of the two principal United States counter-terrorism units, the other being the Naval Special Warfare Development Group, formerly known as Seal Team Six. Created in 1977 by Colonel Charles "Charlie" Beckwith, Delta Force is headquartered at Fort Bragg, North Carolina. Little is known about the elite unit, which is highly trained and well equipped with state-of-the-art weaponry, airborne insertion equipment, and other forms of technology. Delta Force has participated in a multitude of counter-terrorist actions from 1979 onward.

Formation. In forming Delta Force, which was activated in November 1977, Beckwith drew on his experience with the British 22nd Regiment Special Air Service (SAS), with which he worked in an exchange program in 1962 and 1963. Despite the heavy influence of SAS, with which it

often trains—along with France's GIGN, Germany's GSG-9, Israel's Sayeret Matkal/Unit 269, and Australia's Special Air Service Regiment—Delta Force has its own, very distinct and unique, character.

The official name of Delta Force is 1st Special Forces Operational Detachment-Delta, meaning that it is organizationally part of the Special Forces, themselves an elite fighting unit under U.S. Special Operations Command. Yet, Delta Force is housed apart from the Special Forces at Bragg, and in appearance they are unlike any regular army in the world. Many wear their hair well beyond regulation length, and they often work in civilian clothes. Unlike Special Forces or the Rangers, from which many of their personnel are drawn, Delta Force has no distinct outward uniform or insignia.

In addition to special-warfare units, Delta Force members may come from other parts of the army or even other branches of the military. The group conducts limited recruiting, and undertakes specialized efforts to acquire personnel possessing unique and valuable skills. A soldier who speaks an obscure language, or who possesses special technical abilities may be approached and directly recruited by a representative from Delta Force.

Facilities and equipment. Little is known about the inside of the Delta Force compound, though it reportedly has extensive training facilities that include numerous shooting areas (both for battle at close proximity, and for sniping at longer range), an Olympic-sized swimming pool, a dive tank, and a three-story wall for climbing. The compound also reportedly includes a facility for hostage-rescue training, known as the "House of Horror" and modelled on the "Killing House" of SAS.

Delta Force uses an array of equipment, some of it specialized for the group's unique mission. For example, personnel conduct extensive airborne training, including specialized HAHO (high altitude-high opening) and HALO (high altitude-low opening) jumps. HALO work requires a soldier to fall through the air a considerable distance without the opened chute to break his fall, and thus he must keep his hands above his head. However, this can cause much of the blood to flow out of the arms, leaving the soldier to operate at less than full capacity during the first few minutes after he touches ground. To solve this problem, Delta Force arranged to have specially built parachute rigs that allow them to keep their hands at their sides during descent.

Delta Force operations. Delta Force works closely with other services and federal agencies, particularly the Central Intelligence Agency. Its first deployment was an inauspicious one, the attempted rescue of hostages held in the U.S. embassy in Teheran on April 25, 1980. In any case, the failure of this mission, which ended with a fatal helicopter crash before the special unit (composed of elite fighters from several military services) even reached Teheran, had little to do with Delta Force.

Delta Force also participated in the U.S. invasion of Grenada in 1983, and in 1984 and 1985 conducted assaults on jetliners hijacked by terrorists in the Middle East. During the opening moments of Operation Just Cause in Panama in 1989, it rescued Kurt Muse, an American citizen held in a Panamanian prison. In the Persian Gulf War, Delta Force served initially as bodyguards for top U.S. officers, and later as part of an effort to locate and destroy mobile SCUD missile launchers in the Iraqi desert. Delta Force also served in Task Force Ranger in Somalia (1993); a variety of operations associated with the Balkan wars of 1992–2000; Operation Enduring Freedom in Afghanistan in 2001–2002; and Operation Iraqi Freedom in 2003.

FURTHER READING:

BOOKS:

Beckwith, Charlie A., and Donald Knox. *Delta Force.* San Diego: Harcourt Brace Jovanovich, 1983.

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

Griswold, Terry, and D. M. Giangreco. *Delta, America's Elite Counterterrorist Force.* Osceola, WI: Motorbooks International, 1992.

Haney, Eric L. *Inside Delta Force: The Story of America's Elite Counterterrorist Unit.* New York: Delacorte Press, 2002.

Landau, Alan M., et. al. *U.S. Special Forces: Airborne Rangers, Delta, and U.S. Navy SEALs.* Osceola, WI: MBI, 1999.

SEE ALSO

ADFGX Cipher
Asymmetric Warfare
Australia, Intelligence and Security
Carter Adminstration (1977–1981), United States National Security Policy
DOD (United States Department of Defense)
France, Counter-Terrorism Policy
Germany, Counter-Terrorism Policy
Guerilla Warfare
Israel, Counter-terrorism Policy
SEAL Teams
Special Operations Command, United States
United States, Counter-Terrorism Policy

Department of State Bureau of Intelligence and Research, United States

CARYN E. NEUMANN

The Bureau of Intelligence and Research (INR) draws on intelligence from a range of sources to provide continuous independent analysis of global events to the secretary of

state and other diplomatic policymakers. Established in 1946 to aid United States foreign policy and national security goals, the bureau's location within the Department of State means that it has more knowledge of policy ingredients in a given estimative question than the analysts at the Central Intelligence Agency (CIA) or the various military intelligence agencies. Accordingly, INR is a member of the National Counterintelligence Policy Board (NCPB), provides briefings to the entire intelligence community, and helps oversee all U.S. government activities overseas.

The primary objective of INR is to serve the Department of State by ensuring that intelligence activities support foreign policy plans. It acts as the focal point in the department for ensuring policy review of sensitive counterintelligence and law enforcement activities, while also analyzing geographical and international boundary issues. In support of the State Department's responsibility for the oversight of all U.S. government activities overseas, INR coordinates the agency's activities relating to intelligence, security, counterintelligence, investigative, and special operations. It sits on the NCPB and participates in national security community decision-making on visa denial, intelligence sharing, as well as the requirements and evaluation for data collection in all intelligence disciplines.

INR staff draws on all-source intelligence, diplomatic reporting, its own public opinion polling, and interaction with U.S. and foreign scholars to provide early warning and in-depth analysis of events and trends. On an annual basis, INR analysts examine about two million reports to produce more than 6500 written assessments that are read by officials within the State Department, embassy personnel, the White House, the National Security Council, the Department of Defense, Congress, and the intelligence community.

The officers and analysts of INR draw upon a vast amount of knowledge. The bureau consists of about 300 employees who are organized into 19 offices that mirror the other divisions of the State Department. The employees, three-fourths of whom are Civil Service and one-fourth of whom come from the Foreign Service, blend both continuity and country-specific knowledge. They utilize thirty-six different languages to integrate new data and insights into their reports. Seventy-one percent of INR officials hold advanced degrees, with over a quarter possessing doctorates. On average, INR analysts and officers have spent six years within the bureau and 13 years studying the country or issue for which they are responsible.

Perhaps the most significant contribution that INR makes to national security comes through its estimative intelligence. The estimative views of INR help compose the National Intelligence Estimates (NIEs) produced by the National Intelligence Council (NIC). While most NIC officers come from the CIA, INR officials are part of the quarter of NIC analysts that are drawn from other parts of the government. When few facts are available, INR analysts help fill in the picture to predict what might be or might happen.

The major security lapses of the recent past such as the failure to predict the true strength of Soviet military defenses and the surprise testing by India of a nuclear bomb have led to calls to improve U.S. intelligence capabilities. Reinvigorating the diminished place of the State Department, particularly INR, in collecting and evaluating intelligence has been proposed as one means of bettering national security. Policymakers need estimative intelligence to help them understand the more diffuse and ambiguous threats and opportunities of the post-Cold War world and the specific knowledge offered by INR has historically served as a valuable national security component. Accurate and timely intelligence is the critical first line of defense against danger and INR provides exactly this material.

FURTHER READING:

BOOKS:

Ford, Harold P. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating.* Lanham, MD: University Press of America, 1993.

ELECTRONIC:

United States Intelligence Community. "Department of State: Bureau of Intelligence and Research. <http://www.intelligence.gov/1-members_state.shtml> (March 23, 2002).

SEE ALSO

CIA (United States Central Intelligence Agency)
Department of State, United States
Intelligence Community
National Intelligence Estimate
NIC (National Intelligence Council)
Terrorist Organization List, United States

Department of State, United States

JUDSON KNIGHT

The Department of State is a cabinet-level division of the United States government concerned with the planning, conduct, and management of U.S. foreign policy and foreign relations. The secretary of state is the highest-ranking member of the cabinet, and traditionally, secretaries of state have been among the most powerful members of the government. The State Department includes six major sections, each headed by an under secretary of state, concerned with Political Affairs; Economic, Business, and Agricultural Affairs; Arms Control and International Security; Global Affairs; Management; and Public

Diplomacy and Public Affairs. The department manages some 250 diplomatic posts worldwide, along with a number of special offices, bureaus, and agencies tasked to address issues such as counterterrorism, arms control and proliferation, organized crime, and narcotics trafficking. Also notable is the U.S. Agency for International Development (USAID), through which the United States extends assistance to nations recovering from disasters or trying to improve their political and/or economic conditions.

History

Oldest executive department of the federal government, the State Department grew out of the Committee of Secret Correspondence, established by the Continental Congress in 1775. Its first chairman was Benjamin Franklin. Over the next 14 years, the office went through a number of name changes until, on September 15, 1789, Congress designated it the Department of State.

Initially, the department had a range of domestic responsibilities, such as operation of the mint, issuing of patents, and regulation of immigration, that have long since passed on to other departments and bureaus. John Jay, who had served as secretary for foreign affairs (as the title of the chief American diplomat was called between 1781 and 1789) served as acting secretary until President George Washington's appointee, Thomas Jefferson, took office as secretary of state in 1790.

For the next 80 years, appointment as secretary of state tended to be set aside for persons distinguished in politics or government, but not necessarily diplomacy. These included future presidents Jefferson, James Madison, James Monroe, John Quincy Adams, Martin Van Buren, and James Buchanan, as well as other notable leaders, mostly from Congress, including Henry Clay, Daniel Webster, John C. Calhoun, and William H. Seward.

In those early years, America remained largely isolated from the rest of the world, and the State Department saw little activity except in times of war, or when the federal government sought to acquire lands. In the years leading up to the Civil War, Washington sought to ensure European support for the union, a critical matter since Great Britain and France depended to a large degree on cotton from the South.

The State Department only emerged as a vital component of U.S. policy after the Spanish-American War of 1898, as the United States acquired territories overseas and became increasingly involved in foreign affairs. The first modern secretary of state was John Hay, who, during his tenure (1898–1905), negotiated several treaties toward the building of the Panama Canal, and promoted open access to trade in China.

The fact that President Woodrow Wilson went personally to Paris to serve as U.S. negotiator at the post-World War I peace conference shows that even in 1919, the State Department had yet to acquire its present significance. Only in the wake of World War II did the United States, having fully left isolationism behind, begin to place a heavy emphasis on its State Department.

In the early years of the Cold War, three strong secretaries of state—George C. Marshall (1947–49), Dean Acheson (1949–53), and John Foster Dulles (1953–59)—helped forge the framework of U.S. policy. Among the components of that policy were containment of Communism, support for liberal democracies in Europe, and promotion of U.S. interests in the third world. The latter strategy involved not only alliances with pro-American movements, but also assistance. In service of this aim, President John F. Kennedy and Secretary of State Dean Rusk (1961–69) in 1961 created USAID and the Peace Corps. (The latter became an independent agency in 1981.)

Since the Kennedy era, the importance of the secretary of state has risen or fallen depending on the administration. The power of Henry Kissinger's (1973–77)influence was substantial, and was derived from his position as national security advisor, an office he held concurrent with his appointment at state for some time. Among the more active secretaries of State are two from the turn of the twentieth century: Madeleine Albright (1997–2001) and Colin Powell (2001—), who were also the first female and African American, respectively, to hold the position.

Duties and Structure

The State Department has its headquarters in a marshy area, nicknamed Foggy Bottom, near the Potomac River in Washington, D.C. Hence the name "Foggy Bottom" is sometimes used as a metonym for the department itself. The Department's entire foreign affairs budget—including U.S. representation overseas, foreign assistance programs, foreign military training, and efforts against international crime—comprised just one percent of the federal budget, and cost each American citizen about twelve cents a day.

To promote and protect U.S. interests abroad, the State Department works to assure peace and stability in regions of vital interest; to create jobs at home by opening markets overseas; to help developing nations establish stable economies that encourage growth and opportunities; and to bring nations together in order to address global issues such as disease, terrorism, humanitarian crises, environmental threats, weapons proliferation, and nuclear smuggling.

As the lead U.S. foreign affairs agency, the State Department has the primary role in leading interagency coordination in developing and implementing foreign policy; managing the U.S. foreign affairs budget and other foreign affairs resources; leading and coordinating U.S. representation abroad; conducting negotiations and concluding agreements; and coordinating and supporting the international activities of U.S. agencies and officials.

The department maintains embassies in about 180 nations, or all but about a dozen countries (among which are states such as Cuba, Iran, and North Korea), and also has representation with non-governmental organizations

such as the United Nations (UN) or NATO (North Atlantic Treaty Organization). Among the services provided by the department, both as a whole and through its various embassies, are protection and assistance for U.S. citizens living or traveling overseas; assistance for U.S. businesses in the international marketplace; coordination and support for international activities of other U.S. agencies, as well as other diplomatic efforts, including official visits overseas and at home; and keeping the public informed regarding U.S. foreign policy and international relations.

State Department leadership. The significance of the secretary of state, from an official standpoint, is indicated by the fact that he or she is fourth in the line of succession for the presidency, after the Speaker of the House, vice president and president *pro tempore* of the Senate. As chief diplomat, the secretary of State is the president's principal advisor on foreign affairs, and sits on the National Security Council (NSC) and other important committees. In practice, the importance of the secretary's position depends on the significance accorded to the office, or its holder, by the President. The secretary's relationship with Congress is also important to his or her success, because all authorization of funding for foreign policy initiatives comes from Capitol Hill. Additionally, the Senate must approve all treaties and ambassadorial appointments.

The Office of the Secretary of State includes a number of key positions and personnel, among them the Deputy Secretary and Executive Secretariat. The latter is responsible for inter- and intradepartmental coordination on foreign policy initiatives. Additionally, attached to the Secretary's office are a number of important bureaus, including the Policy Planning Staff, which provides the Secretary with independent policy planning and analysis; the Office of Protocol, whose duties include planning and hosting diplomatic events; the Office of the Coordinator for Counterterrorism, which works to improve coordination of U.S. counterterrorism efforts with those other governments; and a variety of other offices.

There are other bureaus that, while not attached to the Office of the Secretary, report directly to the Secretary. These include the Office of the Permanent Representative to the United Nations; the Bureau of Legislative Affairs; the Bureau of Intelligence and Research, part of the State Department's participation in the U.S. Intelligence Community; the Office of Inspector General, which independently audits Department activities; the Office of the Legal Adviser; and the Counselor of the Department, who advises the secretary on major foreign policy problems.

Under secretaries and their responsibilities. There are six under secretaries in the State Department. The under secretary of political affairs manages international crises, and is responsible for looking after U.S. political, economic, and security interests in the nation's bilateral relations. The section has six geographic bureaus—for African, East Asian and Pacific, European and Eurasian, Near Eastern, South Asian, and Western Hemisphere affairs—headed by assistant secretaries. Also within Political Affairs is the Bureau of International Organization Affairs, which coordinates U.S. policy within organizations such as the UN and NATO.

The under secretary for Economic, Business, and Agricultural Affairs is the senior economic official at the State Department, and addresses issues involving economics and trade. Duties include coordination of State Department efforts on behalf of U.S. businesses, as well as working with the Commerce Department to promote American economic interests abroad.

Within the purview of the under secretary for Arms Control and International Security are the Bureau of Arms Control, the Bureau of Political-Military Affairs, the Nonproliferation Bureau, and the Bureau for Verification and Compliance. As a whole, this section of the State Department is concerned with global U.S. security policy, primarily in the areas of nonproliferation, arms control, regional security and defense relations, arms transfers, and security assistance.

The under secretary for Management oversees a number of offices responsible for management improvement, security, information technology, support services, consular affairs, training, and other personnel matters. Among its sections is the Bureau of Diplomatic Security, which manages the Counterterrorism Rewards Program and the Overseas Security Advisory Council.

Included under the heading of the Global Affairs Group, headed by another under secretary, are offices that address a variety of global issues. Among these are the Bureau of Democracy, Human Rights, and Labor; the Bureau of International Narcotics and Law Enforcement Affairs; the Bureau of Oceans and International Environmental and Scientific Affairs; and the Bureau of Population, Refugees, and Migration.

Finally, the under secretary for Public Democracy and Public Affairs is concerned with cultural and educational exchanges, as well as international information programs. Its Bureau of Public Affairs helps Americans understand U.S. foreign policy, while the Bureau of Economic and Cultural Affairs attempts to foster mutual understanding between the Untied States and other nations. The Office of International Information Programs sponsors a variety of information and strategic communication initiatives involving print, electronic media, and the Internet.

FURTHER READING:

BOOKS:

Craig, Gordon Alexander, and Francis J. Lowenheim. *The Diplomats, 1939–1979.* Princeton, NJ: Princeton University Press, 1994.

Gore, Albert. *Department of State and U.S. Information Agency: Accompanying Report of the National Performance Review.* Washington, D.C.: U.S. Government Printing Office, 1993.

Plischke, Elmer. *U.S. Department of State: A Reference History.* Westport, CT: Greenwood Press, 1999.

Principal Officers of the Department of State and United States Chiefs of Mission, 1778–1990. Washington, D.C.: U.S. Department of State, 1991.

"Reinventing Government": Change at State. Washington, D.C.: U.S. Department of State, Bureau of Management, 1993.

State 2000: A New Model for Managing Foreign Affairs: Report of the U.S. Department of State Management Task Force. Washington, D.C.: U.S. Government Printing Office, 1993.

ELECTRONIC:

U.S. Agency for International Development. <http://www.usaid.gov/> (April 25, 2003).

U.S. Department of State. <http://www.state.gov/> (April 25, 2003).

SEE ALSO

Coordinator for Counterterrorism, United States Office
Department of State Bureau of Intelligence and Research, United States
Diplomatic Security (DS), United States Bureau
FEST (United States Foreign Emergency Support Team)
International Narcotics and Law Enforcement Affairs (INL), United States Bureau
Terrorist Organization List, United States

DIA (Defense Intelligence Agency)

JUDSON KNIGHT

The Defense Intelligence Agency (DIA) coordinates intelligence activities within the U.S. Department of Defense (DOD). Established in 1961, DIA has faced a number of territorial challenges both from the intelligence components of the three major armed services, as well as from other intelligence agencies. DIA, which has some 7,000 civilian and military employees worldwide, is headquartered at the Pentagon in Washington, D.C. Its director is a three-star military officer who serves as principal military intelligence advisor to the secretary of defense and the chairman of the Joint Chiefs of Staff (JCS).

Background

Despite the congressional passage of the 1958 Defense Reorganization Act, which created unified military commands, the U.S. Army, Navy, and Air Force each guarded their intelligence organizations. As a result, DOD leadership did not receive consistent, reliable intelligence, a shortcoming that contributed to the failed April 1961 invasion of Cuba. Even before that, President John F. Kennedy complained in his 1961 State of the Union speech about "a growing gap between decision and execution, between planning and reality." In February, 1961, Defense Secretary Robert S. McNamara informed JCS of his decision to create a Defense Intelligence Agency, and instructed the Joint Chiefs to develop a plan for the new organization, which began operation on October 1, 1961.

The intention behind DIA was that it should serve as a tight union, rather than a loose confederation, of defense intelligence and counterintelligence activities, so as not to increase the bureaucratic layering within an already thickly populated defense intelligence community. Its director would report to the secretary of defense through JCS. Upon establishment of DIA, the services transferred various intelligence functions to it gradually, so as to maintain the pace of ongoing activities. The job of DIA would be to collect, process, evaluate, analyze, integrate, produce, and disseminate military intelligence for DOD.

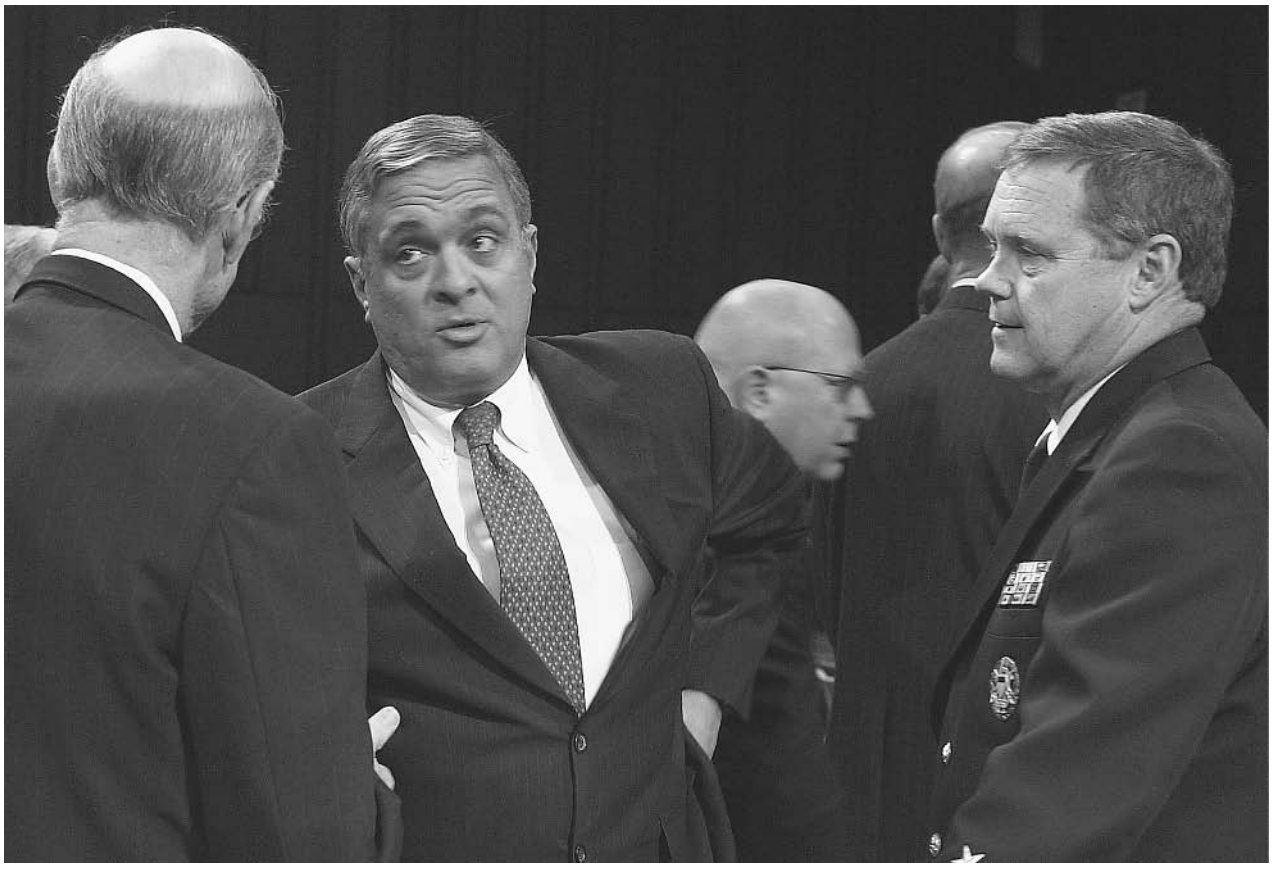
As DIA has admitted in its own official history, its attempts to establish itself as the central military intelligence organization within DOD met with continuing resistance from the military services during the 1960s. First, the services retained their own military intelligence organizations, and their leadership was often wary of sharing intelligence with a relative newcomer. The Vietnam War, in which DIA was tasked with helping to account for missing or captured military personnel, particularly tested the abilities of the fledgling agency.

By the mid-1970s, DIA had gained considerable funding, but its budget of more than $200 million annually made it a target for congressional inquiries, particularly by the Pike Committee, the House equivalent of the more well-known Church Committee in the Senate. Within the Intelligence Community, Admiral Stansfield Turner, director of the Central Intelligence Agency (CIA) criticized DIA's inability to effectively coordinate military intelligence activities on the part of the various services.

Executive Order 12036, signed by President James E. Carter on January 24, 1978, restructured the Intelligence Community and brought DIA's responsibilities into focus. The agency was subsequently reorganized into five directorates, concerned with production, operations, resources, external affairs, and J-2 (joint intelligence) support. During the 1980s, a DIA white paper series on Soviet military capabilities gained wide respect in the intelligence community.

Soon after the Iraqi invasion of Kuwait in August, 1990, DIA established a 24-hour intelligence management center focusing on intelligence relating to the crisis. Some 2,000 DIA personnel participated in Operation Desert Storm, primarily through the National Military Joint Intelligence Center (NMJIC), which DIA established at the Pentagon to integrate intelligence from the war front. On the ground in Kuwait and Iraq, DIA personnel worked closely with military combat units.

In 1992, the Armed Forces Medical Intelligence Center and the Missile and Space Intelligence Center, both controlled by the Army for decades, became part of DIA. The



Vice Admiral Thomas Wilson, right, confers with CIA Director George Tenet, center, after Tenet's testimony before the Senate Armed Servives Committee in March 2002, to discuss the threat to U.S. interests around the world by al Qaeda. AP/WIDE WORLD PHOTOS.

following year saw a thoroughgoing reorganization of DIA as part of the general military downsizing that followed the end of the Cold War. In October 1995, DIA established the Defense HUMINT [Human Intelligence] Service, or DHS.

Structure of DIA

Though DIA was conceived as a military organization, the majority of its personnel today are civilians. The director, however, is always a three-star officer—a lieutenant general or vice admiral. (The only exceptions were General Donald V. Bennett, director from 1969 to 1972, a four-star general, and Dennis M. Nagy, a civilian who served as acting director during the fall of 1991.) In addition to the Command Element, which includes leadership and support staff, DIA consists of three major sections: Analysis, Intelligence Operations, and Support Services.

Within the Analysis section are the directorates for Analysis and Production; Intelligence, Joint Staff (J2); and Policy Support. Analysis and Production manages key components of the intelligence cycle for DOD, its leadership, and its services. The directorate for Intelligence, Joint Staff (J2) supports the chairman of JCS and other uniformed leaders by providing a national-level focal point for crisis intelligence support. Within it is the Defense Intelligence Network, which operates a closed circuit DOD news network modeled on commercial news networks such as CNN, as well as INTELINK, a classified Internet. Policy Support works with the Office of the Secretary of the Defense, as well as the National Security Council and State Department.

Intelligence Operations includes the directorate for Intelligence Operations and the Central MASINT Organization. These are concerned, respectively, with human intelligence and measurement and signatures intelligence. Within the directorate for Intelligence Operations is DHS, the Defense HUMINT Service.

Under Support Services are the directorates for Administration and Information Systems and Services. Among the administration sections is the Counterintelligence and Security Activity, which works to counter foreign intelligence threats, conducts security and suitability interviews, and assists the Federal Bureau of Investigation and military investigative organizations in criminal and counterintelligence investigations. Information Systems and Services supports a number of activities, including the operation of the Joint Worldwide Intelligence Communications System, a high-bandwidth system that makes possible full-motion video teleconferencing and data exchange among major intelligence nodes.

In addition to these main sections, DIA also includes the Program Management directorate, under which is the Military Intelligence Board, the DIA director's advisory committee. Also outside the main sections of DIA is the Joint Military Intelligence College, which is accredited to award bachelor's and master's degrees in intelligence and strategic intelligence.

FURTHER READING:

BOOKS:

Disposition of Production Records of the Defense Intelligence Agency: A NARA Evaluation. Washington, D.C.: National Archives and Records Administration, 1996.

Intelligence Agencies: Personnel Practices at CIA, NSA, and DIA Compared with Those of Other Agencies. Washington, D.C.: General Accounting Office, 1996.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

Scanlon, Charles Francis. *In Defense of the Nation, DIA at Forty Years.* Washington, D.C.: Defense Intelligence Agency, 2002.

ELECTRONIC:

Defense Intelligence Agency. <http://www.dia.mil/> (April 14, 2003).

Defense Intelligence Agency. Federation of American Scientists. <http://www.fas.org/irp/dia/> (April 14, 2003).

SEE ALSO

Air Force Intelligence, United States
Bay of Pigs
DOD (United States Department of Defense)
HUMINT (Human Intelligence)
INSCOM (United States Army Intelligence and Security Command)
Intelligence
Intelligence Community
Intelligence, United States Congressional Oversight
Internet
Kennedy Administration (1961–1963), United States National Security Policy
Measurement and Signatures Intelligence (MASINT)
National Military Joint Intelligence Center
NMIC (National Maritime Intelligence Center)
NRO (National Reconnaissance Office)
NSA (United States National Security Agency)
Persian Gulf War

Dial Tone Decoder

Telephone conversations are sometimes surreptitiously taped using microphones or other bugging devices. These devices run the risk of being detected. In some intelligence-gathering tapings, however, the contact telephone number may yield information that is as valuable as the actual conversation. If the content of a conversation is not essential, the contact telephone number can be obtained with a device called a dial tone recorder.

In a touch-tone telephone, each digit from 0 through 9 produces two tones when the particular key is pressed. Each tone has a particular wavelength (i.e., height of the peak and trough of the wave) and a frequency (i.e., the number of waves and troughs per unit area). One of the tones is from a low group, which represents the rows on the telephone keypad. The other tone is from a high group, which represents the columns on the keypad. The function of the dial tone decoder is to decipher the tone pairs and match up the combination with the row and column location on the telephone keypad. In an operating phone, this information is passed to a switch, which routes the signal to the phone line, allowing the call to proceed.

A dial tone decoder is also a standard feature of touch tone telephones, and makes the phone capable of converting the numerical and symbolic information that is entered using the phone's keypad into a signal that can complete the transmission.

A decoder can also detect a busy signal. In espionage, this allows the eavesdropper to find out whether the telephone being monitored is in use. Dial tone decoders can also route the dial tones to a personal computer equipped with an infrared port, as the electrical impulses of the tones can be converted to infrared radiation. Thus, a computer can be used to record the activity of a telephone over time, including the numbers dialed during that period.

Instances of assassination via cellular telephones equipped with a decoder and an explosive device have occurred in contested areas of the Middle East in the late 1990s. When the subject answered the telephone, a code was entered that triggered a blast. Detection of the code by the dial tone decoder triggers the explosive device. In this way, attacks were carried out from remote locations. In an Islamist militant group Hamas attack in July 2002, five Americans and four Israelis were killed at the Hebrew University in Israel after a bomb placed in a backpack in the university cafeteria was remotely detonated by cell phone.

In police investigations, dial tone decoders are routinely used for intelligence gathering, and are also used by telephone repair crews to verify phone numbers.

FURTHER READING:

BOOKS:

Goleniewski, Lillian. *Telecommunication Essentials.* Boston: Addison Wesley Professional, 2001 .

Ledwidge, Michael S. *Bas Connection.* New York: Simon & Schuster, 2001.

Proakis, John G. *Digital Communications.* New York: McGraw-Hill, 2001.

SEE ALSO

Microphones

Telephone Recording Laws
Telephone Scrambler

Digital Watermarking.

SEE *Steganography.*

Diplomatic Security (DS), United States Bureau

CARYN E. NEUMANN

The Bureau of Diplomatic Security (DS) is the law enforcement and security arm of the United States Department of State. Created on November 4, 1985, it bears responsibility for ensuring the safety of Americans who are serving their government in embassies and consulates overseas as well as protecting foreign dignitaries who visit the United States. It also investigates crimes involving passport and visa fraud.

Diplomats traditionally have given little concern to security. Aware of this shortcoming and the increasing risks of terrorism, the secretary of state convened an Advisory Panel on Overseas Security under the chairmanship of retired Admiral Bobby R. Inman. The 1985 Inman Report warned that growing security demands at home and abroad required the Department of State to establish a professional law enforcement service with its own structure for personnel recruitment, advancement, and assignment. In light of the danger of mob attacks and terrorist sabotage upon U.S. embassies, the panel also recommended that more physically secure sites and buildings replace a large number of diplomatic facilities around the world. The new service would initiate and direct this relocation and building program.

Upon its creation, DS began providing protective details based on the level of threat to selected foreign officials within the U.S as well as to American ambassadors and other officials overseas. It does not protect visiting heads of state but, in response to specific threats made against them, will guard foreign missions in the U.S. through agreements with state and local law enforcement authorities. On the average, DS participates in more than 150 foreign and domestic dignitary details each year. By the mid-1990s, DS personnel had thwarted twenty-two assassinations in progress, eighteen of them overseas. The service also evacuated embassies in nations on the verge of collapse.

To monitor and analyze all international and domestic terrorism matters, DS relies upon Intelligence and Threat Analysis (ITA) to link with the U.S. intelligence community. Besides issuing a classified Daily Security Brief to senior DS and State Department officers, ITA produces two annual publications. *Significant Incidents of Political Violence against Americans* is a narrative and statistical compendium of all acts of terrorism and political violence against U.S. interests in a given year. *Terrorist Tactics and Security* Procedures offers case studies of specific terrorist attacks or security developments that affect the safety of Americans abroad. ITA also distributes the semiannual Security Environment Threat List (SETL), which helps DS prioritize resource allocation by categorizing political risks and crime at all U.S. missions overseas.

DS also attempts to deter the efforts of foreign intelligence agencies to compromise U.S. employees. It investigates crimes involving passport and visa fraud while examining the backgrounds of employees, applicants, contractors, and others who seek access to Department of State information or facilities. Additionally, the service investigates personnel security matters with counterintelligence ramifications in conjunction with the National Counterintelligence Center.

DS generally receives little notice and is probably best known for its regular bulletins of security suggestions for U.S. business representatives overseas. By working with the Department of State's Overseas Security Advisory Council as well as American embassies and consulates, it provides current information about precautions that can provide some degree of protection by serving as psychological and practical deterrents to would-be terrorists. This information includes warnings about new crime strategies, such as kidnappers who first appear as vendors operating carts across from the homes of Americans, as well as time-honored advice like recommendations to vary daily travel routes.

The volume of DS investigations has steadily increased each year. In light of the current high risk of terrorist activity, the demand for DS service will likely continue to grow.

FURTHER READING:

BOOKS:

Katz, Samuel M. *Relentless Pursuit: The DSS and the Manhunt for the al-Qaeda Terrorists.* New York: Tom Doherty Associates, 2002.

Smith, G. Davidson. *Combating Terrorism.* New York: Routledge, 1990.

United States Department of State, Bureau of Diplomatic Security. *Countering Terrorism: Security Suggestion for U.S. Business Representatives Abroad.* Washington, D.C.: Department of State, 1999.

ELECTRONIC:

United States Department of State. "Bureau of Diplomatic Security." March 29, 2003 <http://www.ds.state.gov> (March 29, 2003).

SEE ALSO

Architecture and Structural Security

Assassination
Department of State, United States
Security Clearance Investigations
Terrorism, Intelligence Based Threat and Risk Assessments
Terrorist Organization List, United States

Directed Energy Weapons.

SEE *Defense Initiative and National Missile Defense.*

Dirty Bombs.

SEE *Russian Nuclear Materials, Security Issues.*

Dirty Tricks

Dirty tricks are clandestine activities carried out by a covert-action group to discredit, destabilize, or eliminate an opposing regime, one of its agencies or departments, or an individual. A type of covert operation, dirty tricks include everything from the spreading of false rumors to sabotage, overthrow, and assassination.

American dirty tricks. The history of dirty tricks practiced by the United States Central Intelligence Agency (CIA) is a long one. Among the most significant examples in this extensive catalogue are the many attempts to undermine or neutralize Cuban dictator Fidel Castro. These ranged from large-scale conspiracies such as assassination plans and the Bay of Pigs invasion to bizarre brainstorms at the fringes of practicability. An example of the latter was a plot to introduce a substance that would cause Castro's famous beard to fall off, thus presumably eliminating his machismo and thus his credibility with the Cuban people.

Castro was far from the only foreign leader targeted by CIA dirty tricks. Another example was Chilean president Salvador Allende, who steered his nation toward Marxism in the early 1970s. The CIA bribed members of the Chilean Congress, and employed a number of means to foment unrest in Chile. Evidence gathered by the Church Committee of the U.S. Senate indicates that the CIA may have been behind the truckers' strike of 1972–73 that helped spawn the coup in which Allende lost his life and General Augusto Pinochet took power.

Soviet dirty tricks. Though CIA dirty tricks, such as those that were revealed in the course of the Iran-Contra hearings in the late 1980s, are legendary for their cunning, the United States is hardly the only nation that has employed dirty tricks in its covert operations. Another example is the Soviet Union, whose KGB operatives were past masters at such tactics ranging from disinformation to assassination. The Soviets, of course, had the advantage—at least, in countries where their system gained control—of being able to suppress all undesirable information. Yet, even before the fall of the Soviet empire, extensive information on Soviet activities was available.

To cite one example among many of those noted by British journalist Chapman Pincher in *The Secret Offensive* (1985) the Soviets sought to strike back at Egyptian president Anwar Sadat for his increasingly pro-American acts by printing leaflets attacking him as a U.S. puppet. These tracts, which the CIA traced to the Soviets, but which were purportedly issued by Muslim fundamentalists, helped fan the flames of the Muslim Brotherhood, which had Sadat assassinated in 1981. The KGB also provided the Weathermen, a U.S. radical group in the 1960s, with money and other forms of assistance through Cuban intermediaries, and Soviet support for terrorist groups attempting to destabilize western Europe during the 1970s and 1980s is well-documented.

FURTHER READING:

BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

Carney, John T., and Benjamin F. Schemmer. *No Room for Error: The Covert Operations of America's Special Tactics Units from Iran to Afghanistan.* New York: Ballantine, 2002.

Pincher, Chapman. *The Secret Offensive.* New York: St. Martin's, 1985.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* third edition. Boulder, CO: Westview Press, 1995.

SEE ALSO

Black Ops
Church Committee
CIA (United States Central Intelligence Agency)
Iran-Contra Affair
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*

Disinformation

MARTIN J. MANNING

Disinformation is mostly commonly described as false information created by governments in wartime for military purposes and by totalitarian governments for political

University students protest against possible fraud in the 2000 elections in Peru. The word "SIN" refers to Peru's national intelligence agency, which allegedly used dirty tricks and intimidation to give the incumbent President Alberto Fujimori an unfair advantage over his opponent, Alejandro Toledo. Fujimori later resigned and Toledo gained the presidency. AP/WIDE WORLD PHOTOS.

purposes in peacetime. Rumors, lies, and other forms of disinformation were made public by the Soviet Union to discredit the United States, the latter being the context in which the word is generally applied. The KGB coined the Russian word *dezinformatsiya*; it came into the English language as disinformation. The technique of disinformation goes back at least to 1918 with the end of World War I. Disinformation as a KGB weapon began in 1923 when I. S. Inshlikht, deputy chairman of the GPU, then the name of the KGB, proposed the establishment of a special disinformation office to conduct active intelligence operations.

Soviet active measures. Soviet active measures refer to the influence operations organized by the Soviet government. These include white, gray, and black propaganda, as well as disinformation. White propaganda was created by the Information Department of the Communist Party and included those publicly identified Soviet channels as Radio Moscow, Novosti, and pamphlets and magazines as well as official Soviet government statements. Gray propaganda was organized by the International Department of the Communist Party and used such channels as the foreign Communist Parties and the network of international Soviet fronts. Black propaganda was prepared by the KGB and included agents of influence, covert media placements, and until 1959, assassinations. Forgeries and disinformation were used by the Soviets in all modes. The first effective disinformation campaign was during the Korean Conflict. This was a major Soviet disinformation campaign that generated media attention. The Americans were accused of going into Korean villages during the Korean conflict (1950–1953) and shooting villagers, or killing them with biological weapons and chemical warfare. In fact, the Soviets used anthrax in Korea to kill men, women, and children, and then blamed it on the Americans.

An attempt is now underway with the Cold War History Project at the Woodrow Wilson International Center for Scholars, Smithsonian Institution, in Washington, DC, to counter this account, especially through the work of Katherine Weathersby who discovered that Soviet documents obtained through a Japanese researcher belied these rumors and accusations. The issue re-surfaced in the book *United States and Biological Weapons: Secrets of the Early Cold War and Korea* (Indiana University Press,

1999) by Stephen Endicott and Edward Hagerman. Endicott was the son of one of the men who helped to disseminate the disinformation campaign, James Endicott.

On September 9, 1982, President Ronald Reagan designated the United States Information Agency to lead an inter-departmental effort to counter Soviet propaganda and disinformation. For an advisory body, the administration created the Active Measures Working Group in 1981 to bring together the information the various agencies held to counter Soviet disinformation and forgery. It served as a clearinghouse to expose such information and it had permission to use classified documents and any other resources that were required to meet this goal. The Working Group was chaired by the State Department with representatives from State, Central Intelligence Agency, Defense Intelligence Agency, Arms Control and Disarmament Agency, United States Information Agency, and the Defense and Justice Departments. The Working Group ended in 1991, two years after the collapse of the Soviet Union.

AIDS disinformation campaign. A major effort for the Working Group was the AIDS disinformation campaign, a controversial topic that had basis as a Soviet disinformation campaign. A sensational disinformation story appeared with allegations that the United States deliberately created AIDS in the laboratory to use it as a weapon. The KGB started the story in 1985 with placements in both Soviet and foreign newspapers; by September, 1986, it became a major campaign when an English language paper that actually originated in East Berlin carried the story. "AIDS: Its Nature and Origin," was distributed at the Non-Aligned Movement Summit in Harare, where it contained pseudo scientific verbiage, but the only evidence linking the origin of AIDS to U.S. military laboratories was the following unfounded statement: "The first appearance of AIDS exactly coincides with the opening of a P-4 laboratory at Fort Detrick [Maryland]—taking into account the incubation period. This is also indicated by the fact that the spreading of AIDS to the world emanated from New York, a city in the neighbourhood of Fort Detrick. The assumption that AIDS is a product of the preparation of biological warfare can therefore quite plainly be expressed."

The Soviet disinformation campaign accused the U.S. government of creating the AIDS virus as a weapon against black people and the story quickly appeared worldwide, despite U.S. protests that Fort Detrick, in Maryland, was hundreds of miles from New York. In April 1987, U.S. Surgeon General C. Everett Koop advised the Soviets that if this campaign continued, "direct U.S.-Soviet collaboration on AIDS research would be impossible." The KGB then began winding down the worldwide campaign, but other countries continued to endorse the disinformation. In Africa, stories circulated for years that the United States created the AIDS virus. The U.S. Information Service (USIS, USIA overseas) staff responded with accurate information that countered these charges and defused the situation. In Pretoria, South Africa, and in Lilongwe, Malawi, USIS information was able to refocus the media on AIDS prevention rather than on false blame.

World Trade Center attacks. After the terrorist attacks of September 11, 2001, a disinformation campaign originated that 4000 Jewish persons did not show up for work at the World Trade Center on that day. Authorities have not determined the origin of the disinformation, but have concluded that its source was probably from an Arabic region, as the circulated disinformation did not mention the fact that the hijackers were Arabic. This was the first recorded account of an urban legend that has swept the Arab world, and no facts in it have ever been substantiated. The disinformation appears to be based on concern expressed by the Israeli government for the fate of 4,000 Israeli residents in New York, a small number of whom worked at the World Trade Center. Within a matter of days it was no longer 4,000 Israelis who were supposed not to have turned up to work, but 4,000 Jewish persons; then reports appeared that no Jewish persons died on September 11. In fact, many Jewish Americans died in the attack, as well as four Israeli citizens—two in the World Trade Center and two on hijacked planes, according to the Israeli Foreign Ministry.

In August, 2002, the U.S. Government countered allegations that Abdul Salem Zayef, the former ambassador to Pakistan, had been tortured and killed in captivity at the United States' Guantanamo detention center in Cuba. After the U.S. Embassy in Islamabad alerted the Department of State that the story was appearing in the Urdu press and that allegations were being broadcast as fact on state-controlled media, the State Department worked with elements in the Department of Defense to track how the disinformation was being disseminated, and to prepare guidance. In April, 2003, the Embassy in Islamabad also countered allegations about damage to the Adhamiya Mosque in Baghdad, which houses the Imam Abu Hanifa, with relevant CENTCOM news releases and information given for a story in the *New York Times*. Additionally, in April 2003, the U.S. Embassy in Beirut, Lebanon, responded to allegations about "tranquilizer chemical weapons" with the Department of Defense's statement that "Incapacitating agents are agents that put people to sleep by slowing the nervous system considerably. The Department of Defense does not possess any incapacitating agents and has no plans to conduct research in this area."

Depleted uranium. A Gulf War disinformation campaign that began when a South African minister spoke to the media about the supposed genocide caused by the use of uranium depletion weapons in the 1991 Persian Gulf War. This disinformation was started by Minister Doug Rokke in a presentation to members of the South African Parliament on January 31, 2001, when he made a number of

assertions about depleted uranium. Media reports quoted him saying that he knew only one person from his team who was not sick from depleted uranium exposure, and represented that tests revealed 5,000 times the permissible level of uranium in his body. Rokke was presented as the Department of Defense's (DOD) expert on depleted uranium and the director of the Pentagon's depleted uranium project. His comments resulted in a renewed fear about the effects of spent uranium depletion weapons.

In order to correct the record, the Defense Department revealed Rokke as a private citizen not affiliated with the U.S. Department of Defense. Following the war, Rokke was attached for duty to assist technical experts in the recovery and decontamination of radioactive material and equipment. The team of approximately 10 people was led, not by Rokke, but by a civilian from the Army Munitions and Chemical Command (AMCCOM). Rokke's primary role was to facilitate the recovery operations by ensuring the team had the proper support. In the following years, Rokke reported varying numbers of ill or dead co-workers. DOD staff compiled a list of 29 names of people Rokke reported to be on "his team." Staff members were able to interview 22 of them. Approximately 15 of the 29 people Doug Rokke had identified actually worked on depleted-uranium contaminated vehicles. Two of the 29 had died, however, neither of these two veterans was named as having worked with depleted uranium.

Iraqi propaganda. Early in 2003, the White House issued "Apparatus of Lies: Saddam's Disinformation and Propaganda, 1990–2003" (Washington, D.C.: U.S. Department of State, 2003) compiled by State and Defense Departments disinformation specialist Todd Leventhal. This report highlighted the apparatus used by Saddam Hussein and his cadres to deceive the Iraqi people and the international community. The oppressive and totalitarian nature of Saddam Hussein's regime enabled this deception. This regime, which became expert at obfuscation during the 1991 Persian Gulf War, had more than a decade to perfect these practices before it was finally toppled by the allied forces in March and April, 2003.

In December, 1998, when United Nations weapons inspector Richard Spertzel became exasperated by Iraqi evasions and misrepresentations, he confronted Rihab Taha, the woman the Iraqis identified as the head of their biological weapons program and asked her directly, "You know that we know you are lying. So why do you do it?" She replied: "Dr. Spertzel, it's not a lie when you are ordered to lie." In January, 2003, Taha refused to be interviewed by U.N. weapons inspectors, but after Operation Iraqi Freeedom, Taha surrendered to U.S. authorities on May 12, 2003.

In their disinformation and propaganda campaigns, the Iraqis used elaborate ruses and obvious falsehoods, covert actions and false on-the-record statements, and sophisticated preparation and spontaneous exploitation of opportunities. Iraq has used four types of campaigns to promote its propaganda and disinformation:

- Crafting tragedy: To craft tragedy, the regime places civilians close to military equipment, facilities, and troops, which are legitimate targets in an armed conflict. The Iraqi regime openly used both Iraqis and foreigners as human shields during the Gulf War, eventually bowing to international pressure and releasing many of them. Iraq also placed military equipment next to or inside mosques and ancient cultural treasures. Finally, it has deliberately damaged facilities and attributed the damage to coalition bombing, and has attempted to pass off damage from natural catastrophes, such as earthquakes, as the result of bombing.
- Exploiting suffering: To exploit suffering, Saddam Hussein blamed starvation and medical crises—often of his own making—on the United Nations or the United States and its allies. The Iraqi regime caused or actively ignored hardship and then aggressively exploited the Iraqi people's suffering. During the last decade, the Iraqis have aggressively promoted the false notion that depleted uranium—a substance that is relatively harmless and was used for armor-piercing munitions during the Gulf War—has caused cancers and birth defects among Iraqis. Scientific evidence indicates that any elevated rates of cancer and birth defects are most likely due to Iraqi use and testing of chemical weapons.
- Exploiting religion: Experts know that Saddam Hussein was a non-religious man from a secular—even atheistic—party. In order to exploit religious sentiments, he adopted expressions of faith in his public pronouncements, and the Iraqi propaganda apparatus erected billboards and distributed images showing him in other acts of piety—all while his regime prevented citizens from engaging in religious pilgrimages. Inflammatory disinformation designed to incite Muslims against its adversaries has also been used.
- Corrupting public records: To corrupt the public record, the Iraqi regime used a combination of on-the-record lies, covert placements of false news accounts, self-inflicted damage, forgeries, and fake interviews.

Other main tools of Iraqi disinformation included restricting journalists' movements; false claims or disclosures; false man-in-the-street interviews; self-inflicted damage; on-the-record lies; covert dissemination of false stories; censorship; edited or old television footage and images; and fabricated documents. Recent U.S. government reports, including "A Decade of Defiance and Deception," documented these deceptions regarding UN resolutions and weapons inspections. In order to raise awareness of the many other Iraqi forms of deception, particularly those likely to be repeated, "Apparatus of Lies" examined the facts behind Iraqi disinformation and propaganda since 1990. The U.S. Defense Department countered these disinformation tactics by embedding over 300 world journalists with United States Marines during Operation Iraqi Freedom in March-April, 2003.

The author wishes to acknowledge Herb Romerstein for his contributions to this article.

FURTHER READING:

BOOKS:

Bittmann, Ladislav. *The KGB and Soviet Disinformation.* Washington: Pergamon-Brassey's International Defense Publishers, 1985.

Romerstein, Herbert. *Soviet Active Measures and Propaganda: "New Thinking" and Influence Activities in the Gorbachev Era.* Toronto, Canada: Mackenzie Institute for the Study of Terrorism, Revolution, and Propaganda; Washington, D.C.: National Intelligence Book Center, 1989.

Shultz, Richard H., and Roy Godson, *Dezinformatsia.* Washington: Pergamon-Brassey's International Defense Publishers, 1984.

U.S. Congress. House. Permanent Select Committee on Intelligence. *Soviet Active Measures: Hearings.* 97th Congress, 2d Session. Washington, D.C.: GPO, 1982.

U.S. Congress. Senate. Committee on Foreign Relations. Subcommittee on European Affairs. *Soviet Active Measures: Hearings.* 99th Congress, 1st Session. Washington, D.C.: GPO, 1985.

U.S. Department of State. *Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns.* Washington, D.C.: The Department, 1986.

———. *A Report on Active Measures and Propaganda, 1986–87.* Washington, D.C.: The Department, 1987.

———. *A Report on Active Measures and Propaganda, 1987–1988.* Washington, D.C.: Department, 1989.

PERIODICALS:

Douglass, Joseph D. "The Growing Disinformation Problem," *International Security Review* 4 (1981): 333–353.

Kux, Dennis. "Soviet Active Measures and Disinformation: Overview and Assessment," *Parameters, Journal of the U.S. Army War College* 15, no. 4: 19–28.

McDonnell, Sharon. "In From the Cold," *American Journalism Review* (June 1995): 16–17.

OTHER:

Romerstein, Herbert. "Disinformation as a KGB Weapon in the Cold War." Prepared for a Conference on Germany and Intelligence Organizations: The Last Fifty Years in Review, sponsored by Akademie fur Politische Bildung Tutzing, June 18–20, 1999.

U.S. Information Agency. *Soviet Active Measures in the Era of Glasnost.* Prepared at the request of the U.S. House of Representatives, Committee on Appropriation, for presentation at a hearing on March 8, 1988, by Charles Z. Wick, Director, United States Information Agency. (Washington, 1988).

SEE ALSO

Iraq War: Prelude to War (The International Debate over the Use and Effectiveness of Weapons Inspections.)
Iraqi Freedom, Operation (2003 War against Iraq)
Persian Gulf War
Propaganda, Uses and Psychology

DNA

JULI BERWALD

Because of the uniqueness of every human's DNA and the ubiquity of DNA in cells, this genetic molecule has become an important tool for the identification of individuals, both in forensics and security applications. Deoxyribonucleic acid (DNA) consists of two twisted strands of polymers, made up of mononucleotide units. Each nucleotide is composed of three separate parts: a 2-deoxyribose sugar ("2-deoxy-" because the hydroxyl or -OH group of the ribose sugar is missing from the second carbon position on the sugar ring), a phosphate, and one of the four bases: adenine (A), guanine (G), cytosine (C), thymine (T). The deoxyribose sugar and phosphate are linked by phosphodiester bridges in such a way as to form an unbranched polynucleotide chain. According to the Watson-Crick model, which was published in 1953, the DNA molecule consists of two such polynucleotide chains which are complementary but not identical and which spiral around an imaginary common axis. The two strands are antiparallel, meaning that the phosphodiester links between the deoxyribose units read in opposite directions designated 5′ to 3′ on one chain and 3′ to 5′ on the other. The bases, which are perpendicular to the helix axis, protrude at regular intervals from the two spiral sugar phosphate strands, and reach into the interior of the helix. The strands are annealed together by hydrogen bonds between the bases of opposite strands and for correct annealing to occur a purine (adenine or guanine) on one strand must pair with a pyrimidine (thymine or cytosine) on the other. Within the constraints of the double helix, hydrogen bonds can only form between adenine and thymine (A:T) and between guanine and cytosine (G:C). Through this pairing, the arrangement of bases along one strand determines that of the other and the genetic information is thus coded in these base sequences.

The most commonly described DNA structure is that of the right-handed Watson-Crick double helix, also known as B-DNA, which has a diameter of 20Å. The double helix is not symmetrical and has a broad groove and a narrow groove between the chains, known respectively as the major and minor grooves. Adjacent bases are separated by 3.4Å along the helix axis and related by a rotation of 36° which causes the helix structure to repeat after 10 residues on each chain, that is at intervals of 34Å. DNA is, however, a dynamic molecule whose structure can vary and there are two other commonly found DNA conformations, each with slightly different dimensions.

An FBI official holds a chart of the Combined DNA Index System (CODIS), a computerized database that allows law enforcement officers from around the country to compare DNA genetic evidence taken from convicted felons and gathered in unsolved cases. AP/WIDE WORLD PHOTOS.

The DNA molecule contains all of the genetic information for every organism. Within a cell, DNA is organized into long strands called chromosomes. Every chromosome contains many thousands of different genes. A gene is a functional segment of DNA that codes for a specific protein. During protein synthesis, a portion of DNA is translated into a complementary strand of ribonucleic acid (RNA), which is further transcribed into a sequence of amino acids. A sequence of three nucleotides is required to code for one amino acid and chains of amino acids are further modified outside the nucleus of the cell into the proteins. There are approximately 50,000 different types of proteins in the human body and they either perform tasks or synthesize molecules required for the biological activity that sustains life. The DNA in every individual, therefore, is the source of information the directs all of the biological functions in the body.

The DNA molecule is inherited by every cell and every individual. In asexual reproduction, the DNA in chromosomes is unwound and duplicated before the cell divides. Both daughter cells receive exact copies of the parent cell's DNA. In sexual reproduction, a portion of the DNA is inherited from both the female and the male parent. In humans, there are 23 pairs of chromosomes in the genome. During meiosis, which forms the sex cells or gametes (the egg in females and the sperm in males), the chromosomal pairs separate and each gamete receives 23 unpaired chromosomes. When a sperm fertilizes an egg, its 23 unpaired chromosomes are paired with the 23 unpaired chromosomes in the egg and the resulting zygote contains a unique set of paired chromosomes.

SEE ALSO

DNA Fingerprinting
DNA Recognition Instruments
DNA Sequences, Unique

DNA Fingerprinting

DNA fingerprinting is the term applied to a range of techniques that are used to show similarities and dissimilarities between the DNA present in different individuals.

DNA fingerprinting is an important tool in the arsenal of forensic investigators and intelligence officers. In an era when plastic surgery can be used to alter a terrorist's appearance, DNA fingerprinting allows for positive identification not only of body remains, but also of suspects in custody. DNA fingerprinting can also link physical evidence from incidents that occur in different parts of the world.

Sir Alec Jeffreys at the University of Leicester developed DNA fingerprinting in the mid 1980s. The sequence of nucleotides in DNA is similar to a fingerprint, in that it is unique to each person. DNA fingerprinting is used for identifying people, studying populations, and forensic investigations.

Historical Uses of DNA Fingerprinting

Jeffreys was first given the opportunity to demonstrate the power of DNA fingerprinting in March of 1985 when he proved a boy was the son of a British citizen and should be allowed to enter the country. In 1986, DNA was first used in forensics. In a village near Jeffreys' home, a teenage girl was assaulted and strangled. No suspect was found, although body fluids were recovered at the crime scene. When another girl was strangled in the same way, a 19-year-old caterer confessed to one murder but not the other. DNA analysis showed that the same person committed both murders, and the caterer had falsely confessed. Blood samples of 4582 village men were taken, and eventually the killer was revealed when he attempted to bribe someone to take the test for him.

The first case to be tried in the United States using DNA fingerprinting evidence was of African-American Tommie Lee Edwards. In November 1987, a judge did not permit population genetics statistics that compared Edwards to a representative population. The judge feared the jury would be overwhelmed by the technical information. The trial ended in a mistrial. Three months later, Andrews was on trial for the assault of another woman. This time the judge did permit the evidence of population genetics statistics. The prosecutor showed that the probability that Edwards' DNA would not match the crime evidence was one in ten billion. Edwards was convicted.

DNA fingerprinting has been used repeatedly to identify human remains. In Cardiff, Wales, skeletal remains of a young woman were found, and a medical artist was able to make a model of the girl's face. She was recognized by a social worker as a local run-away. Comparing the DNA of the femur of the girl with samples from the presumptive parents, Jeffreys declared a match between the identified girl and her parents. In Brazil, Wolfgang Gerhard, who had drowned in a boating accident, was accused of being the notorious Nazi of Auschwitz, Josef Mengele. Disinterring the bones, Jeffreys and his team used DNA fingerprinting to conclude that the man actually was the missing Mengele.

In addition to forensics, DNA has been used to unite families. In 1976, a military junta in a South American country killed over 9000 people, and the orphaned children were given to military couples. After the regime was overthrown in 1983, Las Abuelas (The Grandmothers) determined to bring these children to their biological families. Using DNA fingerprinting, they found the families of over 200 children.

DNA has been used to solve several historical mysteries. On July 16, 1918, the czar of Russia and his family were shot, doused with sulfuric acid, and buried in a mass grave. In 1989, the site of burial was uncovered, and bone fragments of nine skeletons were assembled. DNA fingerprinting experts from all over the world pieced together the puzzle that ended in a proper burial to the Romanov royal family in Saint Petersburg in 1998.

The Mechanics of DNA Fingerprinting

The nucleus of every cell in the human body contains deoxyribonucleic acid or DNA, a biochemical molecule that is made up of nearly three-billion nucleotides. DNA consists of four different nucleotides, adenine (A), thymine (T), guanine (G), and cytosine (C), which are strung together in a sequence that is unique to every individual. The sequence of A, T, G, and C in human DNA can be found in more combinations or variations than there are humans. The technology of DNA fingerprinting is based on the assumption that no two people have the same DNA sequence.

The DNA from a small sample of human tissue can be extracted using biochemical techniques. Then the DNA can be digested using a series of enzymes known as restriction enzymes, or restriction endonucleases. These molecules can be thought of as chemical scissors, which cut the DNA into pieces. Different endonucleases cut DNA at different parts of the nucleotide sequence. For example, the endonuclease called SmaI cuts the sequence of nucleotides CCCGGG between the third cytosine (C) and the first guanine (G).

After being exposed to a group of different restriction enzymes, the digested DNA undergoes gel electrophoresis. In this biochemical analysis technique, test samples of digested DNA are placed in individual lanes on a sheet of an agarose gel that is made from seaweed. A separate lane contains control samples of DNA of known lengths. The loaded gel is then placed in a liquid bath and an electric current is passed through the system. The various fragments of DNA are of different sizes and different electrical charges. The pieces move according to their size and charge with the smaller and more polar ones traveling faster. As a result, the fragments migrate down the gel at different rates.

After a given amount of time, the electrical current in the gel electrophoresis instrumentation is shut off. The gel is removed from the bath and the DNA is blotted onto a

piece of nitrocellulose paper. The DNA is then visualized by the application of radioactive probe that can be picked up on a piece of x-ray film. The result is a film that contains a series of lines showing where the fragments of DNA have migrated. Fragments of the same size in different lanes indicate the DNA has been broken into segments of the same size. This demonstrates a similarity between the sequences under test.

Different enzymes produce different banding patterns and normally several different endonucleases are used in conjunction to produce a high definition banding pattern on the gel. The greater the number of enzymes used in the digestion, the finer the resultant resolution.

In DNA fingerprinting, scientists focus on segments of DNA in which nucleotide sequences vary a great deal from one individual to another. For example, five to ten percent of the DNA molecule contains regions that repeat the same nucleotide sequence many times, although the number of repeats varies from person to person. Jeffreys targeted these long repeats called variable number of tandem repeats (VNTRs) when he first developed DNA fingerprinting. The DNA of each person also has different restriction fragment sizes, called restriction fragment length polymorphisms (RFLPs), which can be used as markers of differences in DNA sequences between people. Today, technicians also use short tandem repeats (STRs) for DNA fingerprinting. STRs are analyzed using polymerase chain reaction or PCR, a technique for mass-producing sequences of DNA. PCR allows scientists to work with degraded DNA.

Use as a forensic tool. DNA fingerprinting is now an important tool in the arsenal of forensic chemists. It is used in forensics to examine DNA samples taken from a crime scene and compare them to those of a suspect. Criminals almost always leave evidence of their identity that contains DNA at the crime scene—hair, blood, semen, or saliva. These materials can be carefully collected from the crime scene and fingerprinted

Although DNA fingerprinting is scientifically sound, the use of DNA fingerprinting in courtrooms remains controversial. There are several objections to its use. Lawyers who misrepresent the results of DNA fingerprints may confuse jurors. DNA fingerprinting relies on the probability that individuals will not produce the same banding pattern on a gel after their DNA has been fingerprinted. Establishing this probability relies on population statistics. Each digested fragment of DNA is given a probability value. The value is determined by a formula relating the combination of sequences occurring in the population. There is concern that not enough is known about the distribution of banding patterns of DNA in the population to express this formula correctly. Concerns also exist regarding the data collection and laboratory procedure associated with DNA fingerprinting procedures. For example, it is possible that cells from a laboratory technician could be inadvertently amplified and run on the gel. However, because each person has a unique DNA sequence and this sequence cannot be altered by surgery or physical manipulation, DNA fingerprinting is an important tool for solving criminal cases.

FURTHER READING:

BOOKS:

Griffiths, A., et al. *Introduction to Genetic Analysis,* 7th ed. New York: W.H. Freeman and Co., 2000.

Jorde, L. B., J. C. Carey, M. J. Bamshad, and R. L. White. *Medical Genetics,* 2nd ed. Mosby-Year Book, Inc., 2000.

Klug, W., and M. Cummings. *Concepts of Genetics,* 6th ed. Upper Saddle River: Prentice Hall, 2000.

Watson, J. D., et al. *Molecular Biology of the Gene,* 4th ed. Menlo Park, CA: The Benjamin/Cummings Publishing Company, Inc., 1987.

ELECTRONIC:

The University of Washington. "Basics of DNA fingerprinting." <http://www.biology.washington.edu/fingerprint/dnaintro.html,>(March 4, 2003).

SEE ALSO

DNA Recognition Instruments
DNA Sequences, Unique
Fingerprint Analysis
Genomics
Retina and Iris Scans

DNA Recognition Instruments

AGNIESZKA LICHANSKA

DNA recognition instruments allow rapid identification of the origin of DNA in an environmental or medical sample. Recognition of the source of DNA is important in pathogen (disease-causing agent) identification in public health surveillance, and diagnostic and military applications.

DNA recognition instruments utilize two main methods for DNA detection and identification, nucleic acid hybridization r polymerase chain reaction (PCR). Hybridization of nucleic acids allows differentiation of sequences that differ by as little as one base pair by using high temperature washes that remove partially matched DNA strands. Hybridization relies on the fact that single stranded DNA reforms a double stranded helix with a complementary strand. The method requires a single stranded target (unlabeled) and probe (labeled with a radioactive or fluorescent tag to detect signal). PCR-based detection in modern instruments is based on specificity provided by primers required for DNA amplification and fluorescent probes to detect the product in real time.

A technician places a gene chip into one of the photo lithography machines shown at a production facility in California. Gene chips are dime-sized pieces of glass infused with DNA fragments that allow researchers to study how and why genes react to various stimuli. AP/WIDE WORLD PHOTOS.

New technologies for DNA recognition. The standard methods used in diagnostics are not rapid enough for the immediate identification of pathogens in a case of a biological attack either on military personnel or civilians. Engineers and biologists, therefore, are designing new technologies to make DNA recognition rapid, robust, with increased sensitivity of the assays and improved identification of positive samples. Optical identification methods are primarily used in PCR-based instruments; however, new magnetic and electrochemical methods were developed for hybridization-based assays.

Hybridization-based technologies. Chip-based hybridization assays, where the target DNA is spotted onto a glass or plastic slide and a single stranded DNA probe is used to detect it, were developed recently by a number of companies. Technology allows placement of thousands of DNA molecules on the slide, but detection of the specific reaction is often lacking sensitivity. As a result, a number of research teams and commercial companies are researching better ways to identify a positive signal.

One breakthrough came with the implementation of electrical conductivity as a detection method. This method relies on the use of electrodes with gaps of 30–50nm in size, containing single stranded DNA molecules (oligonucleotides) immobilized on their surface (capture probes) and gold oligonucleotide nanoparticles allowing detection of electrical currents resulting from hybridization. Both oligonucleotides bind to the target sequence when the electrode is immersed in a solution containing target molecules. A modification of this method is the use of signal amplification by using a photographic solution as developed by a Northwestern University team. A salt wash before the addition of photographic developer removes mismatches and the silver coated gold particles can be easily visualized. The chip is then scanned using a flatbed scanner, removing the need for expensive equipment. This method is highly sensitive and very fast. It is able to detect concentrations of DNA (100 times more sensitive than conventional detection methods), in one to three minutes.

A modification of this method was developed in 2002 and incorporates nanoparticle probes that in addition to gold particles, have Raman dye-label (for example Cy3, Cy5, or Texas Red). Detection of these probes can be either by Raman spectroscopy or by using a flatbed scanner to detect silver enhancement. By using multiple labels one is able to design chips detecting multiple target sequences (multiple pathogens).

Hybridization-based instruments. The great advantage of hybridization-based instruments is the fact that they do not require any DNA amplification, are highly sensitive and give rapid results.

Scientists in industry are currently producing instruments that are based on measuring electrical conductivity. One is known as the eSensor. The system consists of bioelectronic chips, reader, and special software. The chips contain capture probes and signaling probes. After an interaction with a target sequence, signaling probes induce electric current, which is detected and interpreted by the sensor's software. This instrument can perform a number of assays simultaneously. A second instrument is directly based on the technology from the Northwestern University group, using a method of conductivity detection that was modified to amplify the signal from gold particles by using a photographic developer solution to coat the gold particles. Although this instrument currently requires a large space, work is underway to design a hand-held device.

One company has licensed a Strand Displacement Amplification (SDA) method, and has devised an electrical method of binding DNA to silicon chips and performing hybridization. SDA oligonucleotides (probes) are localized to spots on the chip by charge and immobilized on the surface by chemical reaction. The sample is then added to the chip and by applying an electric current, the binding of test to the probes is highly accelerated (one to three minutes). By reversing the charge, unbound molecules are removed and only perfect matches remain. The entire process takes about 15 minutes. Chips for identifying pathogens such as the bacteria responsible for anthrax are under development.

PCR-based instruments. The newest technologies in polymerase chain reaction (PCR)-based instruments involve instrument miniaturization and methods for handling and detecting multiple pathogens in multiple samples. The ability to prepare clean PCR templates in a field is often difficult or limited. However, the presence of various chemicals can inhibit the amplification, giving false negative results and, in the case of an attempt to identify a biological threat, possibly endanger people's lives. As a result, a number of companies have started to offer sample preparation units with their PCR instruments.

The advanced nucleic acid analyzer (ANAA), developed in 1997, was the first DNA recognition instrument designed for work in the field. It was portable, but still large and was superseded by a hand-held ANAA (HANAA).

The major differences between the various instruments are in the proprietary heating and cooling systems, detection optics, and sample preparation and handling, as well as size. Speed of most of these instruments is similar with the typical sample analysis taking 7–20 minutes.

A different technology, but still PCR-based, uses a high-performance liquid chromatography to separate the PCR products and identify mutations. The advantage of the system is that it can detect mutations in any genes that could have been altered for designing biological weapons, thus, potentially complementing any other detection methods.

Application of DNA recognition instruments. DNA recognition instruments are likely to be used in general monitoring of the environment, investigation of suspicious objects, and in diagnostics. In all of these applications, detection must be rapid and accurate in order to introduce prevention measures or rapid treatment. Ease of use and result interpretation are important, as in majority of cases, users will be people with minimal laboratory training.

As of 2003, the majority of these advanced DNA recognition instruments were or are undergoing final testing in the field. They are able to cope with samples of water, food, and various clinical samples to detect an environmental contamination or identify a pathogen causing unusual symptoms in humans or domestic animals.

FURTHER READING:

PERIODICALS:

Belgrader, P., W. Bennet, D. Hadley, et al."PCR Detection of Bacteria in Seven Minutes." *Science* no. 5413: 449–450.

Cao, Y. W. C., R. Jin, C. A. Mirkin. " Nanoparticles with Raman Spectroscopic Fingerprints for DNA and RNA detection." *Science* no. 5586 (2002): 1536–1540.

Park, S. J, T. A. Taton, and C. A. Mirkin. "Array-Based Electrical Detection of DNA with Nanoparticle Probes." *Science* no. 5559 (2002): 1503–1506.

SEE ALSO

Biosensor Technologies
Bioterrorism, Protective Measures
DNA Sequences, Unique

DNA Sequences, Unique

AGNIESZKA LICHANSKA

Deoxyribonucleic acid (DNA) contains genetic information of an organism that is unique for each organism. The entire cellular DNA of any organism, bacteria, plant or animal is known as its genome, as is the entire genetic material of a virus. A DNA sequence is considered to be unique if it is present in only one copy in a haploid genome. A haploid genome contains only a single copy of each chromosome. In humans, for example, a haploid number of chromosomes is 23. However, not all of the DNA contained in the genome is considered as unique; there are also various repetitive sequences present.

DNA and Genome Structure

A DNA strand is composed of a strand of nucleotides (nitrogen-based building blocks of DNA and RNA). Each nucleotide contains a phosphate attached to a sugar molecule (deoxiribose) and one of four bases, guanine (G), cytosine (C), adenine (A) or thymine (T). It is the arrangement of the bases in a sequence, for example ATTGCCAT, that determines the encoded gene. This sequence allows scientists to identify organisms, genes, or fragments of genes. One of the main characteristics of DNA is the fact that it forms double stranded molecules (helices) by forming hydrogen bonds between the complementary strands inside the helix and a sugar-phosphate backbone outside. This pairing is not random, A always pairs with T, and C pairs with G; therefore, a sequence complementary to ATTCCGAT will be TAAGGCTA.

Genes are the sequences of encoded proteins, and together with the surrounding regulatory sequences are, considered as unique genomic sequences, because they are present as single copies in a haploid genome. In contrast, some sequences are present in multiple copies and are known as repetitive fragments. The simplest genomes of viruses and bacteria contain mostly unique sequences with only a few repetitive regions. However, the proportion of repetitive DNA increases in higher organisms, for example sea urchins have only 38% unique sequences and human just over 50%.

The genes encoding the same protein in bacteria, plants, and humans show some similarity as the majority of the encoded proteins perform the same or similar function across the species. Such homology between the sequences allows scientists to identify the genes in humans by using fragments of mouse or yeast genes to search for similar DNA fragments. Although most of the genes show some species-dependent differences, not all of them can be used to discriminate between organisms. Only a few genes can be used for this purpose. The two main groups are ribosomal (16S in bacteria and 18S in animals) and mitochondrial genes.

Ribosomal genes are useful for tracing evolution and relationships, especially in bacteria. However, mitochondrial genes have an advantage over the ribosomal genes as they are not encoded by the nuclear DNA, but are present as circular molecules in the cells. As such they are less likely to be degraded with time; therefore bones, teeth, or tissue fragments can be identified even after a long time.

Exploiting Unique DNA Sequences

The presence of unique DNA sequences allows scientists to identify signature sequences that can be later used as probes to detect individual organisms or to detect a particular gene. Changes of even one base pair can be readily detected by most hybridization techniques and by sequencing. Signature sequences are particularly important for diagnosis of viruses, which are the pathogens that lack ribosomal or mitochondrial genes. Their detection and identification is greatly simplified by using these sequences, as traditional methods can take up to a few weeks.

The unique DNA sequences can also be used to design primers (short DNA fragments needed to initiate DNA amplification) for polymerase chain reaction (PCR). There is adequate difference between all the genes within one organism, as well as between organisms from different species, to ensure that the selected primers will only amplify the target sequence even if a mixture of different DNA molecules is present. This allows scientists to design diagnostic and identification tests for the common pathogens and diseases and for parts of the pathogen's genome.

Identification of people. Although every person has unique DNA (except for the identical twins), identification of people is not based on the sequencing of someone's genome. Instead, analysis of mitochondrial DNA in a region of a displacement-loop (D-loop or control region) or of short tandem repeats (STRs) is used for identification purposes. D-loop analysis is used for individual identification in forensic analysis. This is possible due to the polymorphisms of such sequences resulting from substitutions of base pairs during DNA replication process (for example, instead of A, DNA polymerase incorporates T) .

The D-loop region is 1274 base pairs long and is located between the genes encoding transfer RNA (tRNA) for proline and tRNA for phenylalanine and contains the regulatory regions of the for replication other genes.

The main method used for the identification of the changes in this region is PCR amplification and sequencing. However, new microarray approaches are under development.

Encoding secret messages. DNA sequences offer a unique method of encrypting messages or concealing information. A DNA sequence encoding a message is flanked on the sites by primers that will be later used to amplify if by PCR and sequence. An encryption code is selected by a group that is using the system; for example, each letter and number might be assigned three base pairs. The DNA strand with a message is prepared and mixed with human genomic DNA fractionated to the same size as the message. To further conceal the DNA from an enemy, DNA from another species can be added. An intended recipient of the message can decode it by PCR amplification and sequencing. Sending such as message is as simple as writing a letter and enclosing the DNA coded message as a microdot. Once the DNA mix is prepared, it is spotted over a dot on paper from which the microdots are cut out and attached to the full stops in the letter. If such a letter falls

into the wrong hands finding a message will be extremely difficult, as it will be buried among millions of others, and reading it without the primer sequences and encryption code will be impossible.

DNA encrypted messages can be used for safekeeping important information, but also to pass on espionage information. Although the method is simple, it requires molecular biology equipment to decode and can be too troublesome for everyday use.

Use of Unique DNA Sequences

Unique DNA sequences are already used as security tools. The ability to synthetically create DNA molecules allows the generation not only of spy messages, but more importantly, unique signatures that would protect consumers from product fakes. Similar methods were used at the Sydney Olympic Games in 2000 to mark all of the official merchandise. In this case, an invisible ink mixed with DNA obtained from one of the athletes was used. Protection is not limited to manufacturers. Unique DNA sequences are also used by artists such as Thomas Kinkade and cartoon creator Joseph Barbera, who protect their artwork by DNA signatures.

The major use of unique DNA sequences for security, however, is in the area of environmental surveillance and identification of agents of biological warfare. The sequences used for these purposes are often kept secret. Most of the producers of DNA recognition instruments use such sequences to design their products.

Finally, forensic science relies in many cases on the use of unique sequences for identification of biological traces and individual identification.

■ FURTHER READING:

BOOKS:

Strachan, Tom, and Andrew P. Read. *Human Molecular Genetics,* 2nd ed. Oxford: BIOS Scientific Publishers, 1999.

Hartl, Daniel L. *Genetics.* Boston: Jones and Bartlett, 1994.

PERIODICALS:

Clelland, C. T., V. Risca, and C. Bancroft. "Hiding Messages in DNA Microdots." *Nature* no. 6736 (1999): 533–534.

ELECTRONIC:

Wired News. "DNA Tagging." Stewart Taggart. <http://www.wired com/news/print/0,1294,34774,00.html> (15 January 2003).

SEE ALSO

DNA Fingerprinting
DNA Recognition Instruments
Polymerase Chain Reaction (PCR)

DNA Technology.

SEE *Genetic Technology.*

Document Destruction

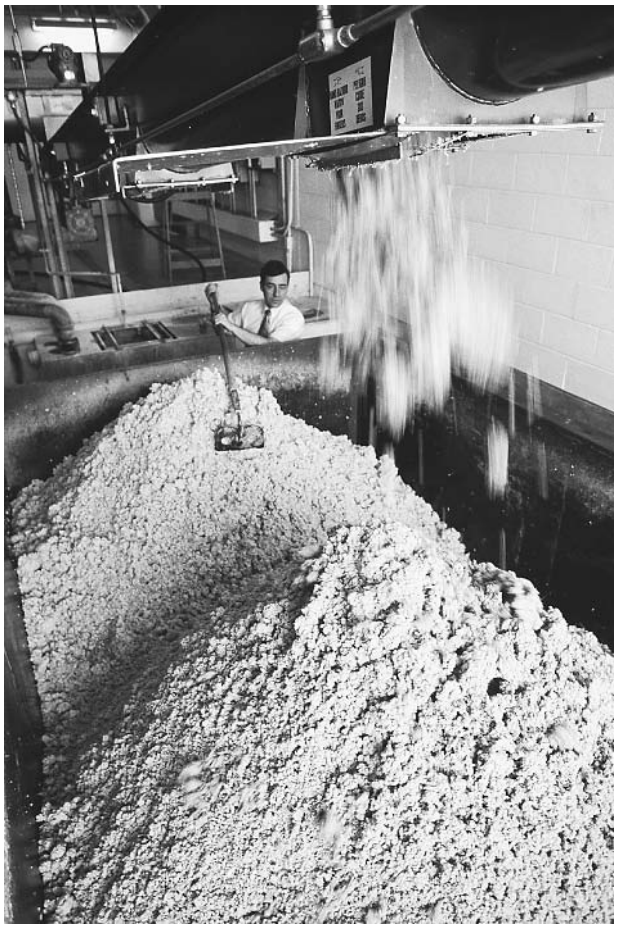
■ JUDSON KNIGHT

Modern society that has become so accustomed to the digitization of data may forget just how much information remains available in physical format. Even documents stored on a computer may circulate as hard copy, and these, combined with other paper items such as phone messages, notes, memoranda, and other items provide an opportunity for the theft of useful information. Businesses targeted for economic espionage are particularly vulnerable, as are individuals, either due to their own carelessness or that of companies charged with maintaining sensitive records. For that reason, businesses have increasingly turned to document destruction, a security solution long applied by government agencies. Document destruction can be achieved with shredders, burn boxes, and other forms of technology, often in industrial facilities dedicated to that purpose.

Stories of document destruction by businesses and public officials regularly appear in the media. In 2002, as a scandal erupted around Enron Corporation for falsifying records of earnings, it was revealed that Arthur Andersen LLP, the accounting firm that had helped Enron falsify its books, had shredded literally tons of documents.

Other businesses employ document destruction for much more legitimate reasons, such as protection against economic espionage. But not only businesses need to destroy documents; so do individuals. According to the United States Postal Service, half a million people each year become victims of identity theft, which occurs when a criminal steals financial information from someone, then poses as that person in order to siphon off funds. One of the most significant avenues of vulnerability in this area is the household trash. A person may receive an unsolicited credit card offer and, dismissing it as junk mail, throw it away. Once garbage is placed on the curb for pickup, it is easy for a thief to pick through it, remove the credit card offer, fill it out, send it in, and obtain a "free" card—all courtesy of an innocent consumer who failed to take appropriate precautionary measures.

In the 1990s, these garbage-combing thieves earned the colorful appellation of "dumpster diver". Private detectives, for purposes either laudatory or malign, also obtain a great deal of their information from trash. (So, too, do law-enforcement officers, who take advantage of the fact that material an individual has discarded is open to search without a warrant.) Yet not every aspect of



SOMAT (soluble materials), or shredded documents, are loaded into disposal bins at C.I.A. headquarters in Virginia. ©ROGER RESSMEYER/CORBIS.

individual vulnerability to identity theft or invasion of privacy involves those intent on misusing individuals' private records.

Forms of Document Destruction

The best methods of document destruction take place on an industrial scale. The document destruction industry, which primarily serves corporate clients, is estimated to generate $1.5 billion a year in revenue. Whereas only about two dozen companies nationwide were in operation in the early 1980s, by 2002 that number had risen to about 600.

Document shredding, which particularly came to national attention in the wake of the Enron debacle, is only one of many methods of document destruction, though it is the one most frequently used. As a report in the *Wall Street Journal* noted, "For routine destruction work, many companies use shredding services because even heavy-duty office-model shredders tend to choke on anything thicker than about 50 pages—and can be stopped dead in their tracks by a binder clip."

Industrial shredders. By contrast, the shredders at a facility such as that of American Document Security Corporation (ADS) in Brooklyn, New York, are capable of chewing through 20 tons (18.14 tonnes) of documents an hour. Clients of such companies range from law and consulting firms to investment banks, hospitals, and many others.

Though document shredding is probably as old as the concept of written documents, shredding by machine dates back to the 1920s, when an American inventor developed the first shredder from a Bavarian noodle cutter. Today's shredders are far more efficient than those used even in 1979, when the students who took over the U.S. embassy in Teheran, Iran, were able to piece together documents shredded by embassy personnel.

Some shredders are known as disintegrators. Often used for destroying CD ROMs, circuit boards, and other items containing computerized data, these chop up materials into a fine dust that can be sifted through a screen at the bottom of the machine. Another variation on the shredder, inasmuch as it destroys documents by purely physical (rather than chemical or electromagnetic) means, is a hammer-and-mill device, which beats paper quite literally to a pulp.

Burning and other methods. Paper that has been put through industrial shredders and hammer-and-mill devices often is recycled. Waste-to-energy plants burn paper waste at temperatures as high as 2,200° F (1,204 °C).

For burning documents on a smaller scale—especially documents for which security is an extremely high concern—a burn box may be used. Actually, the purpose of the burn box is not to destroy documents per se, but to destroy documents discovered by the wrong people. Inside the box, a sturdy metal container, is a volatile chemical mixture attached to a tamper-sensitive switch. If someone opens the box in an unauthorized manner, the chemicals turn the pages to ash.

A focus on security. An intriguing variety of document destruction can be used for electronic media such as CD-ROMs, hard drives, floppies, and so on. This is a degausser, which applies electromagnetic energy to rearrange particles of information. Used either in the form of a stationary box or a hand-held wand, a degausser removes information permanently, leaving the storage device free to be used again.

No matter how advanced the technology, however, it is only as reliable as the individual who operates it. For this reason, security concerns are as much a motivator to document-destruction companies as they are to the firms who hire them. ADS, for instance, equips its trucks with alarms, and tracks them on a global positioning system to ensure that documents are not stolen en route. Its employees are bonded, and must undergo background checks prior to employment. Some 30 security cameras are in

operation at the Brooklyn facility. Similarly, at the trash-to-energy facility in Utah, a closed circuit television system, along with security guards, provides surveillance during the unloading and burning process.

FURTHER READING:

PERIODICALS:

Brown, Ken. "When Enron Auditors Were on a Tear." *Wall Street Journal.* (March 21, 2002): C1.

Choi, Audrey. "VW Discloses GM Documents Were Destroyed—German Car Maker Denies Involvement, But Rival Still Claims Espionage." *Wall Street Journal.* (August 9, 1993): A3.

"Document Destruction." *Government Executive* 30, no. 8 (August 1998): 58.

Eichenwald, Kurt. "Andersen Charged with Obstruction in Enron Inquiry." *New York Times.* (March 15, 2002): A1.

Kirch, John F. "Document Destruction." *Security Management* 42, no. 8 (August 1998): 22–23.

Orey, Michael. "Why We Now Need a National Association for Data Destruction." *Wall Street Journal.* (January 30, 2002): A1.

Rowh, Mark. "Shredders: The Cutting Edge." *Office Solutions* 19, no. 8 (September/October 2002): 42–44.

ELECTRONIC:

National Association for Information Destruction. <http://www.naidonline.org> (March 30, 2003).

Trujillo, Al. "Avoid Risk with Secure Document Destruction." Electronic and Hardcopy Document Processing Technology. December 2002. <http://www.dptmag.com/editorial2.asp?ID=97> (March 30, 2003).

SEE ALSO

Computer and Electronic Data, Destruction
Economic Espionage
Privacy: Legal and Ethical Issues

Document Forgery

MARTIN J. MANNING

The use of forgeries to deceive an enemy or affect public opinion has been a staple of disinformation throughout modern history. Forgeries can be more easily exposed than other types of active deception measures largely because careful analysis can often demonstrate convincingly that the documents are fraudulent. Still, forgery is effective in at least three ways. First, a forgery can cast aspirations on targeted governments and on individuals (silent forgery). This can be the most damaging forgery, as the victim does not know that the forgery is being circulated and may never get the opportunity to refute it. Second, forgeries, when publicized, force the target government to spend time, effort, and funds on refutation. Third, denial never entirely offsets the damage done as doubt can be cast by repeated reference to the forgery and to its contents.

Cadore letter. On August 5, 1810, Jean, Duc de Cadore, a French foreign minister, delivered a diplomatic note to the United States minister John Armstrong. In it, Napoleon I promised to revoke the Berlin and Milan Decrees in November, 1810, if the British Orders-in-Council were repealed, or if the United States reinstated sanctions against Great Britain. The latter happened and non-intercourse against the British resumed on February 28, 1811. The Cadore letter turned out to be a forgery. American ships continued to be sized and President James Madison refused to change his decision with regard to the British embargo.

De Lome letter. Written by the Spanish minister to the U.S., Enrique de Lome, to a friend in Havana, the letter was published in William Randolph Hearst's *New York Journal* in February, 1898. It characterized President William McKinley as "weak and a bidder for the admiration of the crowd" and questioned McKinley's political integrity. This private letter was stolen by a Cuban rebel sympathizer from the Havana mail system and returned to New York. The publication of the letter uncovered the false promise of Spain's foreign policy towards the U.S. In its wake, De Lome immediately resigned, Spain sent an insincere apology, and McKinley let the incident pass, although it ignited American opinion toward future Cuban intervention.

"Protocols of the Learned Elders of Zion." No country, however, has used forgeries as extensively as the Soviet Union, developing forgeries to a level unparalleled in previous times. For the Soviets, forgeries were a weapon of active measures (i.e., influence operations) that supported propaganda themes. The KGB had the responsibility for carrying out active measures and producing forgeries. Describing the role of the KGB in influencing attitudes in the West, Yuri Andropov, then head of KGB, said in 1967, "The state security bodies are also actively participating in the fulfillment of this task. The workers of these bodies are aware that peaceful coexistence is a form of class struggle; that it is a bitter and stubborn battle on all fronts, economic, political, and ideological. In this fight, the state security bodies are obliged to carry out their specific duties efficiently and faultlessly." These Soviet state security bodies built upon the activities of the czarist secret police (Okhrana,) who produced one of history's classic forgeries.

Among the most widely circulated propaganda tracts and the centerpiece of anti-Semitic literature, the infamous "Protocols of the Learned Elders of Zion" appeared shortly before the 1905 uprising against the Czar Nicholas II of Russia. It was authorized by Pyotr Ivanovich Ratchkovski, the head of the Okhrana, who circulated it, although authorship is now given to Mathieu Golovinski. The forgery derived from a French political pamphlet,

Forged passport with picture of himself in disguise enabled Lenin to escape to Finland in the fall of 1917. Warrant for his arrest had been issued in July of that same year.

This false passport and disguise enabled Lenin to escape into Finland after an order for his arrest was issued by the Russian Provisional Government in July 1917. ©HULTON-DEUTSCH COLLECTION/CORBIS.

"Dialoque aux Enfers entre Montesquieu et Machiavel," by Maurice Joly, which was first published in 1864 as an attack on Napoleon III's ambitions for world domination. In the "Protocols," "the Jewish," or "the Jews," were substituted where the French emperor was mentioned in the text.

The Okhrana, was responsible for the "Protocols," a forgery that cost untold number of lives since it was first introduced. The Nazis used this forgery as a justification for genocide against Jewish persons, and even today anti-Semitic groups continue to reprint it.

German-Bolshevik conspiracy. Drawing on the experience of their Czarist predecessors, the Soviet KGB (known earlier as the Cheka, OGPU and GPU) continued to use forgeries. Six months after seizing power, the Bolsheviks were concerned about continuing accusations labeling Lenin and his comrades as German agents. There was some logic to this accusation, as the Germans had helped send Lenin back into Russia to undermine their wartime enemy. The Bolsheviks denied that they were in the pay of the Germans. On September 15, 1918, the United States government released to the press a collection of documents that

purported to show that the Bolsheviks had received money both before and after the Russian Revolution. In October, 1918, the Committee on Public Information (CPI), the World War I predecessor of USIA, released a pamphlet to the press entitled "The German-Bolshevik Conspiracy" which contained translations of 68 documents and reproductions of many of them. In addition, the pamphlet contained an analysis of the documents prepared for the National Board for Historical Service by two distinguished scholars. The report concluded that most of the documents were genuine, although some were questioned. The documents had been obtained in Russia by Edgar Sisson, the CPI representative, and came to be known as the "Sisson documents."

The release of the Sisson documents was reported in the American press on September 16, 1918, but, on September 21, the *New York Evening Post* challenged their authenticity, citing as their source Santeri Nuorteva, who was described by them as "head of the Finnish Information Bureau in New York," a notorious Soviet propapagandist who had been a representative of the short-lived Communist government established in Finland by the Red Army. Nuorteva revealed that the first American to see the documents was Col. Raymond Robins, the Red Cross administrator in Russia who was later identified as a Bolshevik sympathizer.

The controversial Sisson documents are consistent with documents proving German financing of the Bolsheviks that were found in the German Foreign Office after World War II. The possibility exists that the Bolsheviks created a set of forgeries which were then mixed with authentic documents, and passed to the American government by Robins for the purpose of discrediting the thesis that Lenin and company were on the German payroll. In fact, the exposure of the Sisson documents created an atmosphere in which any allegation of German financial support to the Bolshevik was treated with distrust. It was only decades later that the German Foreign Office documents became available and proved the point.

Zinoviev letter. On October 25, 1924, the British Foreign Office released to the press the text of an alleged document of the Communist International ordering the British Communist Party to carry out activities against the Labour government and to organize cells in the army. The document signed with the name of the head of the Communist International, Grigory Zinoviev, is credited with bringing down the British Labour government, which was perceived as being too soft on the Soviet Union.

The Soviet government and Zinoviev denied the authenticity of the letter. However, it was quite consistent with instructions given to the British and other Communist parties by the Fifth World Congress of the Communist International held in Moscow in the summer of 1924. The instructions had been printed in the September 5, 1924 issue of the official Comintern publication, *International Press Correspondence,* published in German and English in Vienna.

Tanaka memorandum. In 1929, a different form of Soviet forgery appeared when a document, purporting to be a memorandum from the Japanese Prime Minister Tanaka to the Emperor Hirohito, found its way into the Western press. This document laid out a Japanese plan for world conquest. According to the introduction to a 1941 publication of the document by the American Communist Party, "The Tanaka Memorial…was written in 1927 as a confidential document. It first came to light in 1929 after it had been purchased from a Japanese by Chang Hsuehliang, then the Young Marshal of Manchuria," a warlord who frequently collaborated with the Chinese Communists. In late 1936, he kidnapped Chiang Kai-shek and demanded that he cooperate with the Communists in the war against Japan.

The Tanaka document was clearly a forgery. It contained errors of fact about Japan and even about Baron Tanaka, but it was widely circulated until the end of World War II. An insight into its Soviet origin was provided in 1941 by Leon Trotsky, who argued that it was authentic. According to an article by Trotsky, written shortly before his death, Felix Dzerzhinsky, the head of Cheka, secured the document in 1925 through a spy in the Japanese Ministry of Foreign Affairs. The document was photographed and then translated for Trotsky. Trotsky did not explain how the Soviets came into possession in 1925 of a document not written until 1927, the year Tanaka became prime minister. It is possible that the Soviets created the forgery based on an authentic document stolen in 1925.

Trotsky revealed that the document was put into circulation in the United States through Amtorg, the Soviet trading corporation, headed by man named Bogdanov. Since Bogdanov did not arrive in the United States until 1930, Trotsky's knowledge of the method of surfacing could only have come through his contacts in the GPU, which he maintained after being ousted from the Soviet leadership. This date would be consistent with the forgery's original surfacing in China in 1929 and its replay in the United States in 1930.

The most recent replay of the Tanaka forgery was a reference to it in a Kuwaiti newspaper in January, 1987. The unsigned article, in Arabic, which showed substantial evidence of Soviet authorship, accused the United States of developing an "ethnic weapon," a biological weapon that would supposedly affect only black or brown skinned people. This bizarre allegation has been repeated in both official Soviet media and in publications influenced by the Soviets for years. The article was also accompanied by a purported picture of the "ethnic weapon" being fired and carried the caption, "The germ bomb is fired from regular tanks looking like regular bombs and spreading the germs." The opening paragraphs of the article accused the United States of taking over biological weapons research from

the Japanese, who were supposedly carrying out the plans revealed by Tanaka in his letter to the Emperor.

Whalen documents. In 1930, the U.S. Congress was planning to establish a committee to investigate Communist propaganda. Shortly before it was formed, the New York City police department received copies of a set of documents purporting to be letters from the Communist International instructing Amtorg to carry out Communist propaganda in the United States. Amtorg actually was deeply involved in Soviet espionage in the United States. The documents were released to the press on May 2, 1930, and appeared in print the next day. They were released by police Commissioner Grover Whalen and came to be known as the "Whalen documents."

An examination of the documents revealed that they were forgeries. For example, the letterhead read "Ispolkom Kominterna" (Excom Comintern). An authentic document would have spelled out "Communist International," rather than using the nickname Comintern. The forgeries were exposed by journalist John L. Spivak, who provided the evidence to Congressman LaGuardia and wrote about the case in the *New York Evening Graphic.*

Spivak claimed that his editor gave him the assignment to trace the documents on May 3. After investigating type foundries and print shops, he said he discovered the identity of the printer of the letterheads on May 8. It took him four days to trace the printing. Spivak's story does not stand up to investigation. When the printer testified before a congressional committee, he revealed that he recognized the letterhead when he saw it reprinted on the front page of the Yiddish language daily newspaper, *The Jewish Daily Forward.* The same day, Spivak came into his store and accused him of being the printer of the letterheads. The printer Max Wagner, signed an affidavit for Spivak acknowledging that he had the printed the letterheads. The statement, read into the *Congressional Record* by Congressman Fiorello LaGuardia, states, "I printed this about four months ago and submitted two copies as a proof, but the man did not come back for the order, Signed, M. Wagner, printer."

The photostat of the letterheads appeared on the front page of *The Jewish Daily Forward* (May 3, 1930), the date that Spivak began his investigation, not four days later. It is clear that Spivak knew the printer's identity as soon as he began his investigation.

The Communist Party newspaper, *Daily Worker* (May 13, 1930) reproduced a photostat of the Wagner affidavit with a slightly different text leaving out the word "printer" and inserting the words "May 8, 1930." This appears to have been concocted to authenticate Spivak's claim that he confronted Wagner on May 8th rather than on May 3, when the incident actually took place.

In 1945, Elizabeth Bentley revealed to the FBI that she had worked as courier for a Soviet spy ring and she identified Spivak as a member of the ring. The Communists used the forgeries to discredit the congressional committee established to investigate Communist propaganda. The committee, headed by Congressman Hamilton Fish of New York, never authenticated the Whalen documents. However, Earl Browder, then head of the Communist Party U.S.A., reported to a meeting of the Executive Committee of the Communist International held in Moscow in April, 1931, that, "the notorious forged 'Whalen Documents,' produced by the Czarist 'General' Djamgaroff, became the occasion for the U.S. Congress to set up the Fish Committee to investigate Communist activities in the U.S. Behind the actions of this committee, which were the most vulgar farce considered in themselves, was the sinister and serious purpose of preparing 'public opinion' for the war of intervention against the U.S.S.R." Badacht was later revealed, by Whittaker Chambers, as the man who recruited him as a Soviet spy. Bedacht was the contact between the leadership of the American Communist Party and the Soviet intelligence service.

Other events. Since World War II, the Soviet Union continued to release forgeries that it expected would damage U.S. relations with its allies. Several were important campaigns. One was designated the Eisenhower-Rockefeller Letter, an extensive forgery presented as a private "letter" from Nelson A. Rockefeller to President Dwight D. Eisenhower in which Rockefeller was portrayed as the advocate of a "bolder program of aid to under-developed countries," as a cover for what the East Germany press called "supercolonialism" ("superkolonialismus"). Its aim was to discredit the U.S. commitment to the removal of the old colonial powers from their involvements in Africa and in Asia.

The document first appeared on February 15, 1957, in the East German daily, *Neues Deutschland,* and circulated throughout the world during what was termed the "Camp David" period of East-West cordiality (1959–1960); it later appeared on Radio Moscow, in *Pravda* (Soviet party newspaper), on Radio Hanoi, on Radio Beijing, in the Czechoslovak domestic press, and in the official news agency of the People's Republic of China.

In 1961, Richard Helms, assistant director of the Central Intelligence Agency, testified before the U.S. Senate. He said, "Long before 1957, the Communists were as skillful as the Nazis in the production and exploitation of forgeries. But in that year, they first began to aim them frequently against American targets, to turn them out in volume, and to exploit them through a wide-flung international network. Then CIA put these fakes under the microscope. We found that each Soviet forgery is manufactured and spread according to a plan. Each is devised and timed to mesh with other techniques of psychological warfare in support of Soviet strategy." During this period, more than 32 forged documents were found.

In a 1980 report to the U.S. Congress, the CIA revealed that "the KGB provides a non-attributable adjunct to the overt Soviet propaganda network. Service A of the KGB's

Foreign Intelligence Directorate plans, coordinates and supports operations which are designed to backstop overt Soviet propaganda using such devices of covert actions as forgeries, planted press articles, planted rumors, and controlled information media. In particular, the number of Soviet forgeries has increased dramatically in recent years. In the early 1970s, this section of the KGB was upgraded from "department" to "service" status—an indication of its increased importance. Service A maintains liaison with its counterparts in the Cuban and the East European services and coordinates its overall program with theirs."

The "U.S. Army Field Manual, FM 30–31B," also known as "Stability Operations-Intelligence," was the most ubiquitous forgery of recent years. In September, 1976, a photocopy of this forgery appeared on the bulletin board of the Philippine Embassy in Thailand, together with a letter addressed to Philippine President Marcos. The forgery said that the United States planned to use leftist terrorist groups in Western countries to promote U.S. objectives. It reappeared in 1978 in two Spanish publications where it had been planted by a Spanish Communist and a Cuban intelligence officer. The next year, copies of a Portuguese language translation were circulated by the Soviets among military officers in Lisbon.

The forged field manual had worldwide distribution in the late 1970s. In January, 1979, *Covert Action Information Bulletin,* published in the United States by CIA defector Philip Agee, reproduced the forgery as if it were an authentic document. While the original forgery was a typescript, the magazine reset it in font that gave the impression that it was a printed document.

In 1983, the Soviets began to replay the story. In the new version, the manual had been discovered in the possession of the Italian Masonic organization P2, which was involved in an important scandal at the time. This was an attempt both to link the United States government to the scandal and to authenticate the forgery.

Presidential review memorandum on Africa. On September 17, 1980, White House press spokesman Jody Powell announced that an unidentified group had sought to sow racial discord by circulating a forged presidential review memorandum on Africa that suggested a racist policy on the part of the United States. The first surfacing on the forgery appears to have been in the San Francisco newspaper, *Sun Reporter* (September 18, 1980). The *Sun Reporter*'s political editor, Edith Austin, claims in that issue of the paper to have received the document from an "African official on her recent visit on the continent." The forgery was replayed by the Soviet news agency TASS on September 18, 1980, and distributed worldwide.

Kirkpatrick speech. Former United States ambassador to the United Nations Jeanne Kirkpatrick has been the target of more than one Soviet forgery. On February 6, 1983, the pro- Soviet Indian weekly, *Link* published the text of a supposed speech by U.N. Ambassador Kirkpatrick outlining a plan for the Balkanization of India. The speech was never given, but this forgery has been replayed many times by Soviet-controlled propaganda outlets. Its most recent appearance was in the book, *Devil and His Dart,* published in 1986. The author, Kunhanandan Nair, was the European correspondent of *Blitz,* another pro-Soviet publication.

On November 5, 1982, the British magazine, *New Statesman* published a photostat of a letter supposedly from a South African official to Kirkpatrick. He was allegedly sending her a birthday gift. The U.S. Mission to the U.N. wrote the magazine on November 19, branding the letter a forgery. *New Statesman* countered this by printing another photostat of the forgery with entirely different spacing between the lines. The magazine claimed that the letter was authentic and that they had received it from a source in the U.S. Department of State. A comparison of this forgery with a letter sent by the South Africa official to a number of U.S. journalists announcing his appointment as information counselor at the embassy revealed that this letter was the exemplar. The real letter had been typed on a computer. The forgery based on it was typed on a typewriter and contained a number of misspellings.

Los Angeles Olympics forgery. In the summer of 1984, two bizarre leaflets were mailed to African and Asian participants in the Los Angeles Olympics, which were boycotted by the Soviets. Signed by the Klu Klux Klan, they threatened the lives of these athletes. These leaflets later proved to be Soviet forgeries, written in poor English. When the U.S. government exposed them and pointed out that there is no organization in the United States called simply the Klu Klux Klan (the organizations bear individual names like White Knights of the Klu Klux Klan or Invisible Empire of the Klu Klux Klan), TASS, the Soviet official news agency, responded on July 12, 1984, by claiming that the leaflets were signed "the Invisible Empire, The Knights of the Klu Klux Klan." TASS attempted unsuccessfully to correct the error on the leaflets made by the KGB. The forgeries were intended to preoccupy African-American and Asian-American athletes with intimidation, and negatively affect their performance. Despite the lack of Soviet competition, Americans won a record 83 gold medals at the 1894 Olympics, led by the 23-year-old African-American Carl Lewis.

Weinberger speech and the Strategic Defense Initiative. During the summer of 1986, West European journalists received a copy of the text of a supposed speech by U.S, Secretary of Defense Casper Weinberger on the Strategic Defense Initiative (SDI). No such speech was ever made. The forgery contained five falsehoods: first, that the U.S. had a desire for military "prevalence" (superiority) over the Soviet Union in order to be able to achieve victory in a "controlled nuclear exchange" (limited nuclear war) or a protracted war; second, that the United States would use

SDI to "prevent the development of unfavorable tendencies" in NATO and to control its allies was false; third, that SDI would enable the U.S "to threaten the Soviet Union with a knock-out blow"; fourth, that SDI would "coerce the Soviet Union and make a practical contribution to the liberation of all nations enslaved by Communist totalitarianism, including, possibly, even the Russians themselves" were false; fifth, that SDI would enable the U.S. to maintain a technological lead over its "rivals" in the free world; and sixth, that the Soviets do not have their own form of SDI were additional false statements. The Weinberger forgery was intended to assist the Soviet active measures campaign. However, it was exposed by the U.S. government and did not serve Soviet purposes.

The Schweitzer-Pinochet letter. In July 1985, an Italian journalist found a copy of a letter signed with the name of General Robert Schweitzer, the head of the Inter-American Defense Board. The letter was a forgery addressed to President Pinochet of Chile asking him to provide troops to fight on behalf of the United States in Central America. The journalist contacted the U.S. Embassy and within the day received evidence that the letter was a forgery. He did not write a story based on the letter. A few days later, however, another Italian press service ran a story datelined Mexico City based on the letter. When they were advised it was a forgery, they investigated and discovered that the letter had been provided to one of their writers by the public relations man for the Guatemalan insurgency, which was supported by Cuba and Nicaragua. The news service ran an expose of the forgery, attributing it to the Cubans and Nicaraguans. This incident points to a problem the Soviets had in surfacing forgeries. On the one hand, the common technique of using a plain, unmarked envelope to surface the forgery creates suspicion in the mind of the recipient. On the other hand, the use of a human being to pass on the forgery provided a trail leading back to the forger.

Former United States Information Agency (USIA) specialist in Soviet disinformation Herbert Romerstein wrote a letter to General Schweitzer on August 16, 1985, providing background on the forgery, then sent a copy of this letter to the U.S. Senate Committee on Foreign Relations, where he testified, for printing in a Congressional report on Soviet active measures. Romerstein wrote the word "copy" on the top of the letter then, at the request of a Czech diplomat, Vaclav Zluva, provided him with a copy of this letter. As a precaution, Romerstein drew a line under the word "copy" on the original from which all subsequent copies were made, which made Zluva's letter unique and identifiable.

In August 1986, the *Washington Post* and *U.S. News and World Report* received a forgery in a plain white envelope signed with Romerstein's name. The *Washington Post* called him in; he looked at it, explained the forgery, and the newspaper carried a story on it (August 19, 1986). The forgery was on the letterhead of the United States Information Agency and was signed with Romerstein's name. At the top of the forgery was the word "copy" with no line under it. This made it clear that the exemplar for the forgery was the letter Romerstein had given to the Czech. When Romerstein confronted Zluva about this, he admitted sending the exemplar to Prague.

In the forgery, Romerstein made it appear as if he had organized a USIA effort to spread all of the false stories that had appeared around the world after the Chernobyl disaster. In fact, the false stories were generated by Soviet reluctance to reveal information about the accident. On April 26, 1987, the Soviet publication *Moscow News* admitted, "The formulation, not for the press, is being used more and more often. Why cannot our press use what is being regularly reported to the International Atomic Energy Agency? There are some who do not understand that rumours and hearsay are generated not by summaries and figures, but by their absence."

Reagan signature. In the 1980s, before the downfall of the Berlin Wall in 1989 and the Soviet Union in 1991, President Ronald Reagan's signature appeared on a number of forgeries. The last to appear was in May 1987. It was a supposed memorandum to the secretaries of state and defense, and the director of the CIA. In this forgery, which bore the date March 10, 1983, the president was supposedly ordering the establishment of a U.S. military force called the "Permanent Peace Forces" to intervene in Latin America. This forgery received wide circulation in Latin America and was designed to inflame nationalist and anti-American feelings.

The usual path of a Soviet forgery was from the KGB to a target newspaper. When the target was a legitimate publication it became difficult for the Soviets to succeed in planting the forgery. They often used publications which they could control or influence for the initial surfacing. One publication frequently used this way was the Indian newspaper, *Patriot.* In testimony before a British court on March 24, 1987, Ilya Dzhirkvelov, a former officer of the KGB, revealed that in 1962, on KGB orders, he participated in setting up this newspaper.

After a forgery appeared in a publication such as the *Patriot,* it was replayed by the Soviet press agencies TASS or Novosti. This provided copies in every language for KGB officers to plant in the world press through their agents but not all forgeries were meant for publication. They were passed by KGB agents of influence to officials of a target government in the hope that they would believe forgeries designed to increase anti-American feeling. Such forgeries were often unknown to American officials, who had no opportunity to refute many of them. With the fall of the Soviet Union and the relaxation of the American-Soviet rivalry, KGB forgeries lessened, but forgeries continue to remain a significant weapon of disinformation stories worldwide.

Acknowledgement. The author wishes to thank Herbert Romerstein, former coordinator of Programs to Counter

Soviet Active Measures, United States Information Agency, for his assistance in compiling this essay, especially in clarifying the different Soviet forgeries. Mr. Romerstein's paper, "Forgeries: A Weapon of Soviet Active Measures," prepared for the 1987 Conference on Soviet Active Measures and Propaganda in the Gorbachev Era: Analysis and Response" should be considered a primary source on the subject. I am grateful to Mr. Romerstein for permission to use this paper and for his helpful comments.

FURTHER READING:

BOOKS:

Baldwin, Neil. *Henry Ford and the Jews: The Mass Production of Hate.* New York: Public Affairs, 2001.

Daugherty, William E. *Psychological Warfare Casebook.* In collaboration with Morris Janowitz. Baltimore, MD: Published for Operations Research Office, Baltimore: Johns Hopkins University by Johns Hopkins Press, 1959.

Segal, Binjamin W. *A Lie and a Libel: A History of the Protocols of the Elders of Zion.* [Translation by Richard S. Levy of 1926 edition] Lincoln, NE: University of Nebraska, 1995.

U.S. Department of State. *Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns.* Washington: The Department, 1896.

———. *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1987–1988.* Washington: The Department, 1989.

U.S. International Communication Agency. *Forgeries of U.S. Documents.* Prepared by the European Branch, Office of Research. Washington: The Agency, 1982.

SEE ALSO

Disinformation
Propaganda, Uses and Psychology

DOD (United States Department of Defense)

JUDSON KNIGHT

Although it originated only in 1947, the United States Department of Defense (DOD) comprises elements that date back to the Revolutionary War. Some 3.2 million people, including active military, reservists, National Guard, and civilian personnel, work for DOD, making it one of the nation's largest employers. DOD manages some 600,000 individual buildings or structures worldwide, the most notable of which is the vast five-sided structure in Washington, D.C., whose name is sometimes used to designate the Department as a whole: the Pentagon. Led by the president, as commander-in-chief of the armed forces, with the advice of the secretary of defense and the National Security Council (NSC), DOD is made up of the military services and the unified commands, whose deployment is coordinated by the Joint Chiefs of Staff (JCS).

Historical Background

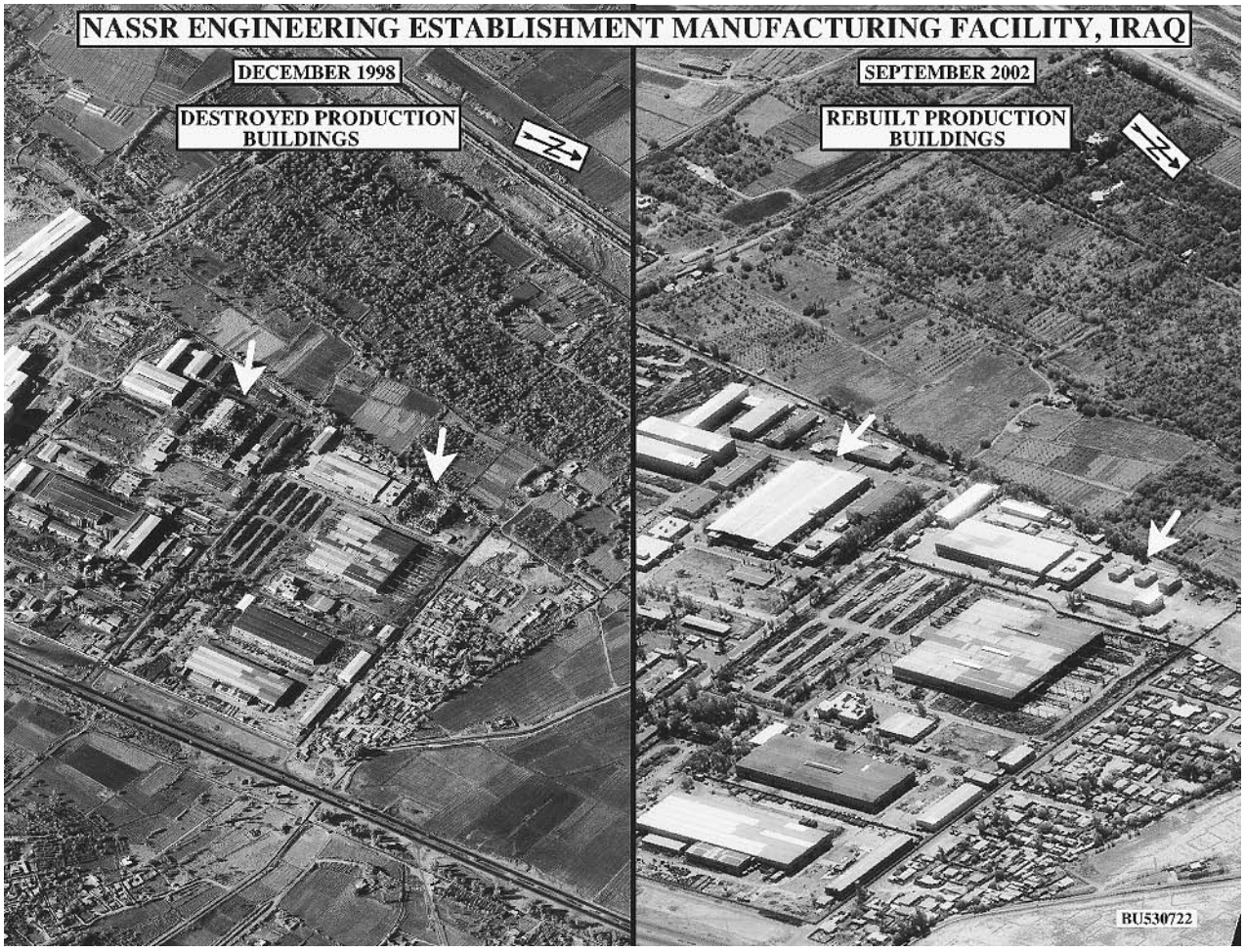
The roots of DOD lie in the establishment of the Army, Navy, and Marine Corps in 1775, at the outset of the American Revolution. In 1789, the new federal government created the War Department, and in 1798 the Department of the Navy, which also includes the Marine Corps. Both the War Department, today known as the Department of the Army, and the Department of the Navy remained Cabinet-level executive departments until 1947.

Another military service, and the only one under DOD control during peacetime, had it roots in the formation of the Revenue Cutter Service in 1790. By 1915, this would become the U.S. Coast Guard, which is today part of the Department of Homeland Security, except in wartime, when it is assigned to DOD. Finally, the U.S. Air Force—which is centered on technology of which the nation's founders could not have conceived—began life as an element of the Army. In 1947, it became a service in its own right.

The statutory foundation of the modern DOD, along with much of the national security apparatus, is the National Security Act of 1947. It created a civilian secretary of defense position, along with a Department of the Air Force. The act transformed the War Department into the Department of the Army, and placed the three major services—Army, Navy, and Air Force—under the secretary of defense. An amendment to the act in 1949 officially created the Department of Defense itself.

The Pentagon. Six years before the National Security Act, just prior to U.S. entry into World War II, the War Department built the structure that today symbolizes DOD: the Pentagon. Prior to its construction, War and Navy department operations were housed in some 17 buildings. The site chosen for the new military headquarters was an area of swamps and garbage dumps at the edge of Washington, D.C., where construction began on September 11, 1941. Just 16 months after the groundbreaking, on January 15, 1943, the building was dedicated. The entire cost of the project, including outside facilities, was $83 million.

A vast structure, the Pentagon covers 29 acres (11.74 hectares) and comprises three times as much floor space as the Empire State Building in New York City. Any one of its five wedge-shaped sections would hold the entire U.S. Capitol Building. Workplace for some 23,000 civilian and military employees, it has 17.5 miles of corridors, yet it takes only seven minutes to walk between any two points in the building. On September 11, 2001—exactly 60 years to the day after construction began on the building—terrorists flew American Airlines Flight 77 into the side of



Department of Defense photo showing the Nassr Engineering Manufacturing facility in Iraq destroyed in 1998, and rebuilt in 2002. Analysts at the Defense Department determined that the rebuilt facility had the capability to produce precision components for nuclear missiles. AP/WIDE WORLD PHOTOS.

the Pentagon, killing over one hundred personnel inside, as well as the people aboard the plane.

DOD Resources

Since the time of the terrorist attacks, DOD has been tasked with the protection of national security through a number of operations, most notably Enduring Freedom in Afghanistan during late 2001 and 2002, and Iraqi Freedom in early 2003. Always important, its significance has become vastly greater since September 2001. Americans following the course of the wars overseas have seen their tax dollars put to use through the deployment of highly trained and equipped troops assisted by the most advanced military technology on Earth.

In almost every regard, the resources available to DOD are remarkable. First among those are the human resources, including 1.4 million active-duty military personnel and 654,000 civilian employees as of 2002. In addition, some 1.2 million serve in the National Guard and Reserve forces. The DOD workforce is also highly trained: whereas 79 percent of working-age Americans have high-school diplomas, 95 percent of DOD employees do, and 5.6 percent of all DOD personnel have master's degrees, as compared to 4.9 percent of the total U.S. work force.

DOD's civilian and active-duty workforce of 2 million makes it among the nation's largest employers, while its budget of $371 billion in 2002 gives it a bottom line far beyond the scope of corporations in the private sector. For comparison, Wal-Mart, with its vast reach, had annual revenues of $227 billion, with 1.3 million employees, in 2001.

When it comes to ownership and management of property, no entity in the private sector can compare with DOD, whose comprehensive inventory of facilities and installations in August, 2002, showed that it was landlord to some 600,000 individual structures at more than 6,000 different sites worldwide. These ranged from tiny unoccupied stations housing a single navigational aid to the Army's enormous White Sands Missile Range in New Mexico, which comprises over 3.6 million acres (5,625 sq. mi.; 14,569 sq. km.)—about the size of Connecticut. In all,

DOD controls some 30 million acres (46,875 sq. mi.; 121,406 sq. km.), an area a little larger than Pennsylvania.

Leadership. Ultimate leadership of DOD rests with the commander-in-chief, the president of the United States. According to the U.S. Constitution, it is the president, the senior military authority, who is responsible for protection of the nation against all enemies, foreign and domestic. The president exercises that authority through two entities that did not exist at the time the Constitution was written: the secretary of defense and the NSC.

Working with these two, the president determines the priorities of national security, and then takes action to ensure that those needs are met. The authority of these executive entities is checked and balanced by that of Congress, which has the power to approve or reject budgets, and whose various committees oversee funding, military operations, and intelligence. Congress exercises oversight in areas ranging from major troop deployments to pay raises.

The Secretary. "National Command Authority" (or "national command authorities") is a term referring to the president and the secretary of defense together. They constitute both a chain of command and, in certain cases, a single commanding entity, though of course the president always has the power to override the secretary.

Notable secretaries of defense have included George C. Marshall (1950–51) under President Harry S. Truman; Robert S. McNamara (1961–68) under presidents John F. Kennedy and Lyndon B. Johnson; Caspar Weinberger (1981–87) under President Ronald Reagan; and Richard Cheney (1989–93) under President George H. W. Bush. In 2001, Cheney became vice president for President George W. Bush, with Donald Rumsfeld—who had served as secretary of defense for President Gerald R. Ford becoming the first secretary to serve nonconsecutive terms.

The Office of the Secretary of Defense carries out policy by assignments to the military departments, which train and equip the military forces; the Chairman of the Joint Chiefs of Staff (JCS), who plans and coordinates military deployment and operations with other JCS members; and the unified commands, which conduct and carry out military operations.

The Joint Chiefs of Staff. The Joint Chiefs of Staff consists of a chairman, vice chairman, and the four heads of the DOD military services (Army, Navy, Air Force, and Marines), each of whom is a four-star general. The chairman sits on the NSC, to which he is principal military advisor. Assisted by the other members of JCS, he plans and coordinates military operations at the National Military Command Center, commonly called "the war room."

During times of military action, the JCS chairman often serves as a public face for the military, conducting high-level media briefings either alongside the secretary of defense, or on his own. Thus, during the Persian Gulf War in 1991, Americans became accustomed to seeing General Colin Powell, as they would a later JCS chairman, Richard Myers, during operations Enduring Freedom and Iraqi Freedom. (Powell, by then secretary of state for George W. Bush, remained a visible figure.)

Unified commands. Actual fighting during wartime is overseen, not by the services themselves, but by the nine unified military commanders. In peacetime, the secretary of defense, acting through the three service secretaries (of the Army, Navy, and Air Force) exercises authority over the training and equipping of troops. In wartime, he exercises authority through the unified commanders, with the advice of the JCS chairman.

On October 1, 2002, DOD established a new Unified Command Plan to prepare it for the wars of the twenty-first century, including the action in Iraq for which U.S. forces were already preparing. The new plan solidified a trend toward unified command that had been taking place in the military for several decades, as leaders recognized the need for integrated warfighting capabilities.

Geographic commands. Of the nine unified commands, five have specific geographic responsibilities. Largest among these is the European Command, whose area of operations extends well beyond Europe, and encompasses 93 nations across 13 million square miles (33,669,850 sq. km.) between the North Cape of Norway and the Cape of Good Hope at the southern tip of Africa, and from the eastern half of the Atlantic Ocean to the Caspian Sea.

Central Command is a name familiar from Operation Iraqi Freedom and other Mideastern deployments, but the word "central" in the title does not mean that it is central command for the entire U.S. military. Rather, it refers to the command's area of operations, in the center of the Eastern Hemisphere, a region that encompasses the Middle East, northeastern Africa, western Asia, and part of the Indian Ocean.

The Northern Command encompasses the continental United States, Canada, Alaska, Central America, and the Caribbean, while the Southern Command is responsible for South America. Finally, the Pacific Command, which covers the largest geographic area—about 50% of Earth's surface, most of it ocean—includes east Asia, Oceania, and the Pacific islands, and shares responsibility for Alaska with the Northern Command.

Non-geographic commands. DOD describes the Joint Forces Command as the "transformation laboratory" for the U.S. military. It is concerned with finding new solutions for future challenges, for developing joint warfighting capabilities through joint training, and for delivering joint forces and capabilities to warfighting commanders.

Strategic Command controls missile, deterrence, space, and satellite systems. The Special Operations Command comprises a number of special support teams, including the Navy SEALs, Army Special Forces, Delta Force, and so on. Finally, the Transportation Command is responsible for moving personnel and materials around the world.

Field activities and defense agencies. In addition to the four services and unified commands, DOD includes seven field activities and 15 defense agencies. The field activities are the American Forces Information Service, Defense Prisoner of War/Missing Personnel Office, Defense Human Resources Activity, DOD Education Activity, TRICARE Management Activity, Office of Economic Adjustment, and Washington Headquarters Services.

Notable defense agencies include the Defense Intelligence Agency, National Imagery and Mapping Agency, and National Security Agency, which, along with the Army, Navy, Air Force, and Marine intelligence components, constitute a majority among the 14 agencies and organizations of the U.S. Intelligence Community. Also significant, from a national security standpoint, are the Defense Security Service, Defense Security Cooperation Agency, Missile Defense Agency, Defense Advanced Research Projects Agency, Defense Information Systems Agency, and Missile Defense Agency.

FURTHER READING:

BOOKS:

Cordesman, Anthony M. *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland.* Westport, CT: Praeger, 2002.

Gilmour, Robert S., and Alexis A. Halley. *Who Makes Public Policy?: The Struggle for Control Between Congress and the Executive.* Chatham, NJ: Chatham House Publishers, 1994.

Ripley, Randall B., and James M. Lindsay. *U.S. Foreign Policy after the Cold War.* Pittsburgh: University of Pittsburgh Press, 1997.

Trask, Robert R., and Alfred Goldberg. *The Department of Defense, 1947–1997: Organization and Leaders.* Washington, D.C.: Office of the Secretary of Defense, 1997.

ELECTRONIC:

U.S. Department of Defense. <http://www.defenselink.mil/> (April 28, 2003).

SEE ALSO

Air Force Intelligence, United States
DARPA (Defense Advanced Research Projects Agency)
Defense Information Systems Agency, United States
Defense Nuclear Facilities Safety Board, United States
Defense Security Service, United States
DIA (Defense Intelligence Agency)
Enduring Freedom, Operation
G–2
INSCOM (United States Army Intelligence and Security Command)
Iraqi Freedom, Operation (2003 War Against Iraq)
Joint Chiefs of Staff, United States
Korean War
Military Police, United States
National Command Authority
National Military Joint Intelligence Center
Navy Criminal Investigative Service (NCIS)
NIMA (National Imagery and Mapping Agency)
NMIC (National Maritime Intelligence Center)
NSA (United States National Security Agency)
NSC (National Security Council)
Persian Gulf War
Special Operations Command, United States
USSTRATCOM (United States Strategic Command)
Vietnam War

DOE (United States Department of Energy)

Though many of its security and intelligence functions have been passed to a subordinate office, the National Nuclear Security Administration (NNSA), the Department of Energy (DOE) is still the principal guarantor of energy security in the United States. It has the task of maintaining the safety and reliability of the U.S. nuclear stockpile, cleaning up the environmental legacy of the Cold War arms race, and advancing science and technology in the service of national interests. In addition to DOE's overall concern for global nuclear security, the DOE Office of Security works to protect employees, DOE contractors, and entrusted assets. Office of Security programs include the Nonproliferation and National Security Institute (NNSI) and the Cyber-Forensic Laboratory. DOE also has an intelligence office that is a component of the U.S. Intelligence Community.

Background

Most Americans tend to think of DOE in connection with civilian activities—for example, its effect on the price of gasoline at the pump—but in fact it is one of the federal government's most significant security assets. Its roots go back to the Manhattan Project, the successful effort to build an atomic bomb during World War II. Though most of the scientists in the Manhattan Project were civilian, the governing authority was military. Thus, in 1942, the first full year of U.S. participation in the war, the U.S. Army Corps of Engineers established the Manhattan Engineer District to oversee the project.

The war's end saw a heated battle in Congress over the issue of whether to place atomic power under civilian

A trauma intervention volunteer plays the role of a casualty of a simulated gas attack during an inter-agency emergency response drill in Portland, Oregon. AP/WIDE WORLD PHOTOS.

or military control. In 1946, the issue was settled with the passage of the Atomic Energy Act, which created the civilian-run Atomic Energy Commission (AEC). In the early Cold War years, AEC put its greatest emphasis on the production of nuclear weapons, and on the development of nuclear reactors to propel naval vessels. A second Atomic Energy Act, in 1954, opened the field of nuclear power to the private sector, and AEC served as the regulatory agency for the new industry.

As a result of U.S. vulnerabilities in the face of the 1973 Arab oil embargo, Congress in 1974 passed the Energy Reorganization Act, which abolished AEC and replaced it with two other agencies: the Nuclear Regulatory Commission (NRC) and the Energy Research and Development Administration. As the energy crisis of the 1970s wore on, however, it became more and more apparent that the government could most effectively deal with energy issues by unifying energy organization and planning. The result was the Department of Energy Organization Act, signed into law by President James E. Carter on October 1, 1977.

The new department replaced not only the Energy Research and Development Administration, but also the Federal Energy Administration, the Federal Power Commission, and programs or offices of other agencies. (NRC remained independent.) At the outset, DOE took the role of providing a framework for the development of a comprehensive national energy plan. It also undertook long-term, high-risk research and development in areas that included energy technology, energy conservation and regulation, federal marketing of power, energy data collection and analysis, and nuclear weapons.

The period since DOE's inception has seen a shift in focus in view of America's changing needs within the global landscape. Faced with the energy crisis of the late 1970s, DOE directed its efforts toward development and regulation of energy resources. The arms buildup that took place under the administration of President Ronald Reagan in the 1980s saw DOE turn its attention to nuclear weapons research, development, and production. With the end of the Cold War, DOE entered a new phase, in which its emphasis was on nonproliferation, nuclear stewardship, retooling of nuclear weapons for peaceful uses, and environmental cleanup.

The DOE Today

Energy efficiency and conservation have remained focal points of DOE efforts, particularly in view of increasing tensions with and in the Middle East—where most of the world's oil is produced. In his 2003 State of the Union address, President George W. Bush, pledged $1.2 billion toward the development of hydrogen-powered fuel cells. Not only would the development of hydrogen power, long an area of research within DOE, free the United States from dependence on Middle Eastern oil, but it would greatly reduce the environmental impact of human activities, and provide an energy resource of almost limitless renewability.

Today, DOE accomplishes its mission along four principal program lines: national defense, energy, the environment, and science. DOE national defense programs, which DOE has continued to list as a top priority, have a

fourfold purpose: to protect U.S. nuclear weapons, to promote nuclear safety internationally, to advance the cause of non-proliferation, and to continue providing safe and effective nuclear power for the operation of U.S. Navy vessels.

In the area of energy, DOE priorities include increasing domestic production, revolutionizing Americans' approach to conservation and efficiency, and promoting the development of renewable and alternative sources—including hydrogen. The environmental program overlaps somewhat with the national defense goal of cleanup of environmental and safety hazards left over from the Cold War. DOE is also committed to the safe and permanent disposal of radioactive waste. There is also overlap between the energy priority and a fourth program area, that of science, in which DOE's greatest interest is revolutionizing the search for, production, and delivery of energy.

Some aspects of DOE's responsibilities for national and global security are the work of NNSA, created by Congress in 1999 as a response to apparent security violations that occurred during the presidency of William J. Clinton. Though NNSA is an agency of DOE, its administrator, an undersecretary within the department, has direct responsibility over most of its functions.

Responsibilities of DOE and NNSA overlap in some areas. For example, both DOE and NNSA are concerned with nonproliferation programs involving Russian and other former Soviet republics. The purposes of these programs include the securing of nuclear weapons, elimination of excess materials, prevention of the outflow of nuclear expertise to other countries, and downsizing of the overall nuclear weapons complex in the former Soviet Union.

A particular area of emphasis in the DOE nonproliferation and verification program is the conversion of highly enriched uranium (HEU) to peacetime uses. In 1994, DOE agreed to purchase 500 metric tons of Russian HEU over the next 20 years, at a cost of $12 billion. The materials would then be converted to low enriched uranium and applied to commercial uses.

Emergency Operations

The Emergency Operations (EO) office of DOE is a joint mission of DOE and NNSA, created to administer and direct the emergency response capabilities of both. Focused on nuclear and radiological emergencies, EO is the principal DOE point of contact for emergency management activities.

EO develops policy for the emergency management of sites, facilities, and operations; manages the response to nuclear and radiological emergencies worldwide on behalf of the U.S. government; coordinates inter- and intradepartmental emergency management activities; evaluates and works to improve emergency response capabilities; and seeks to integrate programs, systems, assets, capabilities, training, and responses to improve emergency capabilities.

Offices of Emergency Management and Response. EO consists of two offices, the Office of Emergency Management (OEM) and the Office of Emergency Response (OER). OEM is charged with developing and implementing DOE's emergency management system for DOE and NNSA facilities, sites, and activities. It is responsible for operations and training, direction of emergency response exercises, development of emergency management policies, and support of DOE and NNSA site emergency planning and response.

OER supports both crisis response and emergency management through various departmental radiological emergency response assets or capabilities. It is responsible for the overall program management and organizational structure of EO in both emergency and non-emergency situations. OER also supports federal counterterrorism and consequence management efforts that have a nuclear or radiological dimension. In addition, EO as a whole represents DOE as needed in multiagency responses to nuclear or radiological threats affecting public safety and health.

Office of Security. Following the September 11, 2001, terrorist attacks, numerous components of the federal security and intelligence apparatus came under scrutiny, and among these was the DOE Office of Security. In 2002, Representative Ed Markey (D-MA) released figures showing that the number of DOE security forces had dropped from 7,091 in 1992 to just 4,262 in 2001, a reduction of 40 percent. Political and intelligence analysts argued that these reductions were typical of the post-Cold War, Clinton-era reduction in security and intelligence resources, and after September 2001, DOE Office of Security director Joseph C. Mahaley worked to rebuild those resources.

In his role as chief functionary responsible for the development of policy regarding the protection of national security assets under DOE control, Mahaley gave a statement to the U.S. House of Representatives Committee on the Budget on December 5, 2001. In his statement, Mahaley explained that, in accordance with the DOE Security Condition (SECON) system, the office had declared a level 2 emergency (SECON 2) on the day of the terrorist attacks, but had since dropped to—and stayed at—SECON 3, the highest alert level that could be maintained indefinitely.

Missions and priorities. The highest DOE security priority, Mahaley explained, is the protection of special nuclear material, or SNM, including everything from raw nuclear materials to complete nuclear weapons. DOE's nuclear safeguards and security program are directed toward preparing for a worst-case scenario involving the theft of these materials.

In addition to its mission of protecting materials and technology—including non-nuclear assets of DOE—the Office of Security also participates in the Technical Support Working Group, an interagency counterterrorism team headed by the State Department. The Office of Security had, at the time of Mahaley's statement, 550 trained counterterrorism personnel in its special response teams at 11 locations, along with 3,500 other armed officers.

Programs. Office of Security programs include NNSI, a training provider not only for DOE, but for students from more than 100 government departments and agencies. Founded in 1984 and formerly known as the Central Training Academy, NNSI is located at Kirtland Air Force Base in Albuquerque, New Mexico. Among its schools are the Professional Development Program, the Defense Nuclear Nonproliferation and International Cooperation Academy, the Foreign Interaction Training Academy, the Emergency Operations Training Academy, the Safeguards and Security Central Training Academy, and the Counterintelligence Training Academy.

The last of these, known as CITA, was established in May 2000, and offers instruction to contractor employees as well as federal workers. In addition to full courses, it offers seminars on subjects such as "Counterintelligence for Managers," "Economic Espionage: Protecting Intellectual Property," and "The Technical Collection Threat to Travelers."

The other major Office of Security program is the Cyber-Forensic Laboratory. Cyber-forensics is the application of science and technology to the discovery, analysis, and reconstruction of data extracted from any element of computers, computer peripherals, or computer systems. The laboratory assists DOE with the collection and study of electronic data relating to DOE security, or that of other government agencies and departments.

Office of Intelligence. DOE's Office of Intelligence (IN) is a member of the U.S. Intelligence Community (IC), producing intelligence for use both within DOE, and across the IC as a whole. Within the IC, the Office of Intelligence is the leading technical intelligence resource in four areas: nuclear weapons and nonproliferation; nuclear energy, safety, and waste; science and technology; and energy security.

The mission of IN within the IC is three-fold: to provide DOE and other agencies and departments, particularly IC members, with timely, accurate, and effective analyses of foreign intelligence; to make DOE's expertise available to the intelligence, law enforcement, and special operations communities; and to provide timely, specialized technological applications and operational support to those communities.

Presidential Decision Directive (PDD) 61, issued by President Clinton in February 1998, reorganized the intelligence structure at DOE. Counterintelligence and foreign intelligence functions were separated, and both offices were made directly answerable to the secretary of energy. The new counterintelligence director would be a senior Federal Bureau of Investigation (FBI) executive, and would have direct access to the directors of Central Intelligence and the FBI as well as the secretary of energy. In conjunction with the Office of Security, the director would work to implement specific security measures designed to reduce the threat to classified and sensitive information at DOE.

DOE operates a number of national laboratories that bring together scientists from a variety of disciplines to work on military and non-military related projects. National laboratory scientists have developed a number of technologies related to national security interests.

FURTHER READING:

BOOKS:

Closing the Circle on the Splitting of the Atom: The Environmental Legacy of Nuclear Weapons Production in the United States and What the Department of Energy Is Doing About It. Washington, D.C.: U.S. Government Printing Office, 1995.

Department of Energy Non-Proliferation Programs with Russia: Hearing Before the Committee on Foreign Relations, United States Senate, One Hundred Seventh Congress, First Session, March 28, 2001. Washington, D.C.: U.S. Government Printing Office, 2001.

Rudman, Warren B. *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy.* Washington, D.C.: President's Foreign Intelligence Advisory Board, 1999.

PERIODICALS:

Carr, Rebecca. "Security at Nuke Labs Lax—DOE 'Indifferent' Despite Sept. 11." *Atlanta Journal-Constitution.* (August 20, 2002): A11.

ELECTRONIC:

Department of Energy. <http://www.energy.gov> (March 7, 2003).

Department of Energy Office of Security. <http://www.so.doe.gov> (March 7, 2003).

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
Energy Technologies
Intelligence Community
NNSA (United States National Nuclear Security Administration)

Domestic Emergency Support Team, United States

Up to the time of its transfer to the newly created Department of Homeland Security (DHS), the Domestic Emergency Support Team (DEST) was the smallest—or, at

least, the most obscure—of the Justice Department offices dedicated to national security and intelligence. It was created under Presidential Decision Directive 39 (PDD 39), "U.S. Policy on Counterterrorism," signed by President William J. Clinton on June 21, 1995. That document called for a "rapidly deployable interagency emergency support team" to assist the State Department in situations of emergency involving U.S. citizens on foreign soil, as well as for a DEST to operate in domestic incidents under the direction of the Federal Bureau of Investigation (FBI).

According to PDD 39, "The DEST shall consist only of those agencies needed to respond to the specific requirements of the incident," indicating that DEST is not so much an office unto itself as it is a coordinating agency. Its function is not only to respond to terrorist incidents; in July 2002, for instance, DEST went on call in response to flooding in Texas. However, President George W. Bush made clear its place in the post-September 11, 2001, security environment by including DEST in the Homeland Security Act, which he sent to Capitol Hill on June 18, 2002. Title V, "Emergency Preparedness and Response," established the position of under secretary for Emergency Preparedness and Response, whose duties would include oversight of DEST. DEST was one of several agencies transferred from Justice to DHS when that department began functioning in March 2003.

A pedestrian passes under the arm of a traffic surveillance system in the Chelsea neighborhood of New York City. AP/WIDE WORLD PHOTOS.

■ FURTHER READING:

PERIODICALS:

Reiss, Tom. "Now Will We Heed the Biological Threat?" *New York Times.* (February 21, 1998): 11.

SEE ALSO

FBI (United States Federal Bureau of Investigation)
Homeland Security, United States Department

Domestic Intelligence

Domestic intelligence is a term for efforts by a government to obtain information about activities that pose an actual or putative threat to internal security. In authoritarian or totalitarian regimes, domestic intelligence-gathering by the government is a regular part of daily life, but in a liberal democratic system such as those of North America or Western European countries, it is more problematic. United States domestic intelligence programs of the post World War II era raised Americans' ire after they came to light, but in the wake of the September, 2001, terrorist attacks, many Americans and Europeans put aside fears of government surveillance in favor of a new demand for heightened security.

World War II to Watergate. Whereas most Americans of the postwar era knew that the intelligence services of the Soviet Union and other totalitarian states kept a close watch on their citizens, most had no idea of the extent to which their own government was watching certain elements. During the 1970s and later, information about massive domestic intelligence programs came to light. Among these was Shamrock, which involved the interception of telegrams and other forms of communication between 1945 and 1975. In another domestic intelligence/surveillance program, Chaos, the Federal Bureau of Investigation (FBI) monitored Vietnam War protesters between 1967 and 1972, looking for ties to the Soviets.

Revelation of these and other activities came to light in the wake of the Watergate scandal, which influenced an attitude among some citizens of suspicion toward the government. Questionable as they may have been in some regards, Shamrock and Chaos subjected only a fraction of the population to government scrutiny, but in the atmosphere of reaction that pervaded the mid- to late

1970s, many Americans began to assume that there was no limit to the government's desire for information on its citizens' private lives. These fears both led to, and were fueled by, investigations in Congress, most notably that of the Church Committee in the Senate.

The twenty first century. Since that time, government agencies have been placed under much tighter restrictions with regard to domestic intelligence and surveillance. The September, 2001, attacks, however, influenced a shift in a different direction. Congress, once suspicious of domestic intelligence-gathering, called for a new effort to root out potential terrorists on U.S. soil. The same was true in Europe, where countries such as Belgium—which had always restricted domestic intelligence efforts—gave their internal security services much freer rein.

During 2002, the U.S. executive and legislative branches debated the question of which agency should handle a new domestic intelligence effort: the FBI (formerly in charge of counterterrorism) or the Central Intelligence Agency (CIA). In February 2003, President George W. Bush placed the CIA in charge of a new domestic counterterrorism intelligence agency, to be formed later that year. The FBI would work with the CIA in the new unit.

FURTHER READING:

BOOKS:

Alden, Edward, and James Harding. "CIA Wins Battle to Defend U.S. Against Terror." *Financial Times* (February 15, 2003): 1.

Crawford, David. "Europe Eases Limits on Police, Intelligence Services—Fear of Islamist Terrorism Erodes Traditional Divide Between the Two Branches." *Wall Street Journal* (December 17, 2002): A15.

Eggen, Dan. "Bush Aims to Blend Counterterrorism Efforts." *Washington Post* (February 15, 2003): A16.

Johnston, David. "FBI Director Rejects Agency for Intelligence in United States." *New York Times* (December 20, 2002): A22.

Lichtblau, Eric. "FBI and CIA to Move Their Counterterror Units to a Single New Location." *New York Times* (February 15, 2003): A14.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

Priest, Dana, and Juliet Eilperin. "Panel Finds No 'Smoking Gun' in Probe of 9/11 Intelligence Failures." *Washington Post* (July 11, 2002): A1.

SEE ALSO

Church Committee
CIA, Legal Restriction
Domestic Intelligence
FBI (United States Federal Bureau of Investigation)
Intelligence and democracy: Issues and Conflicts
Intelligence, United States Congressional oversight
Nixon Administration (1969–1974), United States National Security Policy
Operation Shamrock
Privacy: Legal and Ethical Issues
September 11 Terrorist Attacks on the United States
United States, Counter-terrorism Policy
Watergate

Domestic Preparedness Office (NDPO), United States National

Formed in October 1998, the United States National Domestic Preparedness Office (NDPO) is the coordination center for all federal efforts in response to weapons of mass destruction (WMD). It works with a variety of federal agencies, and assists state and local emergency responders in preparing for the response to a WMD event. The Federal Bureau of Investigation (FBI) originally formed NDPO, which became part of the Department of Homeland Security (DHS) in March 2003.

An August, 1998, stakeholders conference involving leading members of the federal emergency response community resulted in a recommendation that a single office coordinate all federal WMD preparedness assistance programs. The result was the creation of NDPO by Attorney General Janet Reno, who placed the FBI in charge of the new office, initially known as the Office for State and Local Domestic Preparedness.

NDPO works in partnership, not only with the FBI, but also with the departments of Energy, Health and Human Services, and Justice; the Federal Emergency Management and Environmental Protection agencies; the Office for State and Local Domestic Preparedness Support; and the National Guard Bureau. Its mission is to coordinate and facilitate all federal WMD efforts to assist state and local responders in their response to a WMD event. This requires assistance in planning, training, equipment, exercise, and health and medical issues.

FURTHER READING:

PERIODICALS:

"Training Centers Offer Assistance." *Crime Control Digest* 36, no. 18 (May 3, 2002): 11.

Vise, David A. "Senate Panel Blasts FBI's Deployment." *Washington Post.* (July 21, 2000): A29.

ELECTRONIC:

National Domestic Preparedness Office. Federation of American Scientists. <http://www.fas.org/irp/agency/doj/fbi/ndpo/> (March 28, 2003).

Office of Domestic Preparedness. U.S. Department of Justice. <http://www.ojp.usdoj.gov/odp/> (March 28, 2003).

SEE ALSO

FBI (United States Federal Bureau of Investigation)
Homeland Security, United States Department
Weapons of Mass Destruction

Doo Transmitter

A Doo radio transmitter, officially known as a T-1151 radio transmitter, is a radio transmission device camouflaged as a pile of animal droppings or, in its most common form, a large single fecal dropping from an animal indigenous to the area of intended use. Regardless, the external form of the device was designed to discourage close examination and thus, detection or disruption.

Initially developed by United States military intelligence about 1970, the Doo transmitter was a homing device camouflaged as dog or monkey feces for use in Vietnam. At just over four inches long and three-quarters of an inch in height, this inconspicuous spy tool was small enough to be carried easily. It could send or receive radio messages, usually by Morse code. The effectively camouflaged beacon was positioned throughout the jungles of Vietnam, where it transmitted a radio signal that helped aircraft pinpoint key enemy ground sites for strikes or reconnaissance. The device often had a peat moss crusted shell.

Because the Doo transmitter was often left undisturbed, operational life was often a function of the battery life of its nickel-cadmium battery array. This advantage was often essential when the transmitter was utilized as a homing device. Because the device gave the appearance of fecal matter, it was often left undisturbed and thus a retained high efficiency as a homing beacon even when planted days or weeks before a mission.

Another operational advantage of the Doo transmitter was its capacity to remain concealed long after its operational usefulness ended. Accordingly, in addition to detection avoidance while operational, the long-term detection avoidance qualities of the transmitter did not allow the enemy the intelligence advantages of knowing that a particular site was at one time used as a transmission or rendezvous point.

The Doo transmitter design reflects an open concealment design concept used by intelligence agencies. Such open concealment devices remain easily visible, only the operational nature of the device is concealed.

SEE ALSO

Shoe Transmitter
Short-Wave Transmitters
Vietnam War

Doppler Radar.

SEE *Stealth Technology.*

Dosimetry

LARRY GILMAN

Dosimetry measures the amount of radiation energy absorbed over a given period of time by an object (e.g., human body) or by part of that object (e.g., an organ or tumor). Here, radiation refers not only to ionizing radiation of the sort emitted by radioactive materials—fast particles and gamma rays—but to light, radio waves, or ultrasound. Dosimetry is essential wherever radiation is utilized to treat cancer; the treatment must deliver a sufficient dose to target tissues without delivering too large a dose to other parts of the body. Dosimetry is also needed, wherever radioactive materials are handled in significant quantities, to track the cumulative exposure of individuals and to moniotor for accidental releases of radioactive material.

A device that measures cumulative radiation exposure is a *dosimeter*. A Geiger counter is a radiation detector, but not a dosimeter, because it gives only a moment-to-moment reading of radiation intensity; a strip of photographic film, however, whose degree of exposure indicates how much radiation it has absorbed (up to its saturation limit), can act as a dosimeter. Filmstrip dosimeters are, in fact, still used to measure exposure to ionizing radiation. By grading the sensitivity of a specially formulated film strip from one end to the other, it can be made to indicate net, cumulative radiation exposure as a bar of darkening that grows from the most sensitive end of the film to the least sensitive end. Such "badge dosimeters" are common in the nuclear weapons and nuclear-power industries. However, they have the disadvantage that they must be developed to be read, and so do not give the bearer immediate knowledge of their exposure level.

Another type of dosimeter is the pen ionization dosimeter. These devices contain a long, narrow chamber filled with a few cubic centimeters of nonconducting gas. A metallic contact touches the interior of the chamber at each end. When the dosimeter is to be used, an initial electric charge is placed on the gas tube; that is, an imbalance of electrons is created between the two ends. Since the gas in the tube is normally nonconducting, electrons cannot travel through it to even out the charge imbalance. However, ionizing radiation passing through the gas forcibly frees electrons from atoms in the gas (i.e., partly ionizes the gas), and these negatively charged electrons are free to flow toward the end of the tube having a positive charge. The more ionizing radiation the pen dosimeter is exposed to, therefore, the more of its initial

charge is enabled to leak through the gas tube; the amount of charge lost is a measure of the amount of radiation that has passed through the tube. A pen dosimeter can be read by its bearer at any time, and so gives a current reading of exposure; however, pen dosimeters readings can be affected by mechanical shock or vibration.

A more modern dosimeter design is the thermoluminescent dosimeter (TLD). A TLD contains a tiny crystal of lithium fluoride (sometimes mounted in a finger-ring) that undergoes cumulative structural changes as it is exposed to ionizing radiation. When heated, the crystal glows, giving off an amount of light that is proportional to its radiation exposure. This light is observed by an electronic sensor in a readout unit and recorded digitally. This data can be stored in a central database, a convenient feature if an organization wishes to systematically monitor radiation exposure of a large body of personnel. Databasing of TLD data has been used, for example, by Canada to monitor the exposure of its troops to radiation from depleted-uranium munitions used by NATO in Bosnia. TLDs, unlike film badges, can be re-used; however, they must be inserted in a reader that heats the crystal and records the light emitted, a process that may take 20 to 30 seconds and erases the data in the crystal.

An even more recent entry in the dosimeter field is the optically stimulated luminescence dosimeter (OSLD). In this design, a thin film of crystalline aluminum oxide undergoes cumulative structural changes as it is exposed to ionizing radiation; when an exposure reading is desired, the crystal is exposed to green laser light. The amount of blue light emitted by the film in response is proportional to its radiation exposure. Unlike a TLD, an OSLD can supply an instant readout that can be repeated if necessary.

Solid-state devices that measure radiation by detecting ionization leakage current through a transistor device also exist. Radiation detectors and dosimeters based on such solid-state technology have been available since the 1980s, but have not edged out other dosimeter technologies in terms of cheapness, sensitivity, and accuracy.

Dosimetry for laser light, radio waves, and ultrasound, which is often required in medical contexts, is more difficult than dosimetry of ionizing radiation. One method of measuring dose delivered to a volume of tissue is to measure the temperature increase of the tissue; the more increase, the more radio or sound energy has been absorbed. However, these techniques do not work for tissue embedded in living organisms (where temperature measurement is difficult and where heat is rapidly conducted away) or for whole-body exposure, as biologically tolerable doses of laser, radio, and sound energy produce undetectably slight changes in body temperature. Absorption by the body of radio waves is particularly different from absorption of ionizing radiation; the body acts as a complex antenna whose performance is strongly affected by its posture and orientation and by nearby objects. Dosimetry for radio and ultrasound therefore relies heavily on computational models rather than on direct measurements.

FURTHER READING:

ELECTRONIC:

"Measuring Occupational Exposures." Health Physics Society. <http://hps.org/publicinformation/ate/faqs/lowmeasure.html> (April 17, 2003).

"Using and Wearing Radiation Dosimeters." Princeton University: Environmental Health and Safety. <http://www.princeton.edu/~ehs/UsingandWearingDosimetry.html> (April 17, 2003).

SEE ALSO

Radiation, Biological Damage
Radioactive Waste Storage
Radiological Emergency Response Plan, United States Federal

Double Agents

A double agent is person who conducts espionage for two, usually antagonistic, countries. Double agents allow intelligence services to gather information by infiltrating enemy organizations under cover. An organization usually recruits double agents from the ranks of a rival intelligence service, and then "turns" them, using them as spies for their own purposes.

The use of double agents in intelligence tradecraft and strategy is one of the oldest practices in the art of espionage. Spies and double agents appear in literature and written histories from the ancient civilizations of Egypt, China, India, Greece, and Rome. The rise of great civilizations and militaries prompted the need for intelligence gathering through infiltration of enemy organizations.

In the modern era, double agents gained notoriety in a variety of espionage scandals. While some double agents worked in accordance with their ideals, others were paid handsomely with money or political favor for betraying secrets. During the Cold War between the United States and the Soviet Union, exposure of double agents became a key part of counterintelligence operations. Double agents compromised intelligence, military, industrial, and government strongholds in both nations, sometimes with devastating consequences. Since the fall of the Soviet Union, and the dissolution of its KGB intelligence agency, access to formerly secret archives and testimony of former agents has exposed several double agents, and the extent of their decades-long espionage operations. In the United States, double agents working for the Soviet Union (and later for Russia), such as Aldrich Ames and Robert Hanssen were discovered, brought to trial, and sentenced to life in prison.

During the Cold War, and the decade after its end, double agents were popularly associated with intrigue,

Harold "Kim " Philby (standing) is shown during a 1968 news conference after being cleared of allegations that he was the "third man" who tipped off diplomats Guy Burgess and Donald Maclean. In fact, Philby led a spy ring of former Cambridge University students, including Burgess and Maclean, for the Soviet Union. ©BETTMANN/CORBIS.

and trials of double agents gained extensive media attention. However, within the intelligence community, the use of trained double agents waned. Intelligence services replaced human intelligence operations with an increasing reliance on satellite and electronic surveillance technology. Technological surveillance permits intelligence organizations to conduct operations without assuming the high risks associated with using human intelligence or double agents exclusively.

■ FURTHER READING:

ELECTRONIC:

United States Federal Bureau of Investigation. <http://www.fbi.gov/libref/historic/famcases/hanssen/hanssen.htm#anchor26782> (April 2003).

The Center for Counterintelligence and Security Studies. <http://www.cicentre.com/Documents/DOC_Hanssen_1.htm> (April 2003).

SEE ALSO

Ames (Aldrich H.) Espionage Case
CIA (United States Central Intelligence Agency)
Dead Drop Spike
Dead-Letter Box
FBI (United States Federal Bureau of Investigation)
Hanssen (Robert) Espionage Case
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*

Drop

"Drop" is intelligence parlance for the location at which an agent passes information to another, or the act of passing that information—as in "making a drop." In a live drop, the two individuals actually meet. Given the dangers of this, it is more common to employ a "dead drop." The latter term refers to a prearranged spot at which one party passes information to another without actually meeting. Often a dead drop—a term that again refers both to the place and the act—also involves the transfer of money, as when a double agent leaves information for a handler, and the handler returns the favor with cash payment.

It so happens that the most commonly cited examples of drops and dead drops involved agents working for the Soviet bloc during the Cold War. This is probably the case because, for obvious reasons, Western intelligence agencies are not as likely to reveal the methods employed by their own agents.

One oft-cited example is that of John Walker, who passed $1 million of United States Navy secrets to the Soviets before the Federal Bureau of Investigation (FBI) finally caught up with him in 1985. In making his drops, Walker used a garbage bag containing bits of recognizable trash—but nothing that would smell strongly and attract animals—along with documents and other important materials. His KGB handler would in turn leave another bag containing money.

In the same year the FBI caught Walker, the Soviets recruited the FBI's own Robert Hanssen, who accumulated $1.4 million for betraying his country before the authorities caught him in February 2001. At the time of his arrest, Hanssen was making a dead drop under a footbridge at Foxstone Park in Vienna, Virginia.

■ FURTHER READING:

BOOKS:

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today.* New York: M. Evans, 1997.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

ELECTRONIC:

"Traitorous Actions": FBI Agent Charged With Spying for Moscow. <http://abcnews.go.com/sections/us/DailyNews/FBIarrest010220.html> (February 1, 2003).

SEE ALSO

Cambridge University Spy Ring
Dead Drop Spike
Hanssen (Robert) Espionage Case
Walker Family Spy Ring

Drug Control Policy, United States Office of National

JUDSON KNIGHT

The White House Office of National Drug Control Policy, or ONDCP, is an independent office of the executive branch of the United States government, and reports directly to the president. Established by the Anti-Drug Abuse Act of 1988, ONDCP is the principal architect of national drug control strategy. It directs anti-drug efforts, and establishes a gameplan for achieving goals, along with a budget and guidelines for cooperation between federal, state, local, and private entities.

Enabling legislation. The Anti-Drug Abuse Act of 1988, which set a policy goal of creating a "drug-free America," included as one of its key provisions the establishment of ONDCP. It is charged with setting priorities for anti-drug policy, implementing a national strategy for fighting drugs, and certifying federal drug-control budgets. The drug-fighting strategy, as specified by the statute, must be comprehensive and founded in research; must contain measurable objectives and long-range goals; and must seek reductions in drug abuse, trafficking, and the consequences thereof. Specific aims include the discouragement of drug abuse among young people, a reduction in the number of drug users, and decrease in the availability of drugs.

A series of executive orders in 1993 (E.O. 12880) and 1996 (12992 and 13023) collectively placed ONDCP in the lead role for drug policymaking entities within the executive branch of the federal government. In 1994, the Violent Crime Control and Law Enforcement Act added to ONDCP's responsibilities the assessment of budgets and resources related to the overall national drug control strategy.

The 1997 Drug-Free Communities Act empowered ONDCP to undertake a national initiative whereby federal grants would go to community coalitions with a demonstrated record of reducing substance abuse among local populations, encouraging cooperation between the private and public sectors, and involving citizens in anti-drug efforts. In 1998, the ONDCP Reauthorization Act expanded ONDCP's role and established additional requirements for the office, including the development of a long-term national strategy for combating illegal drug use and distribution.

Anti-drug advertising. Also in 1998, the Media Campaign Act charged ONDCP with leading a national media campaign directed toward young people. This placed the office in collaboration with the Partnership for a Drug-Free America (PDFA), a private organization to which advertisers donate resources as a means of discouraging drug use among America's youth. ONDCP in 1998 initiated the National Youth Anti-Drug Media Campaign, which mobilized both the private and public sectors to fight drug use among young people.

Four years later, a private survey commissioned by ONDCP found that advertising had done little to discourage drug use among adolescents. However, PDFA chairman Jim Burke asserted in a *Washington Post* editorial that this assessment was too pessimistic: not only had drug use among teens not increased, but the advertising had helped to raise awareness among parents.

An ONDCP-sponsored campaign that established a connection between drugs and terrorism drew fire from some critics when it debuted at the 2002 Superbowl. While the connection between the heroin trade and terrorist groups such as al-Qaeda has been established, critics maintained the link between terrorism and drugs is less obvious for marijuana, some of which is grown in the United States. Furthermore, in the view of some detractors, the introduction of the terrorism theme complicated what should have been a simple message discouraging drug use for health and social reasons. Nevertheless, the campaign sparked debate and awareness for personal responsibility issues regarding the global implications for illegal drug purchase and use.

FURTHER READING:

BOOKS:

Ojeda, Auriana. *Drug Trafficking.* San Diego, CA: Greenhaven Press, 2002.

Thompson, Stephen P. *The War on Drugs: Opposing Viewpoints.* San Diego, CA: Greenhaven Press, 1998.

PERIODICALS:

Burke, Jim. "Kids, Drugs, and Bureaucrats." *Washington Post.* (May 21, 2002): A17.

Grimm, Matthew. "A Dubious Pitch." *American Demographics* 24, no. 5 (May 2002): 44–46.

"ONDCP Says Anti-Drug Ads Are Ineffective." *Crime Control Digest* 36, no. 20 (May 17, 2002): 4.

ELECTRONIC:

White House Office of National Drug Control Policy. <http://www.whitehousedrugpolicy.gov/> (February 22, 2003).

SEE ALSO

DEA (Drug Enforcement Administration)
NDIC (Department of Justice National Drug Intelligence Center)

Drug Intelligence Estimates

CARYN E. NEUMANN

The National Drug Intelligence Estimate (NDIE), an annual publication of Royal Canadian Mounted Police (RCMP) from 1985 until 1994, identified trends in drug abuse and centers of drug trafficking. NDIE grew out of the realization that illegal drug production, use, and transit affects all countries and that effective international cooperation required an exchange of information. NDIE received wide distribution within Canada and among those countries officially recognized by Canada.

As the Cold War wound down in the 1980s, new elements in the international drug trade emerged at the same time that significant intelligence resources in Western countries became available to combat drug trafficking. The rise in both the supply of drugs and the number of traffickers combined with the reduction of international hostilities to open the possibility of increased international anti-drug trade cooperation. Accordingly, in 1984, the United Nations General Assembly pushed member countries to strengthen and enhance international cooperation in criminal matters relating to the illegal traffic in narcotic drugs. Canada responded to this call by creating NDIE.

The RCMP received the assignment to assemble and distribute NDIE because it is the Canadian agency that is charged with enforcing the nation's drug control laws by apprehending those individuals and organizations involved in illicit drug activities. The Strategic Analysis Branch of the RCMP's Drug Enforcement Directorate produced NDIE as well as regular digests of drug trends and a series of special reports on such matters as money laundering, outlaw motorcycle gangs and aerial cocaine smuggling into Canada. The publications worked together to provide law enforcement personnel with an accurate picture of Canada's relationship to the international drug trade. The RCMP distributed NDIE to all federal departments concerned with drug law enforcement. Provincial and local drug enforcement units also received copies of the estimate, as did RCMP liaison officers stationed at Canadian embassies who shared the information with their host countries.

NDIE revealed a number of trends in drug smuggling. It reported that while some drugs are produced and consumed domestically, much of the drug trade flowed from developing to developed nations. It predicted that drug incidents involving former citizens of the Soviet Union and its Eastern European allies would increase because the collapse of these countries had left the residents in desperate economic straits and vulnerable to exploitation by both domestic and foreign drug trafficking groups. NDIE identified three threats relating to these ex-communist countries: 1) the shipment of Colombian cocaine to Eastern Europe and then to the West; 2) the increased cultivation of opium in the former Soviet republics of Central Asia and its manufacture into heroin and subsequent shipment through Baltic ports; and 3) the production of amphetamines in places like Poland and their distribution to the West.

Heroin, the illegal narcotic of choice in most of the world and a drug increasing in popularity in the 1990s, received particular attention. NDIE indicated that heroin from Southwestern Asia supplied between twenty and forty percent of the Canadian market in the mid and late 1980s, a rate that rose to 65% in the early 1990s. In 1993, the last year of the estimate, Canadian police seized 154 kilograms of heroin, a 30% increase over seizures in 1992. Record seizures were made in Vancouver and Toronto, which joined Montreal as major centers of heroin trafficking and abuse. The primary heroin entry points into Canada were identified as Halifax, Montreal, Toronto, Winnipeg, and Vancouver.

In the wake of the Cold War, many intelligence agencies redefined their role to include the international drug trade as a major concern along with terrorism and nuclear proliferation. NDIE helped to change the view of the drug trade by identifying it as a global concern that could only be changed by international anti-crime cooperation.

FURTHER READING:

ELECTRONIC:

Lee, James. "Drugs and Drug Trafficking." November 1996. <http://www.parl.gc.ca/information/library/PRBpubs/bp435-e.htm> (April 7, 2003).

Stamler, R.T., R.C. Fahlman and G.W. Clement. "Co-operation Between Canada and Other Countries and Territories to Promote Countermeasures against Illicit Drug Trafficking." United Nations Office on Drugs and Crime Bulletin on Narcotics. January 1, 1987. <http://www.undcp.org/odccp/bulletin/bulletin_1987–01-01_1_page009.htmldamtp.cam.ac.uk/user/gr/public/gal_milky.htm> (April 7, 2003).

SEE ALSO

Canada, Intelligence and Security
Cold War (1972–1989): The Collapse of the Soviet Union

Dual Use Technology

JUDSON KNIGHT

The phrase "dual use technology" refers to tools or techniques, developed originally for military or related purposes, which are commercially viable enough to support adaptation and production for industrial or consumer uses. Examples of dual use technology, for which the United States Department of Defense (DOD) has an entire dedicated program, include capabilities of the U.S. Navy that could be adapted for aviation safety, detecting hazards on the ocean floor, and finding abnormalities in an x ray. As promising as dual-use applications are, their potential for theft or appropriation by hostile powers has led to calls for greater controls over their export.

Armies and Technology in History

A line or argument commonly heard among foes of the military, or of a strong military defense, is that money spent on defense projects could be better used toward improving society by providing jobs, raising the standard of living, and solving daily problems. In fact, four millennia of human experience support the claim that spending on the development of new military technology ultimately serves to benefit society.

Probably the first example of this principle in action is the Egyptian adoption of the chariot, which greatly advanced the technology of transportation in the second millennium B.C. Had it not been for the invasion by the Hyksos in c. 1670 B.C., who dealt the Egyptians a brutal blow with their chariot-equipped cavalry, Egyptian civilization might never have adopted the chariot.

In c. 800 B.C., the Assyrians introduced foundational concepts of logistics—a significant component of modern business, involving the allocation and provision of supplies to meet needs—as part of an effort to supply imperial troops. Two centuries later, the concept of a postal service was introduced as Persian emperors sought to maintain communication with field commanders.

The Romans developed their roads, which ultimately provided the blueprint for the modern superhighway system—itself a concept introduced in the 1950s by President Dwight D. Eisenhower with military needs in mind. In about 100 B.C., Chinese armies began using the wheelbarrow, a piece of technology so vital to the transport of military material that the emperor kept its design a secret for many years.

The list of military technological developments with civilian applications continues right up to the U.S. space program in the late twentieth century, without which modern satellite communication—to name just one example—would not be possible. Satellite technology, in turn, facilitated the military's global positioning system (GPS), today used by civilians for navigation in onboard vehicle systems. Additionally, the U.S. intelligence community and military played a pivotal role in developing the Internet.

The Dual Use Science and Technology Program

In an effort to formalize the interaction between military and civilian technological innovations, DOD established the Dual Use Science and Technology (DU S&T) Program, through which it partners with industry. As DOD officials have noted, there can be commonalities of aim between the need to maintain U.S. technological superiority on the battlefield, and the competitive edge of U.S. industry in the marketplace.

In order to facilitate partnerships, DOD has sought to develop streamlined contracting procedures, and to implement cost sharing between its DU S&T Program, the military services, and industry. The benefits to industry inherent in these partnerships include the leveraging of scarce science and technology funds, access to advanced technology, and the means of developing further beneficial partnerships with other firms, defense laboratories, and university research departments.

In order to qualify as a DU S&T project, an undertaking must have a clearly demonstrable dual use potential, and at least half of the project cost must be underwritten by non-federal participants, of which at least one must be a for-profit company or corporation. Awarding must be based on competitive procedures in compliance with federal regulations for equal opportunity, and projects must meet DOD requirements regarding procurement.

Benefits and risks. A 1999 report in *Naval Forces* provided a number of examples of benefits to be reaped from dual-use programs involving technology developed by a single division of the U.S. Navy, the Naval Undersea Warfare Center (NUWC) in Newport, Rhode Island. During the late 1960s, defense contractor General Electric began developing laser-based listening technology for the detection of quiet-operating submarines at great distances deep beneath the ocean surface. Put on hold at the end of the Cold War, the project had received new life through a partnership between the NUWC Weapons Systems Directorate, Flight Safety Technologies, and Lockheed Martin.

The joint project would have applications for air safety by making it possible for pilots to detect hazards that do not show up on ordinary radar. Among these are the turbulence produced in the wake of large aircraft, forms of clear-air turbulence, wind shear, and microbursts, or sharp downdrafts produced in extreme weather conditions. Because these are not accompanied by rain or hail, radar cannot detect them, but much more discriminating laser beams are capable of "seeing" rather than "hearing" sounds, thus potentially providing advance warning of a disturbance that could cause a plane crash.

Undersea warfare (USW) also makes use of sonar, which could be applied in searching a mammogram x ray for minuscule abnormalities. Such was the focus of a program under development in a partnership between the NUWC Technology Transfer Program, the Weapons Systems Directorate, and the Faulkner Sagoff Center for Breast Health Care in Boston. Another promising partnership was a joint project with Precision Signal Incorporated of Boca Raton, Florida, to produce an imaging unit capable of detecting small objects buried under the sea floor. Called the Ocean Bottom Profiler, the device could be used to detect hazardous materials and other items that have sunk to the bottom of the ocean.

The need for controls. Great advances carry with them a number of potential risks, not least of which is the chance that military innovations may be stolen or appropriated by hostile powers. This reality came to the forefront in the late 1990s, as persons both inside and outside the ranks of the federal government became concerned over alleged efforts by the People's Republic of China to appropriate U.S. military technology for its own purposes. Similarly, concerns were raised as to the use of sophisticated technologies by terrorist groups or terror-sponsoring nations to develop weapons of mass destruction.

"In a perfect world," Commerce Department Undersecretary for Export Administration William Reinsch told reporters in January 1998, "I would have multilateral agreements that would require consensus" before sensitive technologies could be exported. As Reinsch noted, "Right now there is no veto [for the United States], but during the Cold War, if the French wanted to sell something to the Chinese, we could block it."

Reinsch, the senior government official responsible for issuing export licenses on dual-use technologies, was referring to a Cold War-era organization known as COCOM, or the Coordinating Committee for Multilateral Export Controls. When COCOM was in operation, its membership—composed of industrialized democracies—had to reach unanimous agreement before civil or military hardware could be exported to states such as the Soviet Union and the Warsaw Pact nations, China, Cuba, North Korea, more aggressive states in the Middle East, and South Africa under the apartheid regime.

With the end of the Cold War, COCOM had disbanded, and no similar mechanism was in place. In lieu of such agreements, the United States and the nations of Western Europe relied on agreements of mutual consent, but these often broke down in the face of conflicting views as to the threat posed by certain nations. In the case of North Korea, most of the world's advanced nations agreed that it posed a threat, but when it came to Iran—a nation the United States accused of supporting terrorism—U.S. and European views differed. In order to prevent the illegal transfer of dual-use and other sensitive technologies to hostile nations, Reinsch called for an increased vigilance on the part of vendor companies, as well as the tasking of more U.S. agents to monitor potential transfers.

FURTHER READING:

PERIODICALS:

Baus, Theresa. "Dual Use Technology." *Naval Forces* 20, no. 3 (1999): S54–S55.

Muradian, Vago. "Better Export Controls Needed to Check Dual-Use Technologies." *Defense Daily* 198, no. 14 (January 22, 1998): 1.

Palfrey, Terry. "The Hidden Legacy of Scott: Weapons of Mass Destruction and the UK Government Proposals to Control the Transfer of Technology by Intangible Means." *International Review of Law, Computers & Technology* 13, no. 2 (August 1999): 163–181.

Sharke, Paul. "The Start of a New Movement." *Mechanical Engineering* 124, no. 8 (August 2002): 47–49.

ELECTRONIC:

Dual Use Science and Technology Program. <http://www.dtic.mil/dust/> (April 14, 2003).

SEE ALSO

Information Security
Satellite Technology Exports to the People's Republic of China (PRC)
Technology Transfer Center (NTTC), Emergency Response Technology Program

This page intentionally left blank

E

E-2C

Built by Northrop Grumman and first used by the U.S. Navy in 1964, the E-2C Hawkeye has served as an airborne early warning and command and control aircraft in the Vietnam and Persian Gulf wars, as well as in the war on drugs. It is also in service with five foreign governments. The most distinctive feature of the E-2C, which provides simultaneous air and surface surveillance, is its rotating 24-foot (7.3-m) radar dome above the fuselage.

The first airborne early warning and command and control aircraft was the Grumman E-1 Tracer, which flew

An E-2C "Hawkeye" surveillance plane assigned to the "Wallbangers" of the Carrier Airborne Early Warning Squadron taxis on the flight deck aboard USS *Carl Vinson* after completing a patrol, September 15, 2001. ©REUTERS NEWMEDIA INC./CORBIS.

from 1954 to 1964. In 1964, the navy phased in the E-2 Hawkeye, the first aircraft designed to be carrier-based and serve an all-weather airborne early warning and command and control function. Nine years later, in 1973, Grumman introduced the E-2C model. Over the next three decades, the E-2C underwent five major changes, with the fifth, known as Hawkeye 2000, introduced in October 2001.

Using computerized sensors to provide early warning, the E-2C is a high-wing aircraft whose rotating dome contains stacked antennae. The airflow over and around the dome necessitates the second most distinctive of its design features, a multiple-surface tail unit.

In addition to their service in Vietnam, Hawkeyes directed F-14 Tomcat fighters on combat air patrol during strikes against terrorist-related Libyan targets in 1986. They also directed both land attacks and combat air patrol missions over Iraq during the Persian Gulf War, providing control for the shootdown of two Iraqi MiG-21 fighter jets by carrier-based F/A-18s in the first days of the conflict.

E-2Cs have also served with the Drug Enforcement Administration and other law-enforcement agencies for the interdiction of smuggled drugs. The governments of Egypt, France, Japan, Singapore, and Taiwan have purchased E-2Cs, which are engineered in Bethpage, New York, and produced and modified in St. Augustine, Florida.

■ FURTHER READING:

BOOKS:

Chant, Christopher. *An Illustrated Data Guide to Modern Reconnaissance Aircraft.* London: Tiger Books International, 1997.

Hardy, M. J. *Sea, Sky, and Stars: An Illustrated History of Grumman Aircraft.* New York: Sterling, 1987.

PERIODICALS:

Dietrich, Bill. "Engineering—Here's What You Can Expect Next Century." *Seattle Times.* (December 15, 1992): D1.

Wilson, George C. "Drug-War Radar Picks up a Funding Blip." *Washington Post.* (April 14, 1987): A21.

"Young Defends $13 Billion CVN-21 Development Investment." *Defense Daily* 217, no. 32 (February 19, 2003): 1.

ELECTRONIC:

E-2C Hawkeye. United States Navy Fact File. <http://www.chinfo.navy.mil/navpalib/factfile/aircraft/air-e2c.html> (March 9, 2003).

SEE ALSO

J-STARS
Persian Gulf War

Ebola Virus

■ BRIAN D. HOYLE

The Ebola virus is one of two members of a family of viruses that is designated as the Filoviridae. The name of the virus comes from a river located in the Democratic Republic of the Congo, where the virus was discovered. Although naturally occurring, some public health experts worry that the lethality of the virus makes it an attractive potential bioterrorism agent. Under natural circumstances Ebola induced hemorrhagic fever carriers have such high death rates that their rapid death actually acts to limit the spread of the virus. Deliberate spread of the virus would counteract this natural limiting factor.

The species of Ebola virus are among a number of viruses that cause a disease, hemorrhagic fever, that is typified by copious internal bleeding and bleeding from various orifices of the body, including the eyes. The disease can be swiftly devastating and results in death in over 90 per cent of cases.

To date, four species of Ebola virus have been identified, based on differences in their genetic sequences and in the immune reaction they elicit in infected individuals. Three of the species cause disease in humans. These are Ebola-Zaire (isolated in 1976), Ebola-Sudan (also isolated in 1976), and Ebola-Ivory Coast (isolated in 1994). The fourth species, called Ebola-Reston, causes disease in primates. The latter species is capable of infecting humans but so far has not caused disease in humans. Ebola-Reston is named for the United States military primate research facility where the virus was isolated, during a 1989 outbreak of the disease caused by infected monkeys that had been imported from the Philippines. Until the non-human involvement of the disease was proven, the outbreak was thought to be the first outside of Africa.

The appearance of the Ebola virus only dates back to 1976. The explosive onset of the illness and the underdeveloped and wild nature of the African region of the virus's appearance have complicated the definitive determinations of the origin and natural habitat of Ebola. The source of the Ebola virus is still unknown. However, given that filovirus, which produce similar effects, establish a latent infection in African monkeys, macaques, and chimpanzees, scientists consider the possibility that the Ebola virus likewise normally resides in an animal that lives in Africa. A search for Ebola virus in such primates has so far not revealed evidence of the virus.

Almost all confirmed cases of Ebola from 1976 to 2002 have been in Africa. In the latest outbreak, which has been ongoing since late in 2001, 54 people have died in the Gabon as of February of 2002. In the past, one individual in Liberia presented immunological evidence of exposure to Ebola, but had no symptoms. As well, a laboratory worker

in England developed Ebola fever as a result of a laboratory accident in which the worker was punctured by an Ebola-containing needle.

The Ebola virus produces a high fever, headache, muscle aches, abdominal pain, tiredness and diarrhea within a few days after infecting a person. Some people will also display bloody diarrhea and vomit blood. At this stage of the disease some people recover. But, for most of those who are infected, the disease progresses within days to produce copious internal bleeding, shock and death.

Outbreaks of infection with the Ebola virus appear sporadically and suddenly. The outbreak rapidly moves through the local population and often just as quickly ends. The initial infection is presumable by contact between the person and the animal that harbors the virus. Subsequent person-to-person spread likely occurs by contamination with the infected blood or body tissues of an infected person in the home or hospital setting, or via contaminated needles. The fact that infected people tend to be in more under-developed regions, where even the health care facilities are not as likely to be equipped with isolation wards, furthers the risk of spread. The person-to-person passage is immediate; unlike the animal host, people do not harbor the virus for lengthy periods of time.

The possibility of air-borne transmission of the virus is debatable. Ebola-Reston may well have been transmitted from monkey to monkey in the Reston military facility via the air distribution system, since some of the monkeys that were infected were never in physical contact with the other infected monkeys. However, if the other species of the virus are capable of similar transmission, this has not yet been documented. Laboratory studies have shown that Ebola virus can remain infectious when aerosolized. But the current consensus is that airborne transmission is possible but plays a minor role in the spread of the virus.

In the intervening years between the sporadic outbreaks, the Ebola virus probably is resident in the natural reservoir.

Currently there is no cure for the infection caused by the Ebola virus. However, near the end of an outbreak of the virus in 1995 in Kikwit, Africa, blood products from survivors of the infection were transfused into those actively experiencing the disease. Of those eight people who received the blood, only one person died. Whether or not the transfused blood conveyed protective factor was not ascertained. A detailed examination of this possibility awaits another outbreak.

The molecular basis for the establishment of an infection by the Ebola virus is still also more in the realm of proposal than fact. One clue has been the finding of a glycoprotein that is a shortened version of the viral constituent in the in the circulating fluid of humans and monkeys. This protein has been suggested to function as a decoy for the immune system, diverting the immune defenses from the actual site of viral infection. Another immunosuppressive mechanism may be the selective invasion and damage of the spleen and the lymph nodes, which are vital in the functioning of the immune system.

The devastating infection caused by the Ebola virus is all the more remarkable given the very small size of the viral genome, or complement of genetic material. Fewer than a dozen genes have been detected. How the virus establishes an infection and evades the host immune system with only the capacity to code for less than twelve proteins is unknown.

FURTHER READING:

BOOKS:

Cormican, M. G. and M. A. Pfaller. "Molecular Pathology of Infectious Diseases," in *Clinical Diagnosis and Management by Laboratory Methods,* 20th ed. Philadelphia: W. B. Saunders, 2001.

PERIODICALS:

Peters, C. J., and J. W. LeDuc. "An Introduction to Ebola: The Virus and the Disease." *The Journal of Infectious Diseases* no. 179 (Supplement 1, February 1999): ix–xvi.

ELECTRONIC:

Centers for Disease Control. "Ebola Hemorrhagic Fever." 2001. <http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/ebola.htm> (March 12, 2003).

———. "Viral Hemorrhagic Fevers." 2000. <http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/vhf.htm> (March 12, 2003).

SEE ALSO

Biological Warfare
Biological Weapons, Genetic Identification
Bioshield Project
Bioterrorism
CDC (United States Centers for Disease Control and Prevention)
Hemorrhagic Fevers and Diseases
Viral Biology

E-Bomb

An e-bomb, or electronic bomb, is a non-explosive artillery shell that sends out an electromagnetic pulse (EMP) of enormous power, capable of permanently disabling mechanical and electronic systems. The concept developed in the 1920s, and was later recognized as an unintended consequence of nuclear explosions. By the beginning of the twenty-first century, United States and British scientists had the technology to develop e-bombs. At the same time, some observers warned that terrorists might be capable of building their own, much less sophisticated, devices for a fraction of the cost to a superpower.

Carbon-graphite coils capable of generating an electromagnetic pulse used to destroy electronics equipment—especially communications equipment—can be fitted to cruise missiles. Carbon-graphite equipped cruise missiles were used by U.S.-led forces in raids on Baghdad, Iraq in 1991 and in 2003.

The Compton Effect and its consequences. In 1925, American physicist and future Nobel laureate Arthur H. Compton demonstrated that when a string of subatomic energy packets called photons were fired into atoms with a low atomic number—that is, atoms with a relatively small number of protons in their nuclei—the atoms would eject electrons. This phenomenon, known as the Compton effect, is the principle underlying the e-bomb. If enough atoms eject enough electrons, which have a negative electric charge, the result is a massive electromagnetic pulse.

In 1958, when the United States conducted nuclear tests high above the Pacific Ocean, the explosions sent out bursts of gamma rays, extremely high-frequency electromagnetic waves. These collided with nitrogen and oxygen, which are the two most abundant elements in the atmosphere, and which both have very low atomic numbers—7 and 8 respectively. The result was an electromagnetic event whose effects were felt thousands of miles away. Street lights in Hawaii were blown out, and radio navigation as far away as Australia was interrupted for up to 18 hours.

Recognizing that these powerful EMPs were a by-product of nuclear explosions, American and allied scientists set out to harden the defenses of U.S. and NATO (North Atlantic Treaty Organization) electronic systems against disruption from nuclear explosions. Still, as long as the threat of thermonuclear exchange remained real during the Cold War, the EMPs themselves seemed a relatively insignificant side-effect of nuclear explosions.

Developing e-bombs for the modern battlefield. After the Cold War ended, physicists began to explore the use of EMPs as a high-tech weapon to yield a low-tech result: the complete devastation of an enemy's engines, telecommunications, and electronic systems by means of vast energy surges that, by overloading those systems, would render them permanently inoperable. Alarmed by news of Russian advances in the development of an e-bomb in 1998, Western scientists stepped up efforts to create their own e-bomb technology.

In 2000, British scientists announced the development of an e-bomb that could be fired from a long-range 155 mm. artillery gun or multiple-launch rocket system. U.S. scientists developed their own version, which was ready for use in the 2003 mobilization against Iraq. Military leaders leaned against using it, however, precisely because of the bomb's capabilities such as demobilizing hospitals and emergency services. Furthermore, in rebuilding an economy, the devastation of infrastructure caused by an e-bomb could create prohibitive costs. However, for a terrorist organization less concerned with moral and practical compunctions, an e-bomb could be an attractive tool for creating vast destruction at a low cost.

FURTHER READING:

PERIODICALS:

Jenkins, Sally. "Peaceful Games, Cold War Sentiment." *Washington Post.* (February 25, 2002): D1.

Sample, Ian. "Just a Normal Town...." *New Scientist* 167, no. 2245 (July 1, 2000): 20.

Squeo, Anne Marie. "Leading the News: U.S. Studies Using 'E-Bomb' in Iraq—Electromagnetic Weapon Can Permanently Damage Telecom, Power Systems." *Wall Street Journal.* (February 20, 2003): A3.

Wilson, Jim. "E-Bomb." *Popular Mechanics* 178, no. 9 (September 2001): 50–53.

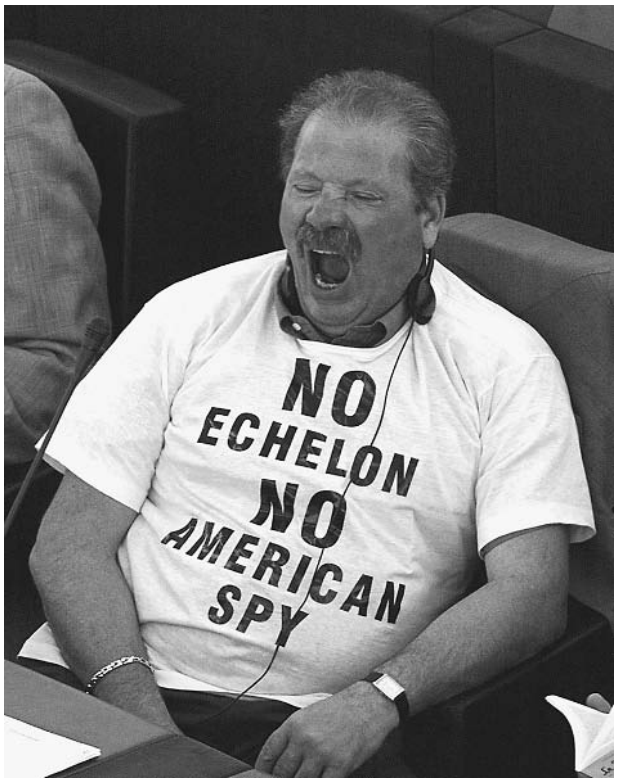
SEE ALSO

Electronic Warfare
Microwave Weaponry, High Power (HPM)

Echelon

Echelon is the name for a global surveillance network consisting of ground stations, satellites, and other listening posts, which collectively intercept and analyze worldwide electronic communications. The signals intelligence agencies of five nations—the National Security Agency (NSA) of the United States, the Government Communications Headquarters (GCHQ) of the United Kingdom, the Communications Security Establishment (CSE) of Canada, the Defense Signals Directorate (DSD) of Australia, and the Government Communications and Security Bureau (GCSB) of New Zealand—all participate, with NSA as the controlling agency. Beginning in 1998, the governments of the European continent expressed increasing outrage over Echelon. However, their efforts to monitor their own citizens' communications suggest that this anger is not so much because Echelon exists at all, but because it is not under European control.

In 1943, the United States and United Kingdom signed the Brusa (British-U.S.A.) Agreement, which established a framework for the exchange of signals intelligence (SIGINT) between the two nations. Three years later, with the war over, the two signed the UKUSA (U.K.-U.S.A.) agreement of March 5, 1946, which brought together then SIGINT efforts of British, American, Canadian, Australian, and New Zealand intelligence. Each UKUSA nation had its own geographic spheres of influence, matched with its listening posts in certain parts of the globe, but the most powerful of the five nations—the United States—remained the unquestioned first among equals. In later years, a



Italian Eurodeputy Roberto Felice Bigliardo wears a t-shirt protesting against the U.S. communications surveillance system Echelon during debates in the European parliament in Strasbourg 05 July 2000. ©AFP/CORBIS.

number of other countries, including Denmark, Germany, Norway, and Turkey, signed "third-party" agreements of participation in the UKUSA network.

Over the years, there emerged a network of listening posts and satellites intercepting cables, telephone communications, radio and microwave signals, wireless communications, e-mail, faxes, and other forms of communication traffic. Almost nothing was immune from the system that came to be known as Echelon, whether a telegram sending birthday greetings to a child in Great Britain, or walkie-talkie communications between East German guards on the Berlin Wall. UKUSA participants were forbidden by law from intercepting communications that originate and terminate in their own countries, but the exchange of information between intelligence services effectively rendered these prohibitions moot. Perhaps NSA, for instance, could not monitor communications within the United States, but GCHQ could with impunity, and it was a simple matter to pass this information on to NSA.

The Echelon system seems to have emerged in something like its present form, though at a much less advanced technological stage, during the early 1970s. In the late 1960s, as NSA and GCHQ geared up for the use of satellites on a grand scale, U.S. and British leadership began to recognize the need for interception and processing sites. The first ground station in what came to be known as Echelon was established at Morwenstow, Cornwall, in England, using two large dish antennae to intercept communications across the Atlantic and Indian oceans. Soon NSA built another such station at Yakima, Washington, to intercept communications across the Pacific. Other sites followed, among them Menwith Hill in England, Stanley Bay in Hong Kong (dismantled and moved to Australia prior to the Chinese takeover in 1997), and Sugar Grove in West Virginia.

The technology of Echelon. Echelon has its own security compartments: SECRET SPOKE instead of CONFIDENTIAL, UMBRA GAMMA instead of SECRET, and TOP SECRET UMBRA instead of TOP SECRET, a compartment that it trumps for level of secrecy and security classification. Echelon also long ago developed its own wide-area network (WAN), much like the public Internet today, only this network is completely inaccessible to public traffic.

The Echelon wide-area network includes an intelligence news network known as Newsdealer, a TV conference system called Giggle, and other components. E-mail and Web pages have an appearance very much like those of their counterparts in the ordinary world, but again, the similarity ends at the superficial resemblance. Through a system known as Intelink, analysts can browse pages on NSA's server and select specific geographic areas from which to obtain products ranging from video clips and satellite photos to intelligence and status reports, as well as databases.

Dictionaries. As the targets of Echelon eavesdropping have evolved—from cable traffic and land-line telecommunications to cell-phone traffic and e-mails—so have its tools. These include not only satellites, but also computers for filtering traffic to extract relevant data.

Once this was a painstaking process, with analysts surveying reams of sheets by hand, marking them for specific items of intelligence. Today, computers do most of this work, thanks to systems known as dictionaries—a computer programmed to scan data for specific terms and keywords.

Echelon dictionary computers around the world scan the traffic under their purview, not only for their own keywords, but also for those of other agencies. In time, keyword searches may be replaced by the more efficient method of topic analysis, which employs principles similar to those of "fuzzy logic" in an effort to better replicate the selection process that the human itself undergoes, albeit at a much slower rate.

Outrage over Echelon. It has been estimated that for a million inputs (a single phone call being an example of an input), Echelon's dictionaries eliminate all but 6,500 as unimportant. Of these, only 1,000 meet the criteria for forwarding them to analysts, who typically select only 10 for closer

study. From these 10, only one warrants the production of an intelligence report. These statistics tend to suggest that, though civil libertarians and others may be outraged over the existence of a system such as Echelon, NSA is really not interested in listening in on most people's phone conversations. It simply sifts through 99.9999 percent of the communication taking place in the world at any given time so as to winnow out the 0.0001 percent that warrants its attention.

Still, concerns about Echelon motivated Margaret "Peg" Newsham, a former computer systems analyst, to release the first reports about the system in 1988. During the early 1990s, New Zealand journalist Nicky Hager painstakingly researched the system to produce his 1996 book *Secret Power,* and in the late 1990s, respected U.S. intelligence writer Jeff Richelson studied Echelon. The European Union also published a report on Echelon in 2001, in which it called on European citizens to encrypt their e-mails as a means of protecting them from snooping by the intelligence services of the English-speaking countries. At the same time, the European Union was considering proposals to require Internet service providers and telecommunications companies to record all their customers' communications and archive them for at least a year—a measure that suggests the UKUSA countries do not have the monopoly on snooping in the liberal democratic world, much less in the world as a whole.

FURTHER READING:

BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

Best, Richard A. *Project Echelon: U.S. Electronic Surveillance Efforts.* Washington, D.C.: Congressional Research Service, 2000.

Hager, Nicky. *Secret Power.* Nelson, New Zealand: Craig Potton, 1996.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

PERIODICALS:

Auer, Catherine. "EU Knocks Echelon, Wants Own Super Spy." *Bulletin of the Atomic Scientists* 57, no. 5 (September/October 2001): 11.

Evers, Joris. "U.S. Spy Technology Failed to Signal Attack Planning." *InfoWorld* 23, no. 38 (September 17, 2001): 28.

Melloan, George. "Civil Liberties Give Way to the Search for Terrorists." *Wall Street Journal.* (October 23, 2001): A27.

Poole, Patrick. "'Echelon' Spells Trouble for Global Communications." *Privacy Journal* 25, no. 11 (September 1999): 3–4.

ELECTRONIC:

Campbell, Duncan. Inside Echelon. <http://www.heise.de/tp/english/inhalt/te/6929/1.html> (March 24, 2003).

Easton, Gary. British Broadcasting Corporation News. <http://news.bbc.co.uk/1/h1/world/americas/1577313.stm> (March 24, 2003).

SEE ALSO

COMINT (Communications Intelligence)
Information Warfare
NSA (United States National Security Agency)
Satellites, Spy
Security Clearance Investigations
SIGINT (Signals Intelligence)
Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom
United Kingdom, Intelligence and Security

Economic Espionage

JUDSON KNIGHT

Economic espionage, sometimes known as industrial espionage, is spying conducted for the benefit of a commercial or industrial enterprise, typically to gain information not available through open channels. (By contrast, economic intelligence conducted on behalf of governments usually draws on information available through open channels.) Technologically advanced nations such as the United States are most vulnerable to economic espionage, which threatens hundreds of billions of dollars in U.S. economic losses to industry. In an attempt to curb industrial and commercial spying, Congress in 1996 passed the Economic Espionage Act, but challenges to U.S. companies have continued.

Vulnerabilities. According to a 1999 report delivered by the American Society for Industrial Security (ASIS) to the Federal Bureau of Investigation (FBI), some $300 billion worth of U.S. intellectual property was directly threatened by industrial espionage in 1997 alone. The ASIS noted more than 270 individual cases of theft and attempted theft involving commercial information. In 2000, the ASIS estimated that each year, losses and potential losses from economic espionage cost American industry more than $60 billion each year. Of 1,300 companies surveyed by the ASIS, fully 1,100 reported that they had been the targets of economic espionage.

Just as the most highly industrialized nations are the obvious potential victims of economic espionage, emerging industrial powers and their economic firms are often the most likely perpetrators. Such is the case with China, which figured in a number of news reports involving economic espionage during the 1990s and early 2000s.

In November, 2001, for instance, the FBI learned of an attempt by individuals operating a Chinese corporation to

Pen Yen Yang, pictured, was among the first to be convicted of economic espionage under the Economic Espionage Act of 1996, which banned the theft of trade secrets. AP/WIDE WORLD PHOTOS.

steal information from Transmeta, a computer hardware company in California's Silicon Valley. According to an affidavit submitted by the FBI to the U.S. District Court in San Jose, Transmeta employee Fei Ye had partnered with fellow Chinese nationals Sun Li and Ming Zhong in a company called Supervision Incorporated. Backing the company, created to develop high-speed, high-performance computer processors, was the Chinese government, according to the FBI.

America is certainly not the only victim of economic espionage. In 2003, for instance, Swedish authorities expelled two Russian diplomats accused of spying at Ericsson, a manufacturer of radar and missile-guidance systems for Sweden's principal strike warplane, the Gripen fighter jet. Nor are the nations involved in spying always inferior technological powers, such as Russia or China; the United States has on several occasions been the target of economic espionage by high-quality producers of technology, including Japan, France, and Israel.

Spying by technological competitors. Despite the close relationship between the United States and Japan in matters of national defense, the Central Intelligence Agency (CIA) estimated in 1987 that 80 percent of Japanese intelligence-gathering activities were directed toward U.S. industry, particularly in high-tech and computer-related fields. U.S. military contractor Recon/Optical in 1992 accused Israel of attempting to appropriate a design for an airborne spy camera, and after lengthy legal wranglings, the Israelis agreed to settle out of court.

In 1993, the CIA warned U.S. aircraft manufacturers to be on the lookout for French spies at the Paris Air Show, and intelligence officials have claimed that France regularly sponsors the theft of information from U.S. companies. A French intelligence official defended his country's efforts in economic espionage with a public statement to the effect that spying in the modern world is primarily directed toward "economic, scientific, technological, and financial" objectives.

U.S. spying. Responding to these and other accusations, the French in 1995 accused a CIA operative of attempting to obtain classified information from an official of their government. Under the leadership of Admiral Stansfield Turner in the late 1970s and early 1980s, the CIA regularly sponsored Commerce Department briefings at which U.S. corporate executives received information on developments in semiconductor and aircraft technology by foreign powers. American authorities continued to deny the French charges in the mid-1990s. For the most part, the leading technology is in America. While U.S. intelligence has a powerful motivation to keep tabs on the activities of foreign technological concerns, the purpose is primarily defensive, because the United States and its companies have less to gain by stealing from overseas.

Protecting U.S. technology. By the same token, U.S. companies are vulnerable to foreign competitors—and to one another. For this reason, the federal government has put in place a number of mechanisms to protect American industry. One of these is the CIA, which monitors potential cases of economic espionage against U.S. companies by foreign concerns. If the CIA uncovers information regarding possible criminal activity such as bribery, it turns this over to the FBI. Additionally, the National Security Agency (NSA), despite the high levels of secrecy involving its activities, sometimes passes on information to the FBI, which notifies threatened companies using documentation that leaves out sensitive NSA information.

The Office of the National Counterintelligence Executive (NCIX), formerly known as the National Counterintelligence Center (NACIC), coordinates and distributes information on economic espionage gained by intelligence. NCIX distributes this information to targeted U.S. companies on an as-needed basis. The U.S. State Department monitors information on economic espionage through its Bureau of Intelligence and Research (INR), and keeps U.S. companies informed of threats by means of its Overseas Security Advisory Council electronic bulletin board.

To provide further protections for U.S. companies, Congress in 1996 passed, and President William J. Clinton

signed into law, the Economic Espionage Act. The act makes it a federal crime to use unauthorized means to obtain any trade secret whose transfer to other parties would cause economic harm to its lawful owner. "Unauthorized means" include the use of undercover employees, pretexts, and the development of confidential informants in order to obtain trade secrets. The act does not address the gathering of information through open sources.

Despite the many efforts of the federal government to protect sensitive trade, industrial, and commercial information, the first and often the best line of defense still lies with the company itself. In order to protect assets from economic espionage, a 2003 report in *Security* recommended that employees be educated, and technology implemented, so as to track proprietary information. The report also recommended a "cultural approach" to security, meaning that companies should recognize the leading role played by people and processes, and not simply address information and facility security from a technological standpoint.

To better protect against economic espionage, according to the *Security* report, a number of steps must be taken, beginning with the often-overlooked measure of conducting an evaluation. During this process, company security personnel should review work practices, identity the most sensitive compartments of information, and note the points and areas at which allegedly secure information is transferred. The company should invest in security technology only after this review, which will assist it in best targeting funds for security.

■ FURTHER READING:

PERIODICALS:

Carr, Chris, Jerry Furniss, and Jack Morton. "Complying with the Economic Espionage Act." *Risk Management* 47, no. 3 (March 2000): 21–24.

Jeffrey, Terence P. "Two Silicon Valley Engineers Indicted for Economic Espionage Aiding China." *Human Events* 59, no. 2 (January 13, 2003): 1.

Joyce, Jim. "Espionage Battleground." *Security* 40, no. 1 (January 2003): 24–25.

Nasheri, Hedieh, and Timothy J. O'Hearn. "High-Tech Crimes and the American Economic Machine." *International Review of Law, Computers & Technology* 13, no. 1 (March 1999): 7–19.

Wolkowitz, Dave. "Facility Security—Playing It Safe." *Area Development Site and Facility Planning* 37, no. 9 (September 2002): 72.

SEE ALSO

Chinese Espionage Against the United States
Counter-Intelligence
Economic Intelligence
Facility Security
NCIX (National Counterintelligence Executive), United States Office of the
Satellite Technology Exports to the People's Republic of China (PRC)
Technical Intelligence

Economic Intelligence

■ MARTIN J. MANNING

Economic intelligence can be loosely defined as information gathered about materials and resources that are developed, produced, or managed outside the United States, and the interpretation and presentation of raw information or unpublished data to reports or analyses that inform policy makers and consumers.

Background. The importance of economic intelligence first surfaced in 1776 when the Committee of Secret Correspondence of the Continental Congress, considered the first U.S. intelligence agency, sent William Carmichael to Europe to survey several economic matters crucial to the emerging government, such as foreign competition in European markets from tobacco grown in the Ukrainian provinces of the Russian Empire. In his secret dispatch (November 1776) from Amsterdam, Carmichael reassured his superiors that, despite the fears that "the Ukraine would supply Europe with tobacco," the best that he saw "is worse than the worst of our ground leaf."

During World War I, an economic intelligence section, within the Army's military intelligence operation, was headed by a future U.S. Secretary of State John Foster Dulles. When this war ended, and President Wilson was preparing for the Versailles Peace Conference, he consulted private experts, the "Inquiry," which gathered economic intelligence from its headquarters at the American Geographical Society, New York.

In World War II, U.S. government agencies, such as the Board of Economic Warfare, studied the Japanese economy while the Office of Strategic Services (OSS) collected information on key commodities, including tungsten; its Russian division, directed by economic experts Abram Bergson and Wassily Leontief, targeted appraisals of the Soviet Union's postwar economic condition.

Post-World War II. In 1945, OSS was abolished; its successor, Central Intelligence Group (CIG), coordinated economic intelligence. Its June 1946 report gathered intelligence on foreign industrial establishments and foreign petroleum extraction, compiled comprehensive geographic information, and utilized the services of its foreign officers to gather data on strategic minerals.

When the Central Intelligence Agency (CIA) was established as part of the National Security Act of 1947, its role to monitor national intelligence, by coordinating the information collected by the various departments of government, was supplemented by a 1949 recommendation of a review group that the CIA create an Office of Research Reports (ORR) to collect and examine economic information.

In National Security Council Intelligence Directive No. 15, *Coordination and Production of Foreign Economic Intelligence* (June 13, 1951), CIA was given responsibility to determine the overall requirements of foreign economic intelligence, to evaluate foreign economic data of significance to national security issues, and to conduct "such foreign economic research and produce such foreign economic intelligence" as required to supplement work being done by other agencies. A year later, Director of Central Intelligence, Walter B. Smith, informed the NSC that the ORR was releasing accurate appraisals of an "enemy's economic potential" and that an interdepartmental Economic Intelligence Committee to establish priorities and publish interdepartmental economic estimates, was in place, chaired by the ORR assistant director.

The allocation of responsibility for economic intelligence over the next 20 years shifted between the CIA and the Department of State. Both worked closely together during the Truman administration when the State Department produced economic intelligence on countries outside the Sino-Soviet Bloc while CIA compiled economic intelligence on the Sino-Soviet Bloc. By 1955, the CIA Office of Research Reports was generally credited with composing the first good pictures of Soviet economic capabilities, including its transport system, current production, and plant capability. This analysis was relied upon by the Kennedy administration.

During the 1960s, the CIA became the government's leading provider of economic intelligence as it expanded its economic analysis to "Free World" economies, especially to examine Soviet bloc economic activity in the developing world. After State's Bureau of Intelligence and Research, hurt by shrinking budgets, cut the majority of its economic research to maintain its expertise for political analysis, CIA supplied regular economic inputs to national intelligence documents and picked up substantial new demands from policy makers, especially for information on developing countries.

By 1968, the CIA replaced ORR with the Office of Economic Research but the CIA's overall importance in the provision of economic intelligence lessened during the Reagan Administration for several reasons: the U.S. Department of the Treasury and the Federal Reserve Board improved their monitoring of international financial issues; new competition came from the highly sophisticated technology of international economic analysis available from the private sector; the international financial institutions, such as the International Monetary Fund (IMF) and the World Bank, supplied their own economic expertise; and a variety of on-line services, newspapers and trade publications made a vast amount of data available to non-government subscribers.

The exact role of economic intelligence remains a widely debated issue. According to Dr. Mark Lowenthal, Senior Specialist in U.S. Foreign Policy, Congressional Research Service, Library of Congress, in testimony before the U.S. Senate's Select Committee on Intelligence, August 5, 1993, no one questions the importance of economic issues but there is "no broad consensus" about the Intelligence Community's proper role in it. He noted that the issue has been oversimplified by calls for "more economic intelligence" unsupported by any "knowledge of long standing activities in that area or of the likely utility of these intelligence activities and products to economic problems or issues." Lowenthal argues that no persuasive case has yet been made that "U.S. economic competitiveness requires large-scale aid from the Intelligence Community."

Types of information. There are three main sources of economic intelligence. The first, open sources, range from official statistical publications, newspapers, radio broadcasts, and trade publications to IMF country studies. Unclassified sources generally constitute the foundation of any economic analysis, an interpretation of the overall picture.

The second are the reports and cables from U.S. embassies and consulates, compiled by State Department economic officers, Treasury Department attachés, and officers of the Foreign Commercial Service.

The third, clandestine information, is obtained without either the knowledge or consent of foreign governments. It can come from satellites, from intercepted communications, or from secrets stolen by a foreign national employed by the United States.

Present situation. The CIA, assisted by other government agencies, provides economic intelligence for U.S. policy, with experts monitoring international transactions (including sanctions enforcement and illicit finance); international economic and environmental problems, including trade and finance; defense markets and logistics; geographic resources, including demographics and commodities; civil technology, including aerospace, advanced manufacturing, and emerging technologies; and energy resources. However, critics feel that American companies don't need the CIA to compete in the global marketplace. The glut of information (sometimes too much information) coming from the Internet, private citizens, groups and organizations with access to foreign economic activities, and subscriber services, such as *The Economist's* Economic Intelligence Unit (EIU) databases, complement and sometimes replace official channels.

Resources. The official record of economic intelligence in U.S. economic diplomacy is in the Foreign Relations of the United States series volumes compiled by the Office of the Historian, U.S. Department of State; published by the Government Printing Office. Beginning with 1944: vol. II; *General: Economic and Social Matters* (Washington: GPO, 1967), individual volumes have dealt with U.S. economic policy.

An excellent introduction to the history of U.S. economic intelligence is: Philip Zelikow, "American Economic Intelligence: Past Practice and Future Principles," *Intelligence and National Security* 12, no. 1 (January 1997):164–177. I am indebted to Mr. Zelikow's research for providing background for this essay.

FURTHER READING:

BOOKS:

Katz, Barry M. *Foreign Intelligence and Research and Analysis in the Office of Strategic Services, 1942–1945.* Cambridge, MA: Harvard University, 1989.

U.S. Congress. Senate. Select Committee on Intelligence. *Economic Intelligence. Hearing, 103d Congress, 1st Session.* Washington, D.C.: GPO, 1994.

PERIODICALS:

Ernst, Maurice. "Economic Intelligence in CIA," *Studies in Intelligence* 28, no. 4 (Winter 1984): 1–16.

SEE ALSO

Economic Espionage

Egypt, Intelligence and Security

Egypt's primary intelligence agency is the General Directorate for State Security Investigations (GDSSI). The Ministry of the Interior administers the GDSSI. The agency collects both foreign and domestic intelligence, using civilian and military operatives and resources. The GDSSI maintains several operational departments and partner agencies, including the Counterintelligence Branch, the Department for Combating Religious Activity, Directorate of State Security Investigations, and a security action unit. The agency cooperates with military and foreign intelligence services in operations intended to protect national interests, especially relating to shipping, oil production, and refinement, and regional anti-terrorism measures. The organization has received criticism from human rights groups and members of the international community for its employment of harsh coercion techniques and conducting espionage on Egyptian citizens.

The government and the individual branches of service coordinate military intelligence. The organization assesses threats to national targets and actively protects military instillations. Operations of the Intelligence Agency are classified.

While Egypt has cooperated with European and American anti-terrorist operations in the past, a recent political shift has prompted Egyptian authorities to withdraw from many Western intelligence and security efforts in North Africa and the Middle East. The rise of Islamist sects and terrorist groups in the region, as well as Egypt's close ties to neighboring Arab states, creates further diplomatic tensions with Europe and the United States. Although Egyptian intelligence agencies aided the United States intelligence community by providing information about the Al-Qaeda terrorist network, many in the Egyptian government opposed the United States led war in Afghanistan in 2001. Regardless, Egypt continues a liberal-use policy of its territorial waters for international shipping, including access to the Suez Canal.

The Egyptian Constitution prohibits religious political parties, but over the past decade, a few Islamist militant organizations have gained some political ground. In the 1990s, Egyptian and United States intelligence forces conducted operations to locate and capture Egyptian militants who had fled the country and were basing possible anti-government and terrorist operations abroad. The two nations successfully captured several suspects, but the Egyptian government garnered international criticism for human rights abuses, including poor treatment of the prisoners and the use of secretive military tribunals.

SEE ALSO

Enduring Freedom, Operation
Terrorism, Intelligence Based Threat and Risk Assessments

Eichmann, Adolf: Israeli Capture

ADRIENNE WILMOTH LERNER

Karl Adolf Eichmann (1906–1962) was the head of the German Gestapo Department of Jewish Affairs from 1941 to 1945. During World War II, Eichmann oversaw the deportation of European Jews to ghettos. In 1942, he organized the Wansee Conference, a meeting of Nazi officials to devise the "Final Solution," the Nazi euphemism for the extermination of European Jews. Eichmann supervised the creation and operation of death camps, and set Nazi policy on the seizure of Jewish property. Immediately following the war, he was identified as one of the primary Nazi war criminals sought by international law enforcement and intelligence agencies.

After his arrest and escape from an American internment camp in 1946, Eichmann assumed a variety of pseudonyms and moved throughout Europe, never contacting his family. British and American intelligence searched for Eichmann for a few months, but as the Nuremberg Trials of other Nazi war criminals began, the focus of attention shifted from Eichmann and other escapees. The onset of

German Gestapo officer Adolf Eichmann listens to the guilty verdict read by the presiding judge as he stands in a bullet-proof glass enclosure in a Jerusalem court in 1961, during his trial for committing wartime atrocities against Jewish Europeans. AP/WIDE WORLD PHOTOS.

the Cold War further distracted the hunt for Nazi fugitives. Eichmann hid throughout Europe until 1950, before fleeing to Argentina with the aid of Nazi sympathizers. Once in South America, Eichmann sent for his family to join him. They eluded the authorities in Britain, Germany, and Israel who continued the search for various perpetrators of the Holocaust. It was through clues left by Eichmann's family, namely his sons Nikolas and Dieter, that authorities finally located Eichmann.

Finding Eichmann. During this time, Eichmann lived under the false name of Ricardo Klement, which he had taken when he escaped Europe. His sons, however, sometimes used the family name of Eichmann. In 1957, Eichmann's son Nikolas became involved with an Argentinean girl named Sylvia. Not knowing that the girl was Jewish, Nikolas often made anti-Semitic remarks and boasted of his father's deeds during the war. Nickolas' remarks, coupled with the occasional use of his real last name, made the girl's father suspicious. He contacted a friend in Germany, jurist Fritz Bauer. Bauer, who was imprisoned by the Nazis twice during the war, devoted his life to the location and capture of Nazi war criminals. Bauer notified Israeli authorities with the information.

Though Israel was a new nation, it had already developed a skilled intelligence service. A special unit of that service was called Mossad. The unit was formed to track down and kill enemies of the state, but dedicated its first few decades to the capture of terrorists and war criminals. The head of Mossad, Isser Harel, immediately took charge of the hunt for Eichmann. He chose a special team of 30 agents, several of them survivors of the Holocaust, to assist in the operation. The Israeli government decided that Eichmann should not be assassinated, but brought back to Israel to stand trial. To further complicate the matter, once Eichmann was found, he would have to be kidnapped and smuggled to Israel, a violation of Argentinean legal sovereignty. Because many Nazi sympathizers found refuge in South America during the war, the Israelis knew that a diplomatic extradition would be difficult, if not impossible, to obtain.

The lead that Bauer gave Mossad turned into a dead end. When an agent tried to locate the family, he discovered that Eichmann and his family had moved, with no forwarding address. Another lead surfaced in 1959. One of Bauer's informants in Italy discovered the pseudonym that Eichmann used when he immigrated to South America. Another agent discovered that a gas meter on the house from the first tip still bore the name Klement. Authorities were convinced that the man was Eichmann.

Mossad hatched a simple plan to find Eichmann's new address. Around the time of Nikolas' birthday, Mossad hired an undercover agent to dress as a bellboy and approach Dieter Eichmann with a package that needed to be delivered to his brother, Nikolas. The undercover agent did not know anything else about the mission. Dieter refused to give the bellboy his brother's address, and took the package himself. Prepared for this outcome, the Mossad team sent the undercover agent back to Dieter a few days later. The agent told Dieter that the sender of the package believed that the package was not delivered and demanded that she be paid for its lost contents. Dieter claimed that the package was not delivered to Nikolas because he was confused about the name, Nikolas Klement, which appeared on the box. Dieter further explained that his brother used the surname Eichmann, so he thought the package belonged to his father, Ricardo Klement. Dieter then reluctantly gave the bellboy his father's address, 14, Garibaldi Street, San Fernando . Mossad agents watched the house for several weeks, tracking Eichmann's daily schedule. One evening, the subject believed to be Eichmann stepped off his usual bus carrying flowers. He was greeted at his home by several people who gathered for a party. The day corresponded with Eichmann's wedding anniversary. These facts convinced the Mossad agents that they had positively identified the subject as Adolf Eichmann.

Eichmann's Capture. After locating Eichmann, agents then devised a plan for his capture and kidnapping. The Israeli team saw an opportunity to ferry Eichmann out of the country during the upcoming celebration of Argentina's

100th anniversary of independence. Several Israeli diplomats were invited to the celebration and would arrive on a specially chartered El Al flight. Agents knew Eichmann would have to be smuggled aboard this flight. Harel contacted the members of his select team who had remained in Israel awaiting further orders. Each agent was sent to a different city, from which he would depart for Argentina, supposedly to join the national celebrations. A series of safe houses was established. Once in Argentina, the Mossad agents changed locations and rental cars every day to avoid being tracked. On the evening of May 11, 1960, four agents were positioned in two cars near Eichmann's house on Garibaldi Street. They pretended to have car trouble. Eichmann was late getting home that evening, so two of the agents decided to leave. Two agents remained, continuing to occupy themselves with their car engine. At 8:30 in the evening, Eichmann alighted from his usual bus. He walked over the agents' car, offering assistance. The agents quickly overpowered Eichmann, put him in the car, and drove to the safe house.

The Mossad team had to keep Eichmann in their custody for several days until he could be smuggled aboard the departing El Al flight nine days later. He was shackled to his bed in the safe house, but was cooperative with Mossad agents. The team had counted on Eichmann's family not contacting local police. His family contacted several friends, trying to learn of his whereabouts, but none offered any information. They did not call the police for fear of drawing attention to Eichmann's real identity.

On May 20, 1960, Eichmann was slightly drugged and dressed in the uniform of an El Al crewmember. The agents who accompanied Eichmann were similarly dressed. A few days prior to their departure, the Mossad team sent one of their agents to a local doctor pretending to have a brain injury. He was issued a medical certificate for travel noting possible side effects, such as difficulty walking and speaking. The agents changed the name on the certificate to match Eichmann's new pseudonym, providing an alibi for his behavior while drugged.

Mossad was successful in its long mission. Eichmann landed safely in Israel on May 22, 1960. Eichmann stood trial for war crimes and crimes against humanity in Israel from April 2 to August 14, 1961. He was convicted and sentenced to death.

Eichmann was executed on May 31, 1962.

FURTHER READING:

BOOKS:

Aharoni, Zvi, Wilhelm Dietl, Meir Amit, and Helmut Bogler (trans.) *Operation Eichmann: The Truth about the Pursuit, Capture and Trial.* New York: John Wiley and Sons, 1997.

Black, Ian and Benny Morris. *Israel's Secret Wars: A History of Israel's Intelligence Services.* New York: Grove Press, 1992.

Isser, Harel. *The House on Garibaldi Street: The First Full Account of the Capture of Adolf Eichmann.* New York: Viking Press, 1975.

ELECTRONIC:

The Nizkor Project. <http://www.nizkor.com> (November 10, 2002).

SEE ALSO

Gestapo
Mossad
World War II

Eisenhower Administration (1953–1961), United States National Security Policy

CARYN E. NEUMANN

To President Dwight D. Eisenhower, the national security of the United States could best be maintained by an interventionist international policy. Under the guidance of Secretary of State John Foster Dulles, his administration abandoned the Cold War policy of containment that had been adopted by President Harry S. Truman in favor of a two-pronged approach to the communist menace. The U.S. would respond militarily to overt communist aggression while advocating active measures to promote the liberation of countries that had converted to communism. This new policy required a strong military and Eisenhower accordingly increased the production of nuclear weapons as a cost-effective way to meet his administration's goals.

Eisenhower won the presidency in 1952 partly because of his record as one of the military heroes of World War II. As president, he sought to maintain America's global presence as the main deterrence to communist expansion, but he regarded military outlays as unproductive. To Eisenhower, every raw material and skill that served the military did so at the expense of the domestic economy. To meet the needs of a steadily growing population, he sought to devote as few resources as possible to the military. This cost cutting led him to emphasize nuclear weapons because they offered more bang for the buck, in both literal and psychological terms.

Popularly thought to have delegated foreign policy strategy to Dulles, Eisenhower in fact controlled its formulation through the mechanism of the National Security Council (NSC). He created the NSC Planning Board to carry out the strategic planning function, while the Operations Coordinating Board coordinated plans for translating approved national strategy into agency operations.

Dulles commanded day-to-day NSC operations and served as foreign policy spokesman for the administration. In time, Dulles became the sole intellectual wellspring of foreign policy conception at the expense of the policy planning staff. The creation of the Southeast Asia Treaty Organization (SEATO) was his effort at reducing communist dangers in the region.

Upon entering office in 1953, Eisenhower immediately had to confront the stalemated Korean War. His administration informed China that further delays in the truce negotiations would enlarge the scale of the war and that a resumption of full-scale fighting might include the American use of nuclear weapons. The Chinese signed an armistice in July 1953. Conflict with China would dominate much of Eisenhower's presidency as the communists periodically tested American intentions before retreating before military threats.

While the Eisenhower administration generally used propaganda and forms of psychological warfare to peacefully weaken communist influence, it occasionally resorted to violence. The pledge to liberate countries from communism meant that limited means would be used to achieve U.S. aims as long as no danger existed of provoking a Soviet-U.S. war. In 1953, the Central Intelligence Agency (CIA) helped stage a coup in oil-rich Iran to replace nationalist and Cold War-neutral Prime Minister Mohammed Mossadegh with the American-allied Shah of Iran. In 1954, the CIA staged another coup to get rid of Guatemalan President Jacabo Arbenz Guzman, a land reformer who had communists among his supporters but lacked any particular ideological ties to the Soviet Union. The involvement of the American government in both operations quickly became widely known.

In order to head off congressional efforts to study the CIA's covert operations following these two coups, Eisenhower commissioned World War II hero Lt. Gen James Doolittle to study the subject. The 1954 Doolittle Report provided an early justification for covert action against communists by stating that no rules applied when faced with an implacable enemy set upon world domination by whatever means and whatever cost. In 1955, the NSC issued NSC-5412/2 to spell out the goals of covert operations. Such activities were to be designed to create and exploit troublesome problems for communism; discredit the prestige and ideology of communism; counter any communist threat to achieve dominant power in a free world country; reduce communist control over any areas of the world; create a positive image of the U.S.; and develop underground resistance to communism.

Eisenhower left office in 1961. His intelligence-related legacy is a mixed one. In 1975, a Senate committee headed by Frank Church charged that the exposure of covert actions in foreign nations damaged the ability of the U.S. to exercise moral and ethical leadership throughout the world. While the Eisenhower administration succeeded in reducing communist influence in the 1950s, the use of covert operations may have caused damage to the long-term national security interests of the United States.

FURTHER READING:

BOOKS:

Boll, Michael M. *National Security Planning Roosevelt through Reagan.* Lexington: University Press of Kentucky, 1988.

Crabb, Cecil V. and Kevin V. Mulcahy. *American National Security: A Presidential Perspective.* Pacific Grove, CA: Brooks/Cole, 1991.

Lord, Carnes. *The Presidency and the Management of National Security.* New York: The Free Press, 1988.

SEE ALSO

ADFGX Cipher
CIA (United States Central Intelligence Agency)
Cold War (1950–1972)
Korean War
National Security Strategy, United States
NSC (National Security Council)
NSC (National Security Council), History
Nuclear Weapons
President of the United States (Executive Command and Control of Intelligence Agencies)
Truman Administration (1945–1953), United States National Security Policy

Eisenhower Doctrine.

SEE *Cold War (1950–1972).*

El Salvador, Intelligence and Security

El Salvador won its independence from Spain in 1821, and joined the Central American Federation. The nation left the Federation in 1839, establishing its own government. Political rivalry has been endemic in El Salvador, reaching a climax in 1980 when the country erupted in civil war. In 1992, leftist rebel guerrillas and the El Salvadoran government signed a peace treaty. Specified in the agreement were numerous government and military reforms desired by opposition forces. Some of these reforms extended to the El Salvadoran intelligence and security community.

Reforms continue today, but the intelligence community of El Salvador underwent several changes under a program of demilitarization in the 1990s. Secret police and anti-dissident units were abolished, but political espionage remains in practice to a lesser degree.

The main intelligence agency in El Salvador is the *Direccion Nacional Civil* (DNI), National Directorate of Intelligence. The DNI collects and processes both domestic and foreign intelligence information. The agency also coordinates the operations of several smaller intelligence units, including counter-terrorism, counterintelligence, anti-narcotics, and anti-paramilitary forces.

The Ministry of Defense and Public Security manages military intelligence and security forces. Though the army and various militias are responsible for their own strategic intelligence forces, the Ministry of Defense aids in the sharing of information among various agencies, and coordinates large-scale surveillance operations for the C-2, the main military intelligence wing.

The El Salvadoran government also maintains a number of special operations units in the intelligence community. An Anti-Riot Unit (UMO) and the Political Reaction Group (GRP) work with law enforcement to conduct surveillance on anti-government groups and paramilitary organizations. The anti-riot squad has acted as peacekeepers during large protests, and helped stop looting after natural disasters.

As part of its series of reforms, El Salvador legalized the U.S. dollar as official currency, alongside the existing national currency, the colon. The government hopes that the influence of a stronger currency will help the nation recover from the effects of civil war and encourage investment in the region. However, the dual currency also opens the nation to increased financial crimes, including money laundering for drug cartels. Working with neighboring nations, the Organization of American States, and the United Nations, El Salvadoran intelligence forces are acting to combat trafficking and financial crimes related to illegal drugs.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. "Columbia" CIA World Factbook <http://www.cia.gov/cia/publications/factbook/geos/es.html>(April 18, 2003).

Electroactive Polymers and Devices.

SEE *Biological and Biomimetic Systems.*

Electromagnetic Pulse

■ LARRY GILMAN

Any nuclear explosion 25 miles (40 km) or higher above the ground produces a high-altitude electromagnetic pulse (HEMP), a short-lived, overlapping series of intense radio waves that blanket a large swath of ground. These radio waves can induce electrical currents in metallic objects and so cause damage to electrical and electronic equipment, including electrical power grids, telephone networks, radios, and computers. The HEMP produced by a single large (i.e., multi-megaton) nuclear weapon detonated 125 miles (200 km) above the center of the continental United States would affect more than half the country; a weapon detonated at 250 miles (400 km) would affect the entire country, though at lower pulse intensities. Military electronics are often "hardened" against HEMP by enclosures of metal foil and by specialized surge protectors. Civilian systems are not hardened against HEMP.

A typical HEMP consists of a series of overlapping radio pulses, each produced by a different physical aspect of the nuclear explosion. The first, briefest, and most intense component of a HEMP is the prompt gamma signal, which is produced as follows: When a nuclear weapon detonates, large numbers of gamma rays (high-energy photons with wavelengths less than .1 nm) range radiate outward from the burst point. Many of these collide with atoms in the Earth's atmosphere, knocking electrons free. These free electrons are created almost simultaneously in a large volume of the atmosphere surrounding the explosion, and travel rapidly away from the burst point in all directions. Because any charged particle crossing magnetic field lines experiences a force at right angles to its direction of motion, the Earth's magnetic field forces these electrons to follow curved paths, and because charged particles following curved paths emit electromagnetic waves (synchrotron radiation), the explosion-liberated electrons spiraling through the Earth's magnetic field emit a strong radio pulse, namely, the prompt gamma component of the HEMP. Additional pulses, of longer duration but lower magnitude, arrive soon afterward. These are caused by scattered neutrons and gamma rays (radiation that has made one or more bounces, rather than following a straight radial path from the burst point) and by the expansion and ascent of the ionized nuclear fireball through the Earth's magnetic field. The electromagnetic pulse caused by the latter effect, termed the magnetohydrodynamic EMP or HD-EMP, is of low intensity but long duration, and is thought to be a particular threat to power transmission lines.

Although the first nuclear weapon was exploded in 1945, HEMP was unknown to U.S. scientists until July 8, 1962, when a high-altitude nuclear test code-named Starfish was conducted by the U.S. approximately 250 miles (400 km) above the Pacific Ocean, some 800 miles (1280 km) from the Hawaiian island of Oahu. Unexpectedly, some 30 strings of streetlights failed in the island's main town simultaneously with the Starfish explosion. Investigation showed that certain of the lines, randomly oriented so as to pick up the HEMP from Starfish like radio antennae, had absorbed enough energy to blow their fuses. Soviet scientists were probably already aware of HEMP,

because the Soviet Union had already conducted high-altitude tests like Starfish. HEMP subsequently became a central component in strategic nuclear war-simulations; many speculative scenarios for a Soviet first strike on the U.S. began with an EMP "lay-down" created by simultaneously exploding a relatively small number of nuclear weapons at high altitude over the United States. The goal would have been to cause widespread damage to civilian and military electrical and electronics systems at relatively low cost, to be followed by a more devastating ground attack. More recently, some U.S. officials considered a smaller-scale EMP laydown attack on Iraq as a prelude to the Gulf War of 1990. (The attack was not carried out.)

Although some planners have worried that a nation or terrorist group possessing only a few nuclear weapons might use one of them to blanket the U.S. with a damaging HEMP, this is thought by most experts to be unlikely. To create a significant HEMP attack, a weapon must be small enough to be lofted on a ballistic missile, and few countries have the know-how either to make powerful nuclear weapons of such small size or to build ballistic missiles. In any case, it is unlikely that an adversary seeking to cause maximal harm and willing to risk using nuclear weapons against a nuclear-armed adversary such as the U.S. would make a HEMP attack. Any nuclear weapon would cause far more destruction by direct blast (if detonated over or in a city) than by HEMP (if detonated at high altitude).

Besides HEMP, two other forms of electromagnetic pulse may be caused by nuclear explosions. The first is generated inside electronic devices by the passage of ionizing radiation (e.g., neutrons and gamma rays) directly into metallic cases, circuit boards, semiconductor chips, and other components, where it can cause brief electrical currents to flow by knocking electrons loose from atoms. This effect is termed systems-generated electromagnetic pulse (SGEMP). The other form of EMP—source-region EMP or SREMP—occurs when a nuclear weapon explodes at low altitude. In this situation, a highly asymmetric electric field is produced in the vicinity of the burst (e.g., within a radius of 3–8 km) having intensities that are much greater than those produced by HEMP. Since the region affected by SREMP corresponds to that effected by the nuclear blast itself, SREMP is relevant only to the defense of hardened targets such as buried missile silos, which are intended to remain functional even in the aftermath of a near-surface nuclear blast.

Carbon-graphite coils capable of generating an electromagnetic pulse used to destroy electronics equipment—especially communications equipment—can be fitted to cruise missiles. Carbon-graphite equipped cruise missiles were used by U.S.-led forces in raids on Baghdad, Iraq in 1991 and in 2003.

Scientists at Lawrence Livermore National Laboratory reportedly developed an HPM weapon for the Department of Justice: aimed at a moving vehicle, the HPM could shut off the electronic ignition, thus bringing a high-speed car chase to an abrupt end.

FURTHER READING:

BOOKS:

"Electromagnetic Pulse Threats to U.S. Military and Civilian Infrastructure." Hearing Before the Military Research and Development Subcommittee of the Committee on Armed Services, U.S. House of Representatives, Oct. 7, 1999 (H.A.S.C. No. 106–31). Washington, DC: U.S. Government Printing Office, 2000.

PERIODICALS:

Kruse, V. J., et al. "Impacts of a Nominal Nuclear Electromagnetic Pulse on Electric Power Systems: A Probabilistic Approach." *IEEE Transactions on Power Delivery.* (Vol. 6, No. 3, July 1991): 1251–1263.

SEE ALSO

Nuclear Weapons

Electromagnetic Spectrum

LARRY GILMAN

The electromagnetic spectrum consists of all the frequencies at which electromagnetic waves can occur, ordered from zero to infinity. Radio waves, visible light, and x rays are examples of electromagnetic waves at different frequencies. Every part of the electromagnetic spectrum is exploited for some form of military, security, or espionage activity; the entire spectrum is also key to science and industry.

Basic Physics

Electromagnetic waves have been known since the mid-nineteenth century, when their behavior was first described by the equations of Scottish physicist James Clerk Maxwell (1831–1879). Electromagnetic waves, according to Maxwell's equations, are generated whenever an electrical charge (e.g., an electron) is accelerated, that is, changes its direction of motion, its speed, or both. An electromagnetic wave is so named because it consists of an electric and a magnetic field propagating together through space. As the electric field varies with time, it renews the magnetic field; as the magnetic field varies, it renews the electric field. The two components of the wave, which always point at right angles both to each other and to their direction of motion, are thus mutually sustaining, and form a wave which moves forward through empty space indefinitely.

The rate at which energy is periodically exchanged between the electric and magnetic components of a given electromagnetic wave is the frequency, ν, of that wave and

has units of cycles per second or Hertz (Hz); the linear distance between the wave's peaks is termed its wavelength, λ, and has units of length (e.g., meters). The speed at which a wave travels is the product of its wavelength and its frequency, $V = \nu\lambda$; in the case of electromagnetic waves, Maxwell's equations require that this velocity equal the speed of light, c (>186,000 miles per second [300,000 km/sec]). Since the velocity of all electromagnetic waves is fixed, the wavelength λ of an electromagnetic wave always determines its frequency ν, or vice versa, by the relationship $c = \nu\lambda$ The higher the frequency (i.e., the shorter the wavelength) of an electromagnetic wave, the higher in the spectrum it is said to be. Since a wave cannot have a frequency less than zero, the spectrum is bound by zero at its lower end. In theory, it has no upper limit.

Electromagnetic waves and matter. All atoms and molecules at temperatures above absolute zero radiate electromagnetic waves at specific frequencies that are determined by the details of their internal structure. In quantum physics, this radiation must often be described as consisting of particles called photons rather than as waves; however, this article will restrict itself to the classical (continuous-wave) treatment of electromagnetic radiation, which is adequate for most technological purposes.

Not only do atoms and molecules radiate electromagnetic waves at certain frequencies, they can absorb them at the same frequencies. All material objects, therefore, are continuously absorbing and radiating electromagnetic waves having various frequencies, thus exchanging energy with other objects, near and far. This makes it possible to observe objects at a distance by detecting the electromagnetic waves that they radiate or reflect, or to affect them in various ways by beaming electromagnetic waves at them. These facts make the manipulation of electromagnetic waves at various frequencies (i.e., from various parts of the electromagnetic spectrum) fundamental to many fields of technology and science, including radio communication, radar, infrared sensing, visible-light imaging, lasers, x rays, astronomy, and more.

The Spectrum

The spectrum has been divided by physicists into a number of frequency ranges or bands denoted by convenient names. The points at which these bands begin and end do not correspond to shifts in the physics of electromagnetic radiation; rather, they reflect the importance of different frequency ranges for human purposes. Below, the various parts of the spectrum are named in order, lowest-frequency to highest-frequency, and their properties described.

Radio. Radio waves are typically produced by time-varying electrical currents in relatively large objects (i.e., at least centimeters across). This category of electromagnetic waves extends from the lowest-frequency, longest-wavelength electromagnetic waves up into the gigahertz (GHz; billions of cycles per second) range. The U.S. government officially allocates sub-bands of the radio frequency spectrum to various military and commercial purposes from 9 x 10^3 Hz to 3 x 10^{11} Hz, dividing this part of the spectrum up into over 450 non-overlapping frequency bands. These bands are exploited by different users and technologies: for example, broadcast FM is transmitted using frequencies on the order of 10^6 Hz, while television signals are transmitted using frequencies on the order of 10^8 Hz (about a hundred times higher). In general, higher-frequency signals can be used to transmit lower-frequency information, but not the reverse; thus a voice signal with a maximum frequency content of 20 kHz (kilohertz, thousands of Hertz) can, if desired, be transmitted on a signal centered in the Ghz range, but it is impossible to transmit a television signal over a broadcast FM station. From 10^9 to 3 x 10^{11} Hz, radio waves are termed microwaves; these are used for high-speed communications links, heating food, radar, and electromagnetic weapons, that is, devices designed to irritate or injure people or to disable enemy devices. The microwave frequencies used for communications and radar are subdivided still further into frequency bands with special designations, such as "X band" and "Y band." Microwave radiation from the Big Bang, the cosmic explosion in which the Universe originated, pervades all of space.

Infrared. Electromagnetic waves from approximately 10^{12} to 5 µlt 10^{14} Hz are termed infrared radiation. The word infrared means "below red," and is assigned to these waves because their frequencies are just below those of red light, the lowest-frequency light visible to human beings. Infrared radiation is typically produced by molecular vibrations and rotations (i.e., heat) and causes or accelerates such motions in the molecules of objects that absorb it; it is, therefore, perceived by the body through the increased warmth of skin exposed to it. Since all objects above absolute zero emit infrared radiation, electronic devices sensitive to infrared can form images even in the absence of visible light. Because of their ability to "see" at night, imaging devices that electronically create visible images from infrared light are important in security systems, on the battlefield, and in observations of the Earth from space for both scientific and military purposes.

Visible. Visible light consists of elecromagnetic waves with frequencies in the 4.3 x 10^{14} to 7.5 x 10^{14} Hz range. Waves in this narrow band are typically produced by rearrangements (orbital shifts) in the outer electrons of atoms. Most of the energy in the sunlight that reaches the Earth's surface consists of electromagnetic waves in this narrow frequency range; our eyes have therefore evolved to be sensitive to this band of the electromagnetic spectrum.

Photovoltaic cells—electronic devices which turn incident electromagnetic radiation into electricity—are also designed to work primarily in this band, and for the same reason. Because half the Earth is liberally illuminated by visible light at all times, this band of the spectrum, though narrow (less than an octave), is essential to thousands of applications, including all forms of natural and many forms of mechanical vision.

Ultraviolet. Ultraviolet light consists of electromagnetic waves with frequencies in the 7.5×10^{14} to 10^{16} Hz range. It is typically produced by rearrangements in the outer and intermediate electrons of atoms. Ultraviolet light is invisible, but can cause chemical changes in many substances: for living things, consequences of these chemical changes can include skin burns, blindness, or cancer. Ultraviolet light can also cause some substances to give off visible light (flouresce), a property useful for mineral detection, art-forgery detection, and other applications. Various industrial processes employ ultraviolet light, including photolithography, in which patterned chemical changes are produced rapidly over an entire film or surface by projecting patterned ultraviolet light onto it. Most ultraviolet light from the sun is absorbed by a thin layer of ozone (O_3) in the stratosphere, making the Earth's surface much more hospitable to life than it would be otherwise; some chemicals produced by human industry (e.g., chlorfluorocarbons) destroy ozone, threatening this protective layer.

X rays. Electromagnetic waves with frequences from about 10^{16} to 10^{19} Hz are termed x rays. X rays are typically produced by rearrangements of electrons in the innermost orbitals of atoms. When absorbed, they are capable of ejecting electrons entirely from atoms and thus ionizing them (i.e., causing them to have a net positive electric charge). Ionization is destructive to living tissues because ions may abandon their original molecular bonds and form new ones, altering the structure of a DNA molecule or some other aspect of cell chemistry. However, x rays are useful in medical diagnosis and in security systems (e.g., airline luggage scanners) because they can pass entirely through many solid objects; both traditional contrast images of internal structure (often termed "x rays" for short) and modern computerized axial tomography images, which give much more information, depend on the penetrating power of x rays. X rays are produced in large quantities by nuclear explosions (as are electromagnetic waves at all other frequencies above the radio band), and have been proposed for use in a space-based ballistic-missile defense system as follows: X-rays emitted by an orbital nuclear explosion would stimulate coherent, highly-directional x-ray emission (x-ray lasing) in special fibers placed next to the warhead that had been pre-aimed at ballistic warheads arcing through space. The resulting x-ray laser bursts would disable the warheads or knock them off course. There are, however, many technical and political problems with such a scheme, and its feasibility has never been demonstrated.

Gamma rays. All electromagnetic waves above about 3×10^{19} Hz are termed gamma rays (γ rays). Gamma rays are typically produced by rearrangements of particles in atomic nuclei. A nuclear explosion produces large quantities of gamma radiation, which is both directly and indirectly destructive of life. By interacting with the Earth's magnetic field, gamma rays from a high-altitude nuclear explosion can cause an intense pulse of radio waves termed an electromagnetic pulse (EMP). EMP may be powerful enough to burn out unprotected electronics on the ground over a wide area; most military hardware is therefore "hardened" against EMP to some degree, although hardening standards vary from one sector of the military to another.

Radio-frequency spectrum allocation. Radio waves present a unique regulatory problem, for only one broadcaster at a particular frequency can function in a given area. (Signals from overlapping same-frequency broadcasts would be received simultaneously by antennas, interfering with each other.) Throughout the world, therefore, governments regulate the radio portion of the electromagnetic spectrum, a process termed spectrum allocation. In the U.S., since the passage of the Communications Act of 1934, the radio spectrum has been deemed a public resource. Individual private broadcasters are given licenses allowing them to use specific portions of this resource, that is, specific sub-bands of the radio spectrum. The United States Commerce Department's National Telecommunications and Information Administration (NTIA) and FCC (Federal Communications Commission) oversee the spectrum allocation process, which is subject to intense lobbying by various telecommunications stakeholders.

Military and security significance of the electromagnetic spectrum. Virtually all forms of military, espionage, and security activity exploit some portion of the electromagnetic spectrum. The transmission, reception, and interception of radio messages are perhaps the most obvious examples, second to the use of light in the visible spectrum for ordinary vision and most technical imaging. More exotic direct applications of electromagnetic radiation are also under development, including the direct use of electromagnetic waves (e.g., laser light) as a destructive weapon, and for various other methods of electronic warfare, defined by the U.S. Joint Chiefs of Staff as "any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy." Jamming of enemy transmissions and protection of friendly forces against enemy jamming attempts are typical forms of electronic warfare.

In summary, it can be said that the manipulation of every level of the electromagnetic spectrum is of urgent

technological interest, but most work is being done in the radio through the visible portions of the spectrum (below 7.5×10^{14} Hz), where communications, radar, and imaging can be accomplished.

FURTHER READING:

ELECTRONIC:

"Electromagnetic Spectrum Use in Joint Military Operations." Chairman of the Joint Chiefs of Staff Instruction. May 1, 2000. <http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3320_01.pdf> (Jan. 30, 2003).

Schroeder, Norbert. "Radio Frequency Spectrum Allocations in the United States." National Telecommunications and Information Administration. July 1, 2000. <http://www.ntia.doc.gov/osmhome/chart_00.htm> (Jan. 30, 2003).

SEE ALSO

Electromagnetic Weapons, Biochemical Effects
Electronic Countermeasures
Electro-optical Intelligence

Electromagnetic Warhead Shrouding.

SEE *Infrared Detection Devices.*

Electromagnetic Weapons, Biochemical Effects

BRIAN HOYLE

Electromagnetic weapons—also known as E-bombs—are designed to release a high-power flash of radio waves or microwaves. Depending on the energy of the electromagnetic pulse, effects can range from the disabling of electronic circuitry to physiological effects in those exposed to the electromagnetic pulse.

The pulse released by an electromagnetic weapon lasts for an extremely short time, around 100 picoseconds (one ten-billionth of a second). The absorption of this blast of high energy by anything capable of conducting electricity, including nerves and neurons, overwhelms the recipient.

Research and development into the effects of electromagnetic weapons on human beings and animals was underway in the 1940s. The Japanese spent considerable sums of money on the development of a "Death Ray" between 1940 and 1945. A review of these studies by the United States military concluded that it was possible to develop a weapon that would produce an electromagnetic ray capable of killing humans five to 10 miles away from the source.

Animal studies have demonstrated the lethal nature of electromagnetic radiation. In the studies, wavelengths ranging from 60 centimeters destroyed the lung cells of mice and ground hogs. Wavelengths less than two meters also destroyed brain cells.

Electronic stimulation can have other, nonlethal effects on humans. Secret research conducted in the United States following World War II demonstrated that electronic stimulation of different regions of the brain of test subjects could produce extreme emotions of rage, lust, and fatigue. Another research program, dubbed "Operation Knockout," operated at the Allan Memorial Institute in Montreal, Canada, with funding from the Central Intelligence Agency. The study's director, Dr. Ewen Cameron, discovered that electroshock treatments caused amnesia. Memories could be erased, and the subjects reprogrammed. Once these "psychic driving" experiments became public, Cameron—then a pre-eminent psychiatrist, endured harsh public and professional criticism.

In the 1960s, the U.S. Defense Advanced Projects Research Agency (DARPA) studied the health and psychological effects of low energy microwaves for weapons applications. The ability of microwaves to damage the heart, create leaks in blood vessels in the brain, and to produce hallucinations were demonstrated.

Many scientists assume that research into the debilitating effects of electromagnetic radiation has continued up to the present day. However, increasing restrictions on the information obtainable through the U.S. Freedom of Information Act have made verification difficult. A 1993 U.S. Air Command and Staff College paper entitled "Non Lethal Technology and Air Power" documented low frequency, "acoustic" and high power microwave weapons that could deter or debilitate humans.

Low frequency electromagnetic waves, also known as acoustic waves, have been commonly used for decades in functions such as ultrasound machines. However, acoustic waves can also cause internal organs of humans to vibrate. The result can be nausea, diarrhea, earache, and mental confusion. The discomfort increases as one gets closer to the source.

Shorter wavelength electromagnetic radiation produces different effects. A common example is microwave radiation, which in a microwave oven can be used to heat up foods and liquids. When directed at humans, a microwave weapon causes atoms to vibrate, which in turn generates heat. At 200 yards away, body temperature increases from the normal 98.6° F to 107° F. At closer range, the temperature increase can be even higher, and is lethal.

Microwave electromagnetic weapons can also stun a victim. This is the result of the stimulation of peripheral nerves. The simultaneous activity of many nerves overwhelms the capacity of the brain to process the incoming information, and can induce unconsciousness.

The biochemical effect of microwave exposure is dependent on the distance from the source, as electromagnetic fields become much weaker as the distance from the source increases.

Experiments with very low frequency electromagnetic radiation have demonstrated that the radiation can induce the brain to release chemicals that induce slumber, or to release a chemical called histamine. In human volunteers, the histamine release produces flu-like symptoms, which dissipate when the radiation stops.

Not all electromagnetic weapons are cloaked in military secrecy. A device called the Pulse Wave Myotron is commercially available. The Myotron emits rapid pulses of electromagnetic radiation. The pulses incapacitate the movement of voluntary muscles by over riding the electrical pulse that normally flows from nerve to nerve within the muscles. Involuntary muscles, such as the heart and muscles that operate the lungs, are unaffected. Thus, a victim is rendered incapable of movement or speech. The effect lasts until the muscles can repolarize; approximately 30 minutes.

FURTHER READING:

BOOKS:

Alexander, John B. *Future War: Non-Lethal Weapons in Twenty-First Century Warfare.* New York: St. Martin's Press, 1999.

PERIODICALS:

Pasternak, D. "Wonder Weapons." *U.S. News & World Report.* July 7 (1997): 38–46.

SEE ALSO

Electronic Warfare
Energy Directed Weapons
Radio Frequency (RF) Weapons

Electronic Communication Intercepts, Legal Issues

MICHAEL J. O'NEAL

The legal issues surrounding the interception of electronic communications are many and varied, primarily because they arise in different contexts: criminal investigations, corporate espionage, employer-employee relationships, and the intelligence activities of the federal government conducted against foreign countries. In recent years, two primary issues have arisen. One, rapid changes in technology can sometimes outpace legislation designed to protect United States citizens from unwarranted electronic intercepts. Two, in response to the threat of terrorism against the United States, the federal government passed legislation that, in the eyes of some, weakened constitutional protections against unwarranted interception of electronic communications.

Electronic intelligence. Traditionally, intelligence-gathering operations have been divided into two broad categories: human and electronic. Human intelligence gathering, or what the intelligence community refers to as HUMINT, involves the use of on-the-scene human operatives who, for example, prepare maps, observe enemy troop movements, steal documents, recruit others to provide information, or physically eavesdrop on conversations.

HUMINT is a dangerous undertaking. The possibility always exists that the operative will be caught, forced to reveal information about his or her activities and purposes, and even imprisoned or executed. For this reason, intelligence agencies whenever possible have come to rely more on electronic intelligence gathering, or ELINT. Spy satellites and high-altitude planes such as the U2, for example, can be used to provide accurate and timely information about troop deployments or missile installations, while wiretaps and hidden microphones allow communications to be intercepted without placing an operative in danger. Further, ELINT can be conducted by those who have no particular training in spycraft (tradecraft) from positions thousands of miles away.

ELINT is divided into two types: trespassory and non-trespassory. As its name suggests, trespassory ELINT requires some sort of trespass; the target's physical premises have to be entered—to install a transmitter or microphone, for example. Non-trespassory ELINT, in contrast, does not require physical invasion of the target premises. Since the end of World War II and throughout the Cold War, the intelligence community has devised various forms of non-trespassory ELINT, enabling it to intercept information transmitted by satellite, radio, cell phone, and microwave transmissions. While ELINT was and is valuable for gathering foreign intelligence, Congress and the public were concerned about possible misuses of it in conducting criminal investigations against U.S. citizens. Accordingly, under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wire Tap Statute"), trespassory interception of electronic communications in criminal investigations without a court order was made illegal. In 1986 the Electronic Communications Privacy Act amended Title III to include non-trespassory interception of e-mail, computer communications, and cell phones calls.

TEMPEST technology. The chief legal issue surrounding non-trespassory interception of electronic communications stems from the use of the word *communication.* Under the act, it would be illegal for authorities to, for example, tap a phone without a court order, because the purpose of a phone call is to communicate a message. But modern

electronic devices emit all sorts of information that is never intended to be "communicated." They do so in the form of what are called emanated transient electromagnetic pulses (ETEP), which can be received and reconstructed. A computer screen, for example, displays information in the form of pixels that glow when they are struck by an electron beam. To keep the pixels on a computer screen lit, the electron beam fires perhaps 60 times per second. The beam's high-voltage electromagnetic emission can be intercepted and read from as far away as a kilometer using classified government technology called TEMPEST, which stands for Transient Electromagnetic Pulse Emanation Standard. Thus, information can be legally intercepted from a computer screen because it is not "communication"; it is merely incidental to the work that the machine is performing.

The potential for abuse is clear. A person or agency with the know-how could intercept from a business computer information that would be beneficial in, for example, making stock market transactions, or steal proprietary information about the development of a new product. But because the U.S. government uses TEMPEST technology to conduct intelligence on foreign governments and potentially to monitor the activities of terrorists, it currently prohibits nongovernment agencies or individuals from owning TEMPEST equipment, making it difficult to research ways to protect legitimate computer users from this modern form of "eavesdropping."

Echelon. In 1947, the United States and Great Britain agreed to join forces to form a "worldwide listening network," primarily to keep themselves apprised of the activities of the Soviet Union and its allies. In the United States, this agreement in 1971 evolved into Echelon, a global communications interception and surveillance system. In its early days, the U.S.-UK system and Echelon focused on phone and radio traffic. Later, the focus shifted to satellite and microwave communications. More recently, Echelon has also been used to monitor digital communication, principally on the Internet.

The workings of Echelon remain secret; the U.S. government barely acknowledges that it exists, and personnel who work for the agencies of foreign governments with access to Echelon (currently, Australia, Canada, Denmark, Germany, New Zealand, Norway, and Turkey) sign lifetime confidentiality agreements. Echelon functions by tapping numerous sources, including ground-based radio antennae, cable devices, satellites, equipment housed in the U.S. embassies of foreign nations, and the Internet. With regard to the Internet, Echelon can intercept e-mail and file transfers, and by using so-called sniffer devices, it can monitor Web browsing. It then uses a "dictionary" to filter information through key words and addresses, as well as to translate messages and even to interpret their content. It is estimated that Echelon can intercept three *billion* communications per day, including 90 percent of Internet and satellite traffic.

Echelon was formed for the purpose of conducting foreign intelligence operations. Under the Foreign Intelligence Surveillance Act, no proof of criminality has to be shown to conduct such operations; the only safeguard is the secret Foreign Intelligence Surveillance Court, which verifies that the target of an operation is an "agent of a foreign government" rather than a U.S. citizen (or permanent resident alien). Once again, though, the potential for abuse is clear. Many governments have pressured the United States to reveal information on surveillance targets and intelligence operations conducted through Echelon. They are concerned because of reports that economic and business information gathered through Echelon has been passed to American companies, giving them an advantage over their foreign competitors. In recent years, too, civil libertarians have expressed concern that Echelon could be used in a way that violates the Fourth Amendment, which preserves the right of American citizens to be free from unreasonable searches and seizures.

The USA Patriot Act. These developments—the pervasiveness of electronic intelligence-gathering capabilities, the existence of sophisticated surveillance technologies, the evolution of Echelon—all coalesced on October 26, 2001, when President George W. Bush signed into law the USA Patriot Act, more formally the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Public Law 107–56; 115 Stat. 272). The act was passed in response to the terrorist attacks against the United States on September 11 that year. Its goal was to provide law enforcement and the intelligence community with tools to combat international terrorism.

Even before it was signed into law, the bill was controversial. Its supporters argued that it was necessary in an environment when attacks could emanate not only from recognized states with identifiable borders but also from loosely affiliated transnational groups such as militant Islamic extremists. These groups, it was pointed out, include American citizens and others living inside the United States, such as many of the September 11 hijackers. To communicate across national borders, launder money, and channel funds, these groups rely on phones, radio, and especially the Internet, and law enforcement's efforts to monitor their communications were shackled by legislation that restricted electronic intercepts. The bill's opponents argued that the act poses significant risk that civil liberties will be infringed and that it does not provide for legislative and judicial overview of the purposes for which such information is used.

The 342-page USA Patriot Act amends fifteen different statutes, including the Electronic Communications Privacy Act, the Computer Abuse and Fraud Act of 1986, and the Foreign Intelligence Surveillance Act. Many of the changes are scheduled to expire on December 31, 2005, unless they are extended by Congress. While many of the changes are minor, they collectively give the Federal Bureau of Investigation (FBI), the Central Intelligence Agency

(CIA), other federal agencies, and local law enforcement sweeping new powers to conduct intelligence operations against terrorists inside the United States. For example, the government can now legally monitor Web surfing, including terms entered into search engines, by informing a judge that doing so could lead to information "relevant" to a terror investigation. Again, civil libertarians fear that a ten-year-old who innocently conducts a Web search for *bomb* or a student doing Internet research on Allah (the name of the deity in the Islamic faith) could actually attract the attention of the CIA—and never know it.

The act made other significant changes in the law. Both the FBI and the CIA had complained that earlier laws requiring a court order to tap a phone were unduly restrictive in the age of cell phones, when a user is not wired to a location and can easily use multiple phones while on the move. Under the USA Patriot Act, they have the authority to conduct roving wiretaps; instead of getting a court order to tap *a phone,* they now can get such an order to tap a person or organization. This means that if a terrorist suspect uses a cell phone, throws it away, then uses another phone, the government can monitor calls made and received on both phones rather than just one. Similarly, the new law makes it easier for the government to get so-called pen/trap orders, referring to "pen register" and "trap-and-trace device" orders. This change authorizes the collection of telephone numbers dialed to and from a particular communication device, including phones of course, but also computers with Internet connections.

Another change involves Internet service providers (ISPs). Previously, the government had to obtain a court order to access the records of an ISP. Now, the government can seek information from ISPs with just a subpoena. This information includes records of session times and durations, network addresses, and methods of payment. The law also authorizes the ISPs themselves to turn over information they believe suggests that a threat against American lives exists. This includes not only "noncontent" information (account numbers, phone numbers, credit card account numbers, and the like) but "content" information—that is, the actual content of messages that suggest a terrorist threat. Again, the purpose of all these changes is to enable law enforcement to monitor the "chatter" of terrorist groups and, on the basis of information gathered, warn the American public about impending threats, thwart terrorist attacks, and round up suspected terrorists.

■ FURTHER READING:

BOOKS:

Ewing, Alphonse B. *USA Patriot Act.* Hauppauge, N.Y.: Nova Science Publishing, 2003.

Reams, Bernard D., Jr., and Christopher Anglim, ed. *USA Patriot Act: A Legislative History of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.* Littleton, CO.: Fred B. Rothman, 2002.

Richelson, Jeffrey T. *The Wizards of Langley.* Boulder, CO.: Westview, 2001.

ELECTRONIC:

Electronic Frontier Foundation. "EFF Analysis of the Provisions of the USA PATRIOT Act that Relate to Online Activities," October 31, 2001 <http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html.

Federation of American Scientists. "Echelon." <http://www.fas.org/irp/program/process/echelon.htm.

United Nations. "Echelon: Legal, Political, and Economic Issues of International Surveillance." <http://www.unesco.org/webworld/observatory/in_focus/290302_echelon.html.

SEE ALSO

Bugs (microphones) and Bug Detectors
Bush Administration (2001–), United States National Security Policy
Computer Fraud and Abuse Act of 1986
Computer Hardware Security
Counter-Terrorism Policy, United States
Domestic Intelligence
ECHELON
Electromagnetic Pulse
Foreign Intelligence Surveillance Act
Foreign Intelligence Surveillance Court of Review
HUMINT (Human Intelligence)
Internet Surveillance
Internet Tracking and Tracing
Patriot Act, United States
Privacy: Legal and Ethical Issues
September 11 Terrorist Attacks on the United States
U-2 Spy Plane

Electronic Countermeasures

Electronic countermeasures (ECM), also known as electronic attack, is a component of electronic warfare (EW), the use or control of electromagnetic energy either in defense, or for the purposes of a military attack on an enemy. Its counterpart is electronic protection or electronic counter-countermeasures (ECCM)—efforts or equipment directed toward the protection of persons or material from the effects of electronic warfare.

Exemplary of electronic countermeasure technology are the systems developed by Bell Helicopter Textron for the U.S. Air Force, tested in the fall of 2002. The CV-22 Osprey tiltrotor, converted from a V-22, was intended for deployment with Air Force Special Operations Command, which has a specialty in low-altitude force insertions under day or night conditions. The aircraft's suite of integrated radio frequency countermeasures includes technology for threat location and radar jamming. The Air Force subjected the aircraft to three months' worth of testing suspended in an anechoic chamber, which simulates an ECM environment.

This April 1999 U.S. Air Force file photo shows the F-22 Raptor in a test flight over Edwards Air Force Base in California. The aircraft features muti-spectral countermeasures and wide field-of-regard offensive and defensive sensors. ©AFP/CORBIS.

The U.S. deployment to Iraq in 2003 tested capabilities both in ECM and ECCM. The relative sophistication of Iraqi electronic systems, built by Western-trained engineers and mathematicians, provided a special challenge to planners. Prior to the commencement of the campaign, Army chief of intelligence Lt. Gen. Robert W. Noonan told *Aviation Week & Space Technology* that in the event of war, "one of the first objectives would be to disrupt local fiber-optic networks, and thus, force the Iraqis to rely on less state-of-the-art communication technologies."

FURTHER READING:

BOOKS:

Chrzanowski, Edward J. *Active Radar Electronic Countermeasures.* Norwood, MA: Artech House, 1990.

Lothes, Robert N., Michael B. Szymanski, and Richard G. Wiley. *Radar Vulnerability to Jamming.* Boston: Artech House, 1990.

PERIODICALS:

Phillips, Edward H. "USAF Testing CV-22 Countermeasures." *Aviation Week & Space Technology* 157, no. 15 (October 7, 2002): 59.

Wall, Robert. "Intelligence Support Seen Crucial to U.N." *Aviation Week & Space Technology* 157, no. 17 (October 21, 2002): 30.

SEE ALSO

Electromagnetic Pulse
Electromagnetic Spectrum
Electronic Warfare

Electronic Warfare

Electronic warfare, or EW, is the use or control of electromagnetic energy either in defense, or for the purposes of a military attack on an enemy. There are three components of electronic warfare: electronic countermeasures or electronic attack, electronic counter-countermeasures or electronic protection, and electronic warfare support measures.

Electromagnetism and the electromagnetic spectrum. Electromagnetism is the branch of physics devoted to the study

A U.S. Navy EA-6B Prowler carries sophisticated electronic equipment on board for jamming radar. ©REUTERS NEWMEDIA INC./CORBIS.

of electric and magnetic phenomena. Its focus is electromagnetic force, which, along with gravitation and the strong and weak nuclear forces, is one of the four fundamental interactions in nature. Electromagnetic energy is conveyed by means of radiation, which transfers energy without the requirement of a medium such as air or water. Sunlight, which travels to Earth through the vacuum of space, is electromagnetic energy.

Electromagnetic waves travel at the speed of light, and, as their name indicates, involve both electric and magnetic components. If one holds one's right hand, palm perpendicular to the floor and thumb upright, the fingers indicate the direction that an electromagnetic wave is moving; the thumb points in the direction of the electrical field, as does the heel of the hand; and the palm and the back of the hand indicate the direction of the magnetic field, which is perpendicular both to the electrical field and the direction of wave propagation.

The electromagnetic spectrum is the complete range of electromagnetic waves on a continuous distribution from a very low range of frequencies and energy levels, with a correspondingly long wavelength, to a very high range of frequencies and energy levels, with a correspondingly short wavelength. Included on the electromagnetic spectrum are—in order of energy levels, from lowest to highest—radio waves and microwaves; infrared, visible, and ultraviolet light; x rays, and gamma rays. Although each occupies a definite place on the spectrum, the divisions between them are not firm; as befits the nature of a spectrum, one simply "blurs" into another.

Using electromagnetic energy in warfare. The uses of electromagnetism for war are myriad, and range from the application of radar for navigation and locating targets to the use of electronic bombs or "e-bombs" to disrupt an enemy's mechanical and electromagnetic systems. Electromagnetic energy can be used to confuse or deceive an enemy, as for instance in radar-jamming applications or the propagation of misleading signals. It can also be used directly as a weapon to disable infrastructure.

The three principal components of electronic warfare are:

1. Electronic attack or electronic countermeasures: The use of electromagnetic or directed energy against personnel or equipment with the aim of degrading or destroying combat capabilities.

2. Electronic protection or electronic counter-countermeasures: Efforts or equipment directed toward the protection of persons or material from the effects of electronic warfare. These includes the unintended side-effects of friendly electronic warfare, as well as enemy actions undertaken for the purpose of degrading or destroying one's combat capabilities.

3. Electronic warfare support: Actions and resources committed toward locating, identifying, and if necessary intercepting or neutralizing sources of electromagnetic energy that pose an immediate threat.

FURTHER READING:

BOOKS:

Browne, J. P. R. *Electronic Warfare.* London: Brassey's, 1998.

Hoffman, Lance J. *Rogue Programs: Viruses, Worms, and Trojan Horses.* New York: Van Nostrand Reinhold, 1990.

Price, Alfred. *War in the Fourth Dimension: U.S. Electronic Warfare, from the Vietnam War to the Present.* London: Greenhill, 2001.

Schleher, D. Curtis. *Electronic Warfare in the Information Age.* Boston: Artech House, 1999.

PERIODICALS:

Wall, Robert. "Focus on Iraq Shapes Electronic, Info Warfare." *Aviation Week & Space Technology.* 157, no. 19 (November 4, 2002): 34–35.

———. "Military Launches New EW Efforts." *Aviation Week & Space Technology.* 157, no. 19 (November 4, 2002): 35–43.

SEE ALSO

Electromagnetic Pulse
Microwave Weaponry, High Power (HPM)

Electro-Optical Intelligence

Electro-optical "intelligence" involves the acquisition of data from the portion of the electromagnetic spectrum of wavelengths that contains ultraviolet radiation, visible light, and infrared radiation.

The term intelligence refers to the use to which the optical spectrum is put. Ultraviolet, visible, and infrared rays can be collected and analyzed for the information they contain. For example, the detection of infrared radiation—either via satellite or localized detection devices—can reveal the location and movements of humans and heat-generating machinery.

Other analyses can reveal information about the composition of the object that is emitting the radiation. For example, the exhaust of a missile can be detected and distinguished from the exhaust of a commercial aircraft.

Electro-optical analysis equipment most commonly includes forms of radiometers, spectrometers, lasers, and laser radar devices.

Radiometers such as the Advanced Very High Resolution Radiometer operated by the National Oceanographic and Atmospheric Administration, and the Multi-angle Imaging SpectroRadiometer operated by the National Aeronautics and Space Administration provide detailed views of the Earth's surface. For example, the removal of vegetation from an area due to clearing and/or construction is readily detected. While used predominantly for climate studies, these instruments may also provide detailed views that allow critical assessment of the industrial and/or military development in a surveyed area.

A laser radar sends out pulses of a laser beam. The beam, a constrained and narrow beam of light, will ultimately encounter an object and be reflected, still as a tightly organized beam. When the beam returns to the source, a detector can measure the time taken for the beam to travel to the object and return. The distance from the source to the object can be measured very accurately over extremely long distances (i.e., Earth to the Moon).

The United States Army's Pulsed Laser Vulnerability Test System (PLVTS) is a CO_2 laser that can be housed in a portable vehicle. The unit can be taken to whatever test or military site requires accurate radar measurements. The PLVTS has been used in the evaluation of the M-1 tank, Black Hawk helicopter, and various missile test launches.

Another aspect of electro-optical intelligence involves the use of cameras that can record information in both the visible and infrared spectra. Because the infrared emissions from objects occur at night as well as during the day, these cameras are capable of gathering information both in day time and at night. Such cameras have been used in high altitude "spy planes" and other reconnaissance aircraft to develop intelligence concerning ground operations shrouded by clouds associated with weather fronts or more permanently obscured by thick indigenous fog or pollution.

Similarly, visible and infrared imaging is incorporated into telescopes operated by the U.S. Space Command in Haleakala, Maui (TEAL BLUE) and Malabar, Florida (TEAL AMBER). The telescopes are used for the tracking of satellites orbiting the Earth (including reconnaissance satellites) and those that are deeper in space.

FURTHER READING:

BOOKS:

Gaffney, Timothy, R. *Secret Spy Satellites: America's Eyes in Space.* Berkeley Heights, NJ: Enslow Publishers Inc., 2000.

Kupperberg, Paul. *Spy Satellites (The Library of Satellites).* New York: Rosen Publishing Group, 2003.

ELECTRONIC:

Institute for Defense Studies and Analysis. "Shaping the Land Battle through Remote Sensing and Satellite-Imagery." JNU Campus. February, 2000. <http://www.idsa.org/an-feb00–5.html>(26 December 2002).

SEE ALSO

Electromagnetic Spectrum
Electronic Warfare
EM Wave Scanners
Infrared Detection Devices
Laser Listening Devices
Lasers
LIDAR (Light Detection and Ranging)
Microscopes
Satellites, Non-Governmental High Resolution
Satellites, Spy
Spectroscopy

Electrophoresis

Diseases caused by microorganisms are a threat to national security. Even in countries with well-developed healthcare systems, a massive outbreak can strain healthcare infrastructure. In other countries that are less wealthy and more politically volatile, the ravages of disease can sow the seeds of resentment against the more wealthy countries of the West. Thus, it is in a country's best interests to combat infectious diseases. One strategy is to examine the relevant microorganisms, particularly to find out the component(s) that are responsible for the infection. For many microbes, proteins are an important factor in the development of a disease. Proteins can function as receptors, to allow the microorganism to adhere to the surface of a host cell. As well, the toxins produced by microbes such as *Escherichia coli* O157:H7 and *Vibrio chlorerae* are proteins. Methods that can "dissect" microorganisms into their components, and which can compare a non-disease causing strain of a microbe to a disease-causing strain to see what they differences are, is a valuable approach to fighting infectious disease. Electrophoresis is especially well suited to this role. Furthermore, specialized types of electrophoresis (i.e., pulsed field electrophoresis) allow the genetic material of the microorganism to be examined. Thus, electrophoresis can reveal much detail at the molecular level.

Electrophoresis is a sensitive analytical form of chromatography. Under the influence of an electrical field charged molecules can be separated from one another as they pass through a gel. The degree of separation and rate of molecular migration of mixtures of molecules depends upon a variety of factors, which can be tailored depending upon the intent of the separation. For example, conditions can be established that allow molecules of very large mass, but which differ from each other by only a fraction, to be visually separated. The factors that influence molecular separation include the individual size and shape of the molecules, their molecular charge, strength of the electric field, the type of support medium used (e.g., gels made of cellulose acetate, starch, paper, agarose, polyacrylamide) and the conditions of the medium (e.g., ion strength and concentration, pH, viscosity, temperature).

The advent of electrophoresis revolutionized the methods of protein analysis. Swedish biochemist Arne Tiselius was awarded the 1948 Nobel Prize in chemistry for his pioneering research in electrophoretic analysis. Tiselius studied the separation of serum proteins in a tube (subsequently named a Tiselius tube) that contained a solution subjected to an electric field.

In electrophoresis, the electric charge often is passed through what is known as a support medium. As summarized above, various support media can be used. They all share the trait that they are a three-dimensional arrangement of intertwined strands, which produces holes (or pores) through the gel matrix. Such matrices act as a physical sieve for macromolecules.

In general, the medium is mixed with a chemical mixture called a buffer. The buffer carries the electric charge that is applied to the system. The medium/buffer matrix is placed in a tray. Samples of molecules to be separated are loaded into wells or slots that have been formed at one end of the matrix. As electrical current is applied to the tray, the matrix takes on this charge and develops positively and negatively charged ends. As a result, molecules that are negatively charged such as deoxyribonucleic acid (DNA), ribonucleic acid (RNA), and protein are pulled toward the positive end of the gel.

Because molecules have differing shapes, sizes and charges they are pulled through the matrix at different rates and this, in turn, causes a separation of the molecules. Generally, the smaller and more charged a molecule, the faster the molecule moves through the matrix.

Intact DNA is so large that it cannot move through the pores of a gel (although the technique of pulsed field electrophoresis does allow very large pieces of DNA to be examined). When DNA is subjected to electrophoresis, the DNA is first cut into smaller pieces by restriction enzymes. Restriction enzymes recognize specific sequences of the building blocks of the DNA and cut the DNA at the particular site. There are many types of restriction enzymes, and so DNA can be cut into many different patterns. After electrophoresis, the pieces of DNA appear as bands (composed of similar length DNA molecules) in the electrophoresis matrix.

Proteins have net charges determined by charged groups of the amino acids from which they are constructed. Proteins can also be amphoteric compounds (a

compound that can take on a negative or positive charge depending on the surrounding conditions.) A protein in one solution might carry a positive charge in a particular medium and thus migrate toward the negative end of the matrix. In another solution the same protein might carry a negative charge and migrate toward the positive end of the matrix. For each protein there is a pH in which the protein molecule has no net charge (the isoelectric point). By varying the pH in the matrix, additional refinements in separation are possible.

Sodium dodecyl sulfate (SDS) polyacrylamide gel electrophoresis techniques pioneered in the 1960s provided a powerful means of protein separation. Still, because proteins of similar mass did not always clearly separate into discrete bands in the gel only small numbers of molecules could be separated.

The development in the 1970s of a two-dimensional electrophoresis technique allowed greater numbers of molecules to be separated. Two-dimensional electrophoresis is actually the fusion of two separate separation procedures. The first separation (dimension) is achieved by isoelectric focusing (IEF) that separates protein polypeptide chains according to the arrangement of amino acids that comprise a chain. IEF is based on the fact that proteins will, when subjected to a pH gradient, move to their isoelectric point. The second separation is achieved via SDS slab gel electrophoresis, which separates the molecule by molecular size. Instead of broad, overlapping bands, the result of this two-step process is the formation of a two-dimensional pattern of spots, each comprised of a unique protein or protein fragment. These spots are subsequently subjected to staining and further analysis.

Electrophoresis can be combined with the prior addition of a radioactive food source to the culture of bacteria. The bacteria will use the food to make new proteins, which will be radioactive. Following electrophoresis, the gel can be placed in contact with x-ray film. The radioactive bands or spots will register on the film, and so will determine what proteins were being made at the time of the experiment.

There are many other variations on gel electrophoresis with wide-ranging applications. These specialized techniques include Southern, Northern, and Western Blotting. Blots are named according to the molecule under study. In Southern blots, DNA is cut with restriction enzymes then probed with radioactive DNA. In Northern blotting, RNA is probed with radioactive DNA or RNA. Western blots target proteins with radioactive or enzymatically-tagged antibodies.

Modern electrophoresis techniques now allow the identification of DNA sequences that are the same, and have become an integral part of research into gene structure, gene expression , and the diagnosis of heritable diseases. Electrophoretic analysis also allows the identification of bacterial and viral strains and is finding increasing acceptance as a powerful forensic tool.

FURTHER READING:

BOOKS:

Birren, Bruce W., and Eric Hon Cheong Lai. *Pulsed Field Electrophoresis: A Practical Guide.* San Diego: Academic Press, 1997.

Rabilloud, Thierry. *Proteome Research: Two-Dimensional Gel Electrophoresis and Identification Methods (Principles and Practice).* Berlin: Springer Verlag, 2000.

Westermeier, Reiner. *Electrophoresis in Practice.* Weinheim: Vch Verlagsgesellschaft 2001.

ELECTRONIC:

Colorado State University. "Gel Electrophoresis of DNA and RNA." Biomedical Hypertextbooks. January 15, 2000. <http://arbl.cvmbs.colostate.edu/hbooks/genetics/biotech/gels/>(5 January 2003).

SEE ALSO

Chemical and Biological Detection Technologies
DNA Recognition Instruments
Microbiology: Applications to Espionage, Intelligence and Security
Thin Layer Chromatography

ELINT (Electronics Intelligence).

SEE *SIGINT (Signals Intelligence).*

EM Wave Scanners

In order to observe phenomena that cannot be glimpsed through direct contact, for example, the activities of an isolated weapons-testing site in a hostile nation, it may be necessary to employ remote-sensing equipment and techniques. These typically involve views from the air or from space, which require the use of electromagnetic radiation (EMR) across a wide spectrum. Though the information rewards can be high, intelligence services using electromagnetic (EM) scanners in space must deal with a variety of challenges in data collection and analysis.

Electromagnetic radiation from the sun. Light from the sun is electromagnetic radiation, and it contains both electric and magnetic components. The direction of propagation for an electromagnetic wave is mutually perpendicular with directions of its electrical and magnetic fields, whereas the electrical field might be thought of as the *x*-axis on a Cartesian coordinate plane, and the magnetic field the *y*-axis, the direction of wave propagation is the *z*-axis.

About 30% of the electromagnetic radiation from the sun that reaches Earth is reflected back into space unchanged, without entering Earth's atmosphere. This is due

to the planet's albedo—its reflective power, or the proportion of incoming radiation that it reflects. Another 25% of solar radiation is absorbed by the atmosphere, while about 45% is absorbed at the planetary surface by living and non-living materials. This energy is later re-radiated to space in degraded form, that is, at a longer wavelength.

The atmosphere and its current conditions have a powerful effect on the amount of visible light reflected, and this—along with the loss of electromagnetic energy from the sun—places constraints on the observational abilities of remote-sensing equipment.

Detecting images. There is a continuous distribution of electromagnetic energy levels, from extremely low to extremely high, that together constitutes the entire electromagnetic spectrum of energy. At the lowest level are radio waves, then microwaves (the section of the spectrum across which television transmission takes place). Higher in frequency and energy levels are such forms of light as infrared, visible, and ultraviolet. Still higher are x rays, and highest of all are gamma rays, which have an extremely small wavelength and extremely high frequency.

Of most interest in remote sensing are the energy levels near the middle of the spectrum: microwaves, infrared, visible light, and ultraviolet light. Remote sensing satellites measure the EMR reflected from features on Earth back into space. Photographic cameras on remote-sensing satellites are capable of detecting light from the near infrared to the near ultraviolet. Remote sensing equipment typically divides the infrared portion into relatively low-energy near-infrared images, and higher energy thermal infrared images. The satellite may have a thermal scanner that operates in the thermal infrared portion, or a multi-spectral scanner operating across a range from ultraviolet to thermal infrared. There may also be passive microwave and active radar systems operating in the microwave portion of the spectrum.

Scanning and processing images. Satellites equipped with multi-spectral scanners can make precise measurements across a number of narrow bands. These scanners may be of the oscillating or "wisk-broom" type, which scan along a line perpendicular to that of the satellite's trajectory, or of the "push-broom" type, which detect entire scan lines at once.

These multi-spectral scanners record electromagnetic radiation as electrical signals, convert them to digital format, and transmit the information to an Earth receiving station. The latter interprets various numbers as brightness values on a gray scale. Depending on the needs of the observing agency, images may be adjusted for resolution. For example, spatial resolution improves the detail for smaller objects, while radiometric resolution allows for the greatest levels of contrast. The analyzing agency may, in the digital image processing phase, add false color to enhance the readability of images for specific data—for example, red to indicate heat levels at areas where weapons are being tested.

FURTHER READING:

BOOKS:

Chen, C. H. *Information Processing for Remote Sensing.* River Edge, NJ: World Scientific, 1999.

Dehqanzada, Yahya A., and Ann Florini. *Secrets for Sale: How Commercial Satellite Imagery Will Change the World.* Washington, D.C.: Carnegie Endowment for International Peace, 2000.

Firschein, Oscar, and Thomas M. Strat. *RADIUS: Image Understanding for Imagery Intelligence.* San Francisco, CA: Morgan Kaufmann Publishers, 1997.

Krepon, Michael. *Commercial Observation Satellites and International Security.* New York: St. Martin's Press, 1990.

ELECTRONIC:

"Earthshots: Satellite Images of Environmental Change (U.S. Geological Survey)." <http://edcwww.cr.usgs.gov/earthshots/slow/tableofcontents> (February 26, 2003).

"Remote Sensing Data and Information." <http://rsd.gsfc.nasa.gov/rsd/RemoteSensing.html> (February 26, 2003).

"Satellite Remote Sensing." University of Waterloo Faculty of Environmental Sciences. <http://www.fes.uwaterloo.ca/crs/geog165/srs.htm> (February 26, 2003).

"Visualization of Remote Sensing Data." <http://rsd.gsfc.nasa.gov/rsd/> (February 26, 2003).

SEE ALSO

Satellites, Spy

Emergency Response Teams

Emergency response teams are the front line of the Environmental Protection Agency (EPA) Emergency Response Program, which is in turn at the center of the national infrastructure for responding to environmental hazards such as oil spills. The Emergency Response Program brings together a wide range of activities directed toward ensuring appropriate, timely responses in the event of an emergency involving the release of oil or hazardous substances. After state and local first-responder capabilities have been exceeded, emergency response teams provide additional support to see that all hazards are dealt with in accordance with federal guidelines for the safety of human populations and the natural environment.

The larger framework. The EPA response system is part of a larger national framework designed to respond to hazards such as the release of toxic chemicals and oil. Among the key facilities is the National Response Center operated by the Coast Guard, which is the first point of contact for

An emergency response team heads to the site of a mock biological threat during a bioterrorism training exercise at Camp Blanding, Florida in 2002. AP/WIDE WORLD PHOTOS.

reporting environmental hazards and other related public emergencies. Linked to the Response Center is the National Response Team, an interagency group co-chaired by EPA and the Coast Guard.

Just as there is a national infrastructure for hazard response, with EPA as a key component, there are guidelines governing the response at the state and local level. This is especially important because in a real-world situation, the personnel most readily available to assist on the scene will likely be local authorities and not functionaries dispatched by Washington.

Local community responses to environmental hazards are guided by the Emergency Planning and Community Right-to-Know Act or EPCRA, passed by Congress in 1986. EPA plays a key role in administering EPCRA, which groups federal agencies into 12 functional areas (for example, Hazardous Substances, which includes EPA) for emergency support.

The National Response System. Each year within the United States, there are some 20,000 emergencies that involve the release, or the potential release, of oil, toxins, and other hazardous substances. While local firefighters, emergency personnel, and police occupy the most visible role in responding to these emergencies, they are supported behind the scenes by the National Response System, in which EPA again is a key player.

The National Response System is designed to act quickly and effectively in emergencies involving oil and hazardous substances. A multi-tiered network, it involves representatives of not only local, state, and federal governments, but also industry and other groups whose knowledge and equipment are necessary to address a chemical threats to human safety and the environment.

The National Contingency Plan. Guiding the National Response System is the National Contingency Plan (NCP), also known as the National Oil and Hazardous Substances Pollution Contingency Plan. Described by EPA as a federal blueprint for emergency responses, the NCP evolved over the final third of the twentieth century, as the leadership of the United States and the industrialized world became increasingly aware of the threat that oil spills and accidental releases of chemicals could pose to societies.

A 1967 oil spill caused by the sinking of the tanker *Torrey Canyon,* which dumped more than 37 million gallons of crude oil off the British coast, prompted the development of the first NCP in the following year. Observing the massive damage with which their British counterparts were faced, U.S. officials sought to achieve a system for reporting of accidents, containment of spills, and cleanup of affected sites. The system was designed to include a response headquarters, a national reaction team, and regional teams. These teams were the forerunners, respectively, of the national and regional response teams.

The congressional passage of the Clean Water Act in 1972 led to the revision of the NCP in 1973 to incorporate a plan for the response not only to oil spills, but also to hazardous substance spills. In 1980, Congress passed the Superfund legislation, or the Comprehensive Environmental Response, Compensation, and Liability Act. As a result, the scope of the NCP grew to include the release of substances at hazardous waste sites where emergency removal actions are required. Passage of the Oil Pollution Act of 1990 prompted more changes to the NCP in 1994.

The Emergency Response Program. The principal aims of the Emergency Response Program are to take necessary steps toward the prevention of oil spill and hazardous substance emergencies; to prepare local, state, and federal emergency response personnel to deal with such situations; and to respond in a timely and effective manner to incidents as those arise.

The Emergency Response program involves coordination of the ten superfund regions into which the nation is divided geographically, and of five EPA organizations. The latter include the Office of Emergency and Remedial Response, which directs domestic emergency responses; the Chemical Emergency Prevention and Preparedness Office, which oversees responses to chemical emergencies; the Prevention, Pesticides, and Toxic Substances

program, which mobilizes community resources; the Radiation program; and the Office of Underground Storage Tanks, which protects against the release of petroleum from underground tanks.

An example of the EPA emergency response teams at work alongside their counterparts from other federal agencies occurred in the aftermath of the September 11, 2001, terrorist attacks, when the EPA sent more than 200 personnel to the World Trade Center and Pentagon sites. Among their ranks were specialists whose roles are not commonly associated with EPA in the public imagination, including criminal investigators, forensic scientists, and technical experts.

FURTHER READING:

BOOKS:

An Overview of the Emergency Response Program. Washington, D.C.: U.S. Environmental Protection Agency, 1992.

PERIODICALS:

Hogue, Cheryl. "Regulators at Scenes of Attacks." *Chemical & Engineering News* 79, no. 39 (September 24, 2001): 11.

Wallgren, Christine. "EPA Team Does Its Work Behind the Scenes." *Boston Globe.* (August 1, 2002): 1.

ELECTRONIC:

Emergency Response Program. U.S. Environmental Protection Agency. <http://www.epa.gov/superfund/programs/er/> (February 23, 2003).

U.S. National Response Team. <http://www.nrt.org/production/nrt/home.nsf> (January 22, 2003).

SEE ALSO

Chemical Safety: Emergency Responses
Coast Guard National Response Center
EPA (Environmental Protection Agency)
National Response Team, United States

Encryption of Data

LARRY GILMAN

Data are any useful information and encryption is any form of coding, ciphering, or secret writing. Encryption of data, therefore, includes any and all attempts to conceal, scramble, encode, or encipher any information. In the modern world, however, the term data usually implies digital data, that is, information in the form of binary digits ("bits," most often symbolized as 1s and 0s). Digital data are stored, transferred, and processed in increasingly large quantities at virtually every level of government and in the private sector, especially in industrialized countries. Money is transferred between accounts or disbursed from automatic teller machines on the basis of exchanges of digital data; medical records, criminal records, tax records, personal documents and telephone conversations, business negotiations, diplomatic communications, and military communications are all, almost without exception, cast into digital form before being transmitted or stored. All transmission media are vulnerable, however, to interception, and stored records may be accessed by unauthorized persons. The need for encryption of digital data is almost universal; anyone who transfers or stores important digital data has an interest in its security.

Governments have always had the strongest interest in data encryption, both as users of ciphering and coding systems (cryptosystems) and as attackers of the cryptosystems of other governments. The United States government, for example, uses encryption for transmission not only of classified (officially secret) data, but also of many unclassified data. Encryption is thus, distinct from classification. Classification is the official assignment of a particular degree of secrecy to data, whereas encryption refers to the translation of data, classified or not, into a form that is difficult for unauthorized parties to read.

Methods of encryption. Because digital data are numerical, their efficient encryption demands the use of ciphering rather than coding. A cipher is a system of rules for transforming any message text (the plaintext) into an apparently random text (the ciphertext) and back again. Digital computers are ideal for implementing ciphers; virtually all ciphering today is performed on digital data by digital computers.

The U.S. military, the State Department, and the intelligence agencies (including the Central Intelligence Agency, Federal Bureau of Investigation, National Security Agency [NSA], and others), utilize a variety of secret ciphering methods or "cryptosystems," whose nature is classified and about which little information is publicly available. The NSA, which is dedicated to eavesdropping—that is, to the collection of "signals intelligence" (sigint) both in the U.S. and globally, devotes millions of dollars annually to the breaking of ciphers and codes, and is the world's leading employer of mathematicians and purchaser of computer hardware. In the military, different cryptosystems are employed to achieve different levels of security, ranging from person-to-person communications on the battlefield to the exchange of messages with nuclear submarines at sea and other critical, high-end applications where budgets run high.

Government departments handling nonclassified information, industrial and academic organizations, and private individuals produce and transmit even greater quantities of data than do the military, intelligence agencies, and other handlers of classified data. Because of both the private sector and governmental need for reliable, standardized ciphering of nonclassified data, the National Bureau of Standards (an arm of the federal government) first solicited proposals for "cryptographic algorithms for

protection of computer data during transmission and dormant storage" in 1973 (*Federal Register* 38, No. 93, May 15, 1973). An algorithm developed by German-American cryptographer Horst Feistel, then working for IBM, was eventually chosen as the federal Data Encryption Standard (DES) on July 15, 1977. All information about the DES cipher algorithm is public and no licensing fees need be paid by anyone who wishes to incorporate it into a product. Thus, from 1977 to the present, DES has been built into thousands of data products, becoming among the most widely used cipher in history.

DES is a block cipher, meaning that it chops the message bitstream into blocks or sequences of 64 bits each, then produces a 64-bit ciphertext block by processing the message block through an algorithm (series of mathematical operations) governed by a key (secret number, in this case a 56-bit binary number). The ciphertext block appears to be a random string of bits; to recover the original message block, the 56-bit key that was used to encipher it must be given, stolen, or guessed.

When first implemented, DES was effectively unbreakable—except, probably, by the NSA, which reportedly lobbied the National Bureau of Standards to keep the key length down to a level that NSA supercomputers could cope with. Key length is a basic aspect of cipher security because any cipher can in theory be cracked by the brute-force method known as exhaustion, that is, the trying out of every possible key. In the case of DES, there are 2^{56} > 72,000,000,000,000,000 (72 x 10^{16}) possible keys. For many years, DES-enciphered data were safe because few organizations possessed the computing power to test 72 x 10^{16} keys in a reasonable time, but this ceased to be true several years ago. In July, 1998, a team of cryptographers cracked a DES-enciphered message in 3 days by the exhaustion method, and in 1999 a network of 10,000 desktop PCs cracked a DES-enciphered message in less than a day. DES was clearly no longer invulnerable, but a replacement was not yet in view; users therefore switched to an algorithm termed "triple DES." Triple DES encrypts a plaintext block using one 56-bit key, re-encrypts the resulting ciphertext block using a second 56-bit key, and then re-re-encrypts the result of the second encryption using a third 56-bit key. However, cryptographers have determined that triple DES is unsatisfactory as a long-term solution, and in 1997, the National Institute of Standards and Technology (NIST) solicited proposals for a cipher to replace DES entirely, the Advanced Encryption Standard (AES).

An algorithm named Rijndael (pronounced RAIN doll), created by Belgian cryptographers Vincent Rijmen and Joan Daemen, was announced as the AES in December, 2001 (Federal Information Processing Standard 197). AES is structurally similar to DES—both are block ciphers, for example—but AES uses blocks and keys that are 128, 192, or 256 bits long (at the user's discretion—longer blocks and keys entail slower processing), rather than a mere 56 bits long as in the original DES. According to the NIST, a computer that could try out all possible 56-bit DES keys in one second would require approximately 1.49 x 10^{14} years to try out all possible 128-bit AES keys. Triple DES is still the most commonly-used cryptosystem for the encryption of data and will remain an approved cryptographic standard for the foreseeable future; however, AES has started appearing in commercial products.

Encryption scientists expect that AES will remain secure for at least twenty years. However, in September 2002, two cryptographers—Nicolas Courtois of France, and Josef Pieprzyk of Australia—announced that they had designed an attack on AES that would reduce the number of calculations to crack the cipher from order 2^{256} (for the longest key option) to order 2^{100}. This remains beyond the capabilities of present-day computers, but raises concern for the long-term security of AES.

Both DES and AES are symmetrical-key cryptosystems, meaning that both the sender and receiver must be in possession of an identical secret key to encrypt and decrypt messages to each other. Systems based on public-key cryptography have also become important in the last decade or so, especially the RSA system (named for its inventors, Ronald Rivest, Adi Shamir, and Leonard Adleman). Public-key systems are widely favored for occasional transmissions among networks of users, rather than for dedicated links. RSA has been licensed to the makers of Web browsers such as Netscape and Explorer, allowing their users to employ public-key cryptography for sending encrypted e-mails, making online purchases, and doing online banking (most often without knowing that they are employing cryptography at all). RSA has also been used, without authorization, in the freeware program known as PGP (pretty good privacy). PGP can be downloaded for free from a number of Web sites for personal use.

■ FURTHER READING:

BOOKS:

Meyer, Carl H., and Stephen M. Matyas, *Cryptography: A New Dimension in Computer Data Security.* New York: John Wiley & Sons, 1982.

Singh, Simon. *The Code Book.* New York: Doubleday, 1999.

PERIODICALS:

"Race to Pick a Better Cipher." *Science* no. 5382 (1998): 1411.

Seife, Charles. "Crucial Cipher Flawed, Cryptographers Claim." *Science* no. 5590 (2002): 2193.

ELECTRONIC:

National Institute of Standards and Technology. "Advanced Encryption Standard: Questions and Answers." Computer Resource Security Center. March 5, 2001.<http://csrc.nist.gov/encryption/aes/round2/aesfact.html> (November 16, 2002).

Nechvatal, James, et al. "Report on the Development of the Advanced Encryption Standard." National Institute of Standards and Technology. October 2, 2000.

<csrc.nist.gov/encryption/aes/round2/r2report.pdf> (Nov. 16, 2002).

SEE ALSO

Codes and Ciphers

Enduring Freedom, Operation

JUDSON KNIGHT

Operation Enduring Freedom was the initial United States military response to the attacks of September 11, 2001, in which almost 3,000 Americans and other nationalities were killed by members of the al-Qaeda terror network. When the Taliban, Islamist extremists who controlled Afghanistan, refused to surrender al-Qaeda leader Osama bin Laden, the United States launched its attack the following month on October 7. The operation, initially named "Infinite Justice," was accompanied by a homeland security military effort named Noble Freedom. A part of Enduring Freedom was Operation Anaconda, an undertaking to root out al-Qaeda and Taliban personnel in northern Afghanistan. With the success of Enduring Freedom in 2002, the United States would go on a year later to the second phase of its war on terrorism: Operation Iraqi Freedom.

Stages of the Conflict

After the bombing of two U.S. embassies in Africa in 1998, the administration of President William J. Clinton conducted retaliatory air strikes on a terrorist training camp in Afghanistan, where bin Laden was believed to be in hiding. The air strikes failed to neutralize al-Qaeda, however, and after September 11, President George W. Bush demanded that the Taliban turn bin Laden over to the United States.

The Taliban stalled for weeks, claiming no knowledge as to bin Laden's whereabouts, while the Bush administration prepared for war. Rather than undergo a lengthy process of obtaining United Nations approval for a multinational force, Bush called on the help of America's major ally among the major world powers: the United Kingdom. (Canada and Australia later also contributed troops to the coalition force.) On October 7, U.S. and British forces launched air strikes against Afghanistan.

On October 25, approximately 25 aircraft (including 15 carrier-based tactical planes and eight to 10 long-range bombers) struck seven strategic targets, including military training facilities, surface-to-air missile storage sites, and al-Qaeda infrastructure. By November 9, the northern city of Mazar-e-Sharif had fallen to the Northern Alliance, a loose coalition of Afghan factions opposed to the Taliban. Four days later, a combination of allied air assaults and ground maneuvers by the Northern Alliance forced the Taliban to surrender Kabul, the capital, and on November 17, the Taliban confirmed that al-Qaeda military chief Mohammed Atef had been killed in the allied bombing.

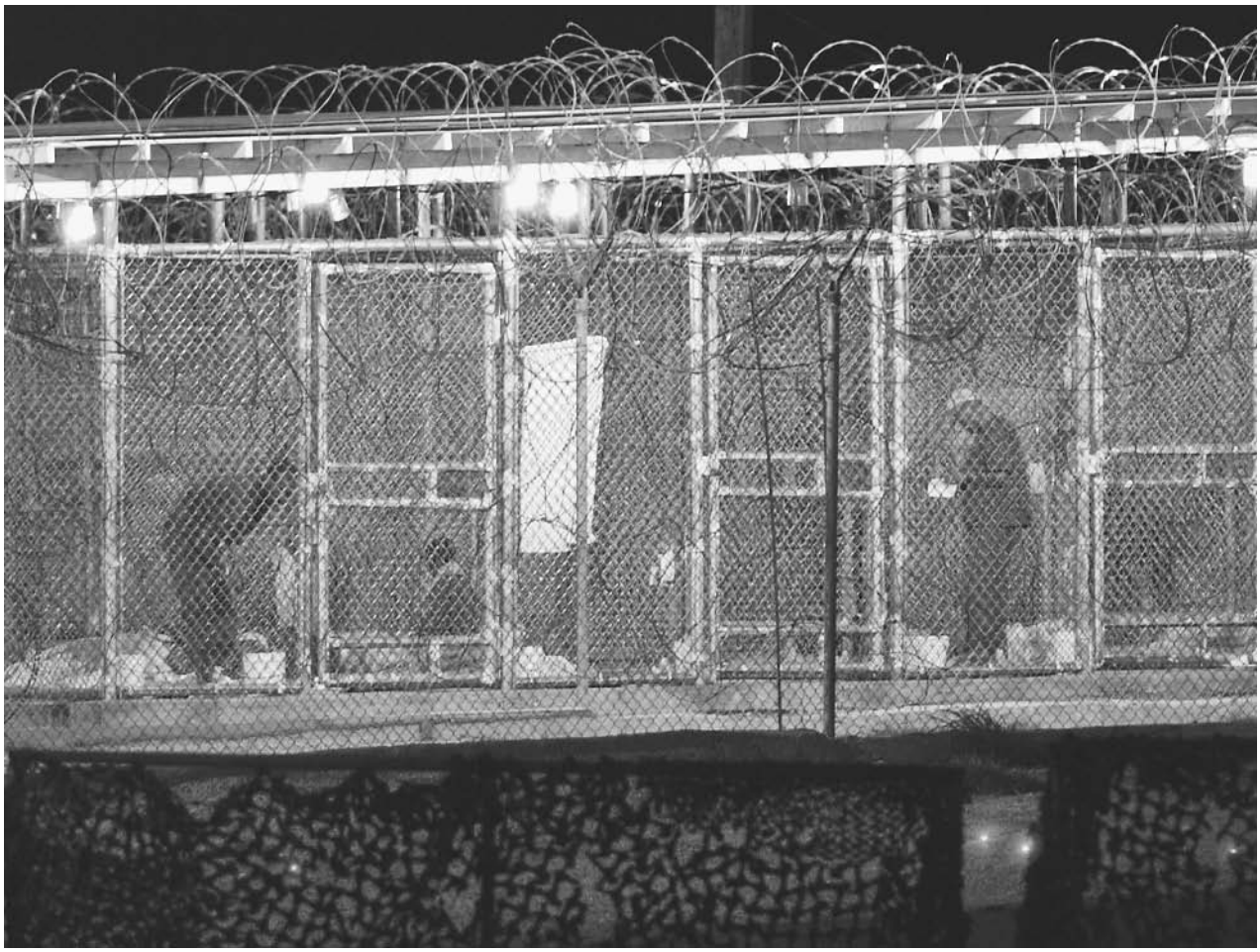
Near the beginning of the war's eighth week, on November 25, Central Intelligence Agency officer Johnny "Mike" Spann became the first combat casualty when he was killed in an uprising at Mazar-e-Sharif. Three U.S. soldiers were killed, and 19 wounded, when a U.S. bomb missed its target on December 2.

In December 2001, one dramatic phase of the war ended as the Taliban surrendered their last major stronghold in the southern city of Kandahar on December 7. Both bin Laden and Taliban leader Mullah Muhammad Omar apparently escaped from the city. December 16 saw the fall of Tora Bora, a cave complex where al-Qaeda and Taliban holdouts had hidden. Six days later, on December 22, Hamid Karzai was sworn in as chairman of a six-month interim government. Women, treated as slaves under Taliban rule, could again vote, participate in government, and receive an education.

Early 2002: Operation Anaconda. On January 4, 2002, U.S. Army Sergeant First Class Nathan Ross Chapman became the first member of the U.S. military to be killed by hostile fire. Fighting continued in spurts until March 2, the launch of Operation Anaconda. The largest ground operation of the war, Anaconda involved some 2,000 U.S., Afghan, and allied troops, and would result in eight U.S. deaths. Its purpose was to eliminate Taliban and al-Qaeda fighters still holding out in the mountains of southeastern Afghanistan. But as the mission came to a close some two weeks later, assessment of its success was difficult.

Over the course of an 11-day battle near Shah-i-Kot, for instance, U.S. military commanders had been forced to reassess original estimates of enemy strength in the region upward from 150 or 200 to 1,000. As that part of the offensive came to a close on March 17, it appeared that the U.S. military had produced as many as 800 enemy casualties, but numbers were difficult to determine. In any case, civilian and military leaders were not inclined to evaluate the offensive in terms of body counts—a lesson learned from the Vietnam War a generation earlier.

Infinite Justice and Noble Eagle. Enduring Freedom, as the larger operation came to be known in November, was initially called Infinite Justice. The change resulted from concerns that the original name had religious connotations, suggesting that God was on the side of the coalition forces. (Similarly, in the wake of the September 11 attacks, Bush had once mentioned a "crusade," an unfortunate choice of words that played right into the terrorists' claims that the war on terrorism was an attack by Christians against Islam.). Still, the coalition took extraordinary measures, including dropping thousands of leaflets and radio



Illegal combatants and terrorist supporters from Operation Enduring Freedom in Afghanistan being held at Camp X-Ray, on the US naval base in Guantanamo Bay, Cuba. AP/WIDE WORLD PHOTOS.

broadcasts, to assure the population of Afghanistan that the warfare was directed at eliminating al-Qaeda terrorists, not the practitioners of Islam.

Accompanying Enduring Freedom was Noble Eagle, a military operation designed to safeguard homeland security during the war in Afghanistan. The U.S. Coast Guard (USCG), principal guarantors of stateside port security, played a central role in Noble Eagle. USCG deployed 55 cutters (small armed vessels), 42 aircraft, and hundreds of boats to establish port and coastline patrols. It also called up more than 2,800 reservists to support homeland security operations at the country's 361 ports.

■ FURTHER READING:

PERIODICALS:

"Black September 11." *Air Force Magazine* 95, no. 9 (September 2002): 46–53.

Blumenstein, Rebecca, and Matthew Rose. "Name that Op: How U.S. Coins Phrases of War." *Wall Street Journal.* (March 24, 2003): B1.

"Enduring Freedom." *New York Times.* (August 11, 2002): 4.

"Military Operations Named." *Marine Corps Gazette* 85, no. 11 (November 2001): 4.

Thompson, Loren B. "The Lessons of 'Enduring Freedom'." *Wall Street Journal.* (January 7, 2002): A24.

ELECTRONIC:

Operation Enduring Freedom. U.S. Army. <http://www.army.mil/operations/oef/index.html> (April 4, 2003).

———. U.S. Navy Office of Information. <http://www.chinfo.navy.mil/navpalib/news/news_stories/pentstruck.html> (April 4, 2003).

Operations Enduring Freedom and Noble Eagle. U.S. Air Force. <http://www.af.mil/news/efreedom/index.shtml> (April 4, 2003).

SEE ALSO

Bush Administration (2001–), United States National Security Policy
Clinton Administration (1993–2001), United States National Security Policy
Enduring Freedom, Operation
Iraqi Freedom, Operation (2003 War Against Iraq)

Persian Gulf War
September 11 Terrorist Attacks on the United States
Vietnam War

Energy Directed Weapons

LARRY GILMAN

Weapons that use energy to disable or destroy equipment or people are referred to as energy directed weapons. Examples include lasers, high-power microwave weapons, and charged particle beam weapons.

The genesis of energy directed weapons was the work of Albert Einstein. Einstein's 1905 Special Theory of Relativity related electric and magnetic forces in the equation $E=mc^2$. The equation demonstrated that even particles of small mass moving at the speed of light possess tremendous energy.

Energy directed weapons concentrate large amounts of energy at a specific wavelength and frequency and then direct the beam of energy at the intended target. Because the particles are moving at a speed that approaches the speed of light, the beam will have a devastating amount of energy.

Rationale for energy directed weapons. Those who favor energy directed weapons argue that their development would increase the ability to fight and win a conflict.

In theory, energy directed weapons would operate at or near the speed of light. Even rapidly moving missiles would be essentially motionless to the beam. For example, a missile 50 kilometers away moving at 20,000 feet per second would only move five feet from the time a energy weapon was "fired" until contact. As well, the weapons could operate over thousands of kilometers, even in space. Finally, as long as there was power to generate the high energy, no other ammunition is required.

The use of energy directed weapons in space, particularly on Earth-orbiting satellites, has been proposed. One reason is that conventional weapons do not operate well or at all in the semi-vacuum of Earth orbit. Energy directed weapons face no such limitation. Another reason is the proliferating use of space for offensive weapons. In 1972, only nine nations were known to have ballistic missiles. By 2001, this number had grown to at least 28 nations. This increase has bolstered the argument for the ability to defend and if necessary retaliate from space.

Laser weapons. A laser—an acronym for "light amplification by stimulated emission of radiation"—emits a tightly focused beam of specific radiation that does not diverge from the beam path. Chemical lasers use reactive energy between compounds (i.e., oxygen/iodine and deuterium/fluoride). Solid state lasers use electricity to produce the beam. Chemical lasers currently produce much more energy than do solid-state lasers. This power, however, comes at the expense of a large volume for the great quantities of chemicals required.

High power laser light can damage or permanently destroy the eyes, and obliterate objects in its path. For example, a weapon called the Saber 203 is a "laser grenade" that is capable of temporarily blinding those in the path of the ray. The weapon was deployed, but never used with United States troops during the 1990 Gulf War, and with troops deployed to Somalia in 1995. Another weapon called the Dazer fires up to 50 laser pulses per minute. It is being used by U.S. Special Operations Command forces.

Research by the U.S. Army and Navy to develop lasers for air and sea has been underway since the early 1970s. A chemical laser weapon capable of being mounted on the next generation of fighter jet (Joint Strike Fighter) and destroyer (DDX) is scheduled to be ready for testing in 2010. As of 2002, a chemical laser was to be built aboard a modified Boeing 747 aircraft. The airborne chemical laser, which will be the first in the U.S., is controversial because of the possibility of environmental damage from the chemicals carried aboard the aircraft.

Military use of lasers is currently confined to low-power units that measure the distance to a target or help aim other weapons. Lasers could become much more formidable weapons. For example, experts agree that a 25 to 100 kilowatt laser would be powerful enough to disable equipment hundreds of miles away, and could burn through metal, such as the outer casing of a missile, dozens of miles away.

High-power microwave weapons. High-power microwave (HPM) weapons are also known as Radio Frequency weapons and Ultra-Wideband weapons. HPM weapons have been in development by the United States, Russia, China, and other countries for decades. The weapons produce high-energy bursts; a typical HPM weapon consists of a power source that can be electrical or explosive, a microwave generator, and an antenna to direct the beam of radiation. The intense surge of energy that is emitted disables electronics in vehicles, communications equipment, and other weapons. Such a weapon was successfully field tested by the U.S. in April 2001.

Particle beam. Development of the particle beam weapon (PBW) began in the U.S. in the late 1950s, under the code name Seesaw. A PBW operates by accelerating components of a hydrogen atom—either the negatively charged electron or the positively charged proton—to almost the speed of light, and then focusing these atoms into a beam. The destructive power of the particle beam is due to the collision of the positively or negatively charged ions with

A U.S. Navy pilot inspects the laser guided weapons aboard his F/A-18C Hornet prior to his mission from the aircraft carrier USS *Theodore Roosevelt*. AP/WIDE WORLD PHOTOS.

the atoms of the target. The energy transfer causes an explosion, which obliterates the target.

The charged version of a particle beam weapon would be utilized where there is an atmosphere. The neutral particle beam weapon, which is not as powerful, is more suitable to the friction-free atmosphere of space, where it retains enough power to be destructive. A space version of a PBW does not yet exist. Among the developmental limitations is an aiming system capable of accuracy over thousands of kilometers, and the maintenance of a tightly focused beam over such vast distances (a beam composed of like-charged particles will tend to broaden out, as the particles repel one another).

Limitations and criticisms of energy directed weapons. Because energy directed weapons are beamed at the target, they are "line of sight" weapons. Unless technological changes allow the beams to be precisely bent or reflected, objects that are not directly in front of the beam will not be targeted. In contrast, a conventional weapon such as bomb can destroy its target even when the weapon is slightly off the intended destination. Furthermore, laser beams are blocked by clouds, limiting their use to all but fair weather.

Those who oppose energy directed weapons argue that civilian casualties and infrastructure damage will be greater than with the present methods of warfare. Also the weapons could be an ideal terrorist tool. The source of energy directed weapons could be disguised, and no traces are left behind.

The collateral effects of energy directed weapons such as lasers are still unclear. While an enemy target would certainly be disrupted or even destroyed, the possibility of damage to civilian structures (i.e., equipment in hospitals) or civilians themselves (i.e., disruption of pacemakers) has made the deployment of energy directed weapons controversial. Even if the energy weapon can be contained in a relatively narrow beam prior to the strike, dispersion of the energy at ground level will likely occur. It is this traveling shock wave of energy that could produce the collateral damage.

■ FURTHER READING:

BOOKS:

Duffner, Robert. *Airborne Laser: Bullets of Light*.New York: Plenum Trade, 1997.

ELECTRONIC:

In These Times. "Now You See, Now You Don't." The Institute for Public Affairs. September 27, 2002. <http://www.inthesetimes.com/issue/26/24/news1.shtml>(17 December 2002).

Lexington Institute,1600 Wilson Boulevard, Suite 900, Arlington VA 22209. (703) 522–5828. <http://www.lexingtoninstitute.org/defense/energyforum_thompson.htm>.

SEE ALSO

DARPA (Defense Advanced Research Projects Agency)
Electromagnetic Weapons, Biochemical Effects
Lawrence Livermore National Laboratory (LLNL)

Energy Regulatory Commission, United States Federal

The U.S. Federal Energy Regulatory Commission (FERC) is an independent regulatory agency within the Department of Energy (DOE) responsible for regulating energy utilities nationwide. As such, it has a significant oversight role in America's critical infrastructure. In the aftermath of the September 11, 2001, terrorist attacks, FERC has worked to help ensure protection of information concerning energy utilities.

FERC is responsible for regulating, in interstate commerce, the transmission of oil by pipeline, the transmission and sale of natural gas for resale, and the transmission and wholesale sales of electricity. It also licenses and inspects private, municipal, and state hydroelectric projects, approves site choices, and plans for abandonment, of interstate pipeline facilities; and oversees environmental issues as these relate to natural gas, oil, electricity, and hydroelectric power projects. Additionally, FERC administers the accounting and financial reporting regulations, and the conduct of jurisdictional utility companies.

At the time the Department of Energy Organization Act established DOE on October 1, 1977, the national utilities oversight organization was known as the Federal Power Commission (FPC). The FPC was later disbanded and FERC established in its place. FERC's membership comes from five presidential appointees, no more than three of whom may belong to the same political party. Its members, whose appointments are made with the advice and consent of the Senate, serve terms of five years. Although there is a chairperson designated by the president, all members have equal voting power.

In the atmosphere of heightened security consciousness that emerged after the September, 2001 terrorist attacks, FERC has worked with entities in the private and public sectors to ensure greater protection of interstate utilities. In September 2002, FERC proposed new rules limiting public access to information on power plants, pipelines, and other aspects of critical infrastructure as it relates to energy. Information that had been easily available on its Web site would thenceforth be granted purely on a need-to-know basis.

FURTHER READING:

PERIODICALS:

"FERC Streamlining to Reflect Industry." *Oil & Gas Journal.* 96, no. 26 (June 29, 1998): 33.

Gips, Michael A. "They Secure the Body Electric." *Security Management* 46, no. 11 (November 2002): 77–81.

Matthews, William. "Energy Agency Says Web Info Poses Threat." *Federal Computer Week* 16, no. 34 (September 23, 2002): 46.

ELECTRONIC:

Federal Energy Regulatory Commission. <http://www.ferc.fed.us/> (February 23, 2003).

SEE ALSO

Critical Infrastructure Assurance Office (CIAO), United States
DOE (United States Department of Energy)

Energy Technologies

LARRY GILMAN

Energy technologies are techniques for moving energy from a source to a point of use, for transforming it from an original source-form to an end-use form, or both. They are often lumped into two groups, conventional and alternative. Conventional energy technologies derive energy from fuels, either fossil (coal, oil, natural gas) or nuclear (uranium, plutonium). These technologies first turn the energy latent in fuel into heat, then transform some percentage of that heat into another, more useful form of energy (or apply the heat directly, as to warming a building, smelting ore, or the like). Approximately 90% of present-day energy use is provided by conventional sources.

Alternative energy technologies, in contrast, harvest energy from renewable, natural flows rather than from fuels. Technologies that collect energy from sunlight, wind, wave action, or plants are considered alternative energy technologies. (An exception to the alternative/conventional classification scheme is hydroelectric power, the generation of electricity from water flowing downhill. Hydroelectric power, although it harvests an energy flux from the environment rather than burning a fuel, is usually considered conventional because it has been utilized on an industrial scale for so long.)

Many energy technologies, conventional and alternative, produce electricity. Electricity is a uniquely useful form of energy, not a source of energy. Thus, the belief that an electric-powered device such as an electric car is "clean" is only correct when the electricity that it uses is produced cleanly. Most electricity is produced by coal-burning power plants or nuclear power plants; the former

involves environmentally destructive mining and air pollution, while the latter involves some environmentally destructive mining and produces growing inventories of radioactive material that might be released to the environment either accidentally or deliberately, as by wartime or terrorist action. Therefore, there is nothing intrinsically "clean" about electricity. About 51% of United States electricity is currently produced by coal-burning power plants, 21% by nuclear power plants, 17% by natural-gas-fired power plants, 6% from hydroelectric dams, 3% from oil-fired power plants, and 2% from wind, wood, and photovoltaics.

Several national-security issues arise with respect to energy technologies:

(1) *Self-sufficiency.* An energy source that must be imported, such as oil, is vulnerable to cutoff by hostile parties. This was demonstrated by the oil crisis of 1973, when the Organization of Oil Producing Countries (OPEC) suddenly quadrupled its oil prices from about $3 to about $13 per barrel (1 barrel = 42 United States gallons or 159 L) in retaliation for United States support of Israel. This triggered an economic crisis in the United States and elsewhere. In contrast, the United States has large domestic stocks of coal and uranium, and is not vulnerable to a cutoff of these energy sources; nor is it entangled politically or militarily with foreign sources of these fuels, as is the case with oil. (However, coal and uranium produce electricity, which, unlike oil, does not yet run affordable cars; therefore, coal and uranium cannot, at present, significantly decrease United States dependence on foreign oil.) Renewable or alternative energy resources also have the advantage that they are not imported.

(2) *Fragility.* Energy sources that can be disrupted at central points or along key transmission routes are more vulnerable to terrorism and war than distributed energy sources. For example, much of the United States electrical grid—a tuned, interdependent, dynamic network—could be blacked out for days or weeks by the destruction of relatively few switching points, control centers, or transmission lines. Locally-harvested alternative-energy sources such as rooftop photovoltaics or woodlots are immune to large-scale disruption, but cannot serve all purposes; rooftop photovoltaics are still expensive relative to grid electricity, and there are no wood-burning computers or refrigerators. Between the resilience of locally-produced energy supplies and the brittleness of the coal- and nuclear-fueled electrical grid lie the energy systems that rely on distributed stocks of fuels such as gasoline and natural gas. Although these energy technologies still rely on a few centralized refineries or long-distance pipelines, they are tolerant of temporary or local damage.

(3) *Hazardousness.* Some energy sources are hazardous due to toxicity or explosive potential. Standard nuclear power plants cannot explode, but they do contain large inventories of radionuclides that could be deliberately released by an enemy; after the terrorist attacks of September 11, 2001, the United States Nuclear Regulatory Commission ordered immediate, drastic increases in security for nuclear power plants. A less well-known source of vulnerability is liquefied natural gas, which is imported to the United States in large tanker ships and stored in centralized tank farms for national distribution via long-distance pipelines.

(4) *Pollution.* Pollution or greenhouse-gas emissions that harm a country's citizens, environment, and economy can be thought of as a danger to national security. All sources of energy, including wind and solar, require the extraction and refinement of metals and other substances, some toxic; conventional sources further require the extraction and (often) refinement of fuels and either (a) release combustion products to the atmosphere or (b) require the near-perfect, near-perpetual containment of increasing quantities of radioactive materials.

(5) *Adequacy.* Whatever combination of energy technologies is used by a modern industrial state, its energy system must provide *sufficient* energy. The present energy system of the U.S.—primarily gasoline for transport, coal and nuclear (primarily) for electrical generation, and oil for heating some buildings—does supply adequate energy; however, some experts maintain that given increased end-use efficiency, the industrialized countries could shift almost entirely to alternative energy sources in about 50 years. If technically feasible this would increase self-sufficiency and decrease fragility, hazardousness, and pollution, but is not likely to occur without a major shock, or several major shocks, to the conventional energy system, as for example a major terrorist act involving a nuclear power plant, a second oil embargo, or radical climate change. In the meantime, prices are falling slowly for alternative energy sources, especially wind and solar, making them increasingly competitive on the market with conventional electricity sources. Gasoline continues to be the only affordable energy source for most vehicles, with the mileage of the United States fleet recently declining rather than rising.

One change in the present U.S. energy system that, if technically feasible, would increase self-sufficiency by decreasing dependence on oil and which would also decrease pollution is a long-term shift (probably only partial) to hydrogen "burned" in fuel cells. Fuel cells are chemical reactors in which a fuel (not necessarily hydrogen) combines with oxygen to create electricity, with water vapor as the only by-product. Hydrogen is available on Earth only in chemically stable combination with other substances (e.g., in H_2O); it is therefore not a primary fuel but, like electricity, a *form* of energy, and must be manufactured either by using electricity to split water molecules or by chemical processing of a fuel such as coal. Although hydrogen is not currently available in large quantities and fuel cells remain expensive (i.e., about 10 times as expensive, per horsepower delivered, as a conventional automobile engine), U.S. President George W. Bush has announced two funding programs for hydrogen fuel cells:

Freedom Car (2002) to accelerate development of hydrogen-powered automobiles, and Freedom Fuel (2003), to accelerate development of techniques for manufacturing hydrogen from coal. Freedom Car receives about $50 million per year, and Freedom Fuel has been allotted $144 million per year for five years. The announced goal of the twin programs is to make fuel-cell powered cars commercially available in 20 years. The United States is working in partial cooperation with the European Union, which also seeks to develop hydrogen-powered fuel cells for cars. The European Union's program, unlike the U.S. Freedom Fuel program, seeks to produce hydrogen using electricity generated by wind and solar power.

FURTHER READING:

BOOKS:

Brockris, J. O'M. *Energy Options.* Redfern NSW, Australia: Halsted Press, 1980.

Lovins, Amory, and L. Hunter Lovins. *Brittle Power: Energy Strategy for National Security.* Andover, MA: Brick House Publishing, 1982.

PERIODICALS:

Banerjee, Neela. "U.S. and Europe in Fuel Cell Pact." *New York Times.* March 7, 2003.

SEE ALSO

DOE (United States Department of Energy)

Former Treasury Secretary Paul O'Neil, left, looks at newly-printed bills with a Bureau of Printing employee during a tour of the Western Currency facility in Fort Worth, Texas. AP/WIDE WORLD PHOTOS.

Engraving and Printing, United States Bureau

The United States Bureau of Engraving and Printing (BEP) is the largest producer of security documents in the nation. Although it is most widely known for the production of Federal Reserve notes, paper currency is only one of many printed materials that originate from its facilities in Washington, D.C., and Fort Worth, Texas. BEP is also responsible for printing postage stamps, identification cards, Treasury securities, and other sensitive documents.

Background. BEP had its beginnings in 1862, when a small room in the basement of the Treasury building in Washington was set aside for the separating and sealing, by hand, of United States $1 and $2 notes printed by private companies. Over time, BEP's mission expanded as it began to produce some currency notes, as well as revenue stamps, certificates recording obligations of the U.S. government, and a variety of other security documents authorized by various governmental departments. BEP became the sole authorized producer of U.S. paper currency in 1877, and in 1894 began producing postage stamps.

By 1985, officials at the Treasury Department had become aware of the need for a BEP facility west of the Mississippi River, which would reduce the cost of transporting notes to Federal Reserve banks in San Francisco, Dallas, and Kansas City. Treasury therefore authorized BEP officials to accept proposals from potential host cities, for which there were 83 applications. In November 1986, BEP chose Fort Worth, and in 1987 began building what is today known as the Western Currency Facility. The design of the building, which in 1991 received an award from the local chapter of the American Institute of Architects, includes a glass pyramid intended to replicate the truncated pyramid on the reverse side of a one-dollar bill.

Production. Today BEP continues to produce all paper money in the United States, while the United States Mint produces all coins. Both distribute their products solely through the Federal Reserve System, which in turn issues

currency and coinage solely through member financial institutions. BEP is also responsible for the processing of claims for the redemption of mutilated currency. Its research and development department is concerned with anti-counterfeiting technology, which is perpetually upgraded in an effort to remain many steps ahead of counterfeiters.

Although the production of U.S. currency is perhaps the most visible of BEP's activities, it is far from the only one. BEP produces a number of stamps and notes, including postage stamps for the United States Postal Service, license stamps such as those used on alcohol products, and Treasury securities. The lowest-value note ever issued by BEP was a $0.002, or one-fifth cent, wine stamp, while the item of highest value was a $100,000,000 International Monetary Fund special note. BEP has also manufactured currency for other nations, including pre-Communist Cuba.

BEP produces federal identification cards, certificates of naturalization, and other security documents as requested by particular government agencies. Among its most specialized products are engraved White House invitations.

FURTHER READING:

BOOKS:

History of the Bureau of Engraving and Printing, 1862–1962. Washington, D.C.: Treasury Department, 1964.

The Money Factory. Washington, D.C.: Bureau of Engraving and Printing, 1993.

Sincerbox, Glenn T. *Counterfeit Deterrent Features for the Next-Generation Currency Design.* Washington, D.C.: National Academy Press, 1993.

ELECTRONIC:

Bureau of Engraving and Printing. <http://www.bep.treas.gov/> (February 5, 2003).

SEE ALSO

Counterfeit Currency, Technology and the Manufacture
Federal Reserve System, United States
Treasury Department, United States

Engulf, Operation

JUDSON KNIGHT

Engulf was a series of operations whereby the British Security Service, MI5, intercepted Egyptian and French cipher transmissions during a period from the mid-1950s to the mid-1960s. The first major operation of Engulf took place during the Suez crisis of 1956, when a team led by British spymaster Peter Wright planted a bug in the cipher room of the Egyptian embassy in London.

The Suez crisis began in July 1956, when Egyptian president Gamal Abdel Nasser seized the Suez Canal, formerly under the control of Britain and France. Britain and the United States, well aware of Nasser's increasingly close ties with the Soviet Union, had refused to fund Nasser's plans to build the Aswan High Dam. Therefore, Nasser took over the canal, not only as an act of retaliation, but as a means of raising money by collecting the tolls charged to ships passing through the canal. Britain and France, in a plan orchestrated with Israel, forced the evacuation of Egyptian troops, but were ultimately forced to themselves evacuate by the threat of United Nations or Soviet intervention.

In the months leading up to the crisis, MI5 undertook efforts to plant a listening device (bug) in the Egyptian embassy. The British postal service, which controlled telephone service, deliberately created problems with the embassy's phones, and an MI5 undercover team arrived under the guise of repairing the equipment. While there, they planted bugs that allowed them to hear the noises made by the setting of the machines. Skilled specialists were able to translate these noises into usable intelligence.

An unexpected conduit from Moscow to London. As Wright later recalled in his autobiography *Spycatcher,* intercepting the Egyptian cipher transmissions allowed MI5 to follow discussions between the Egyptians and Soviets in Moscow, the specifics of which were regularly passed on to the embassy in London. From these transmissions, the British learned that the Soviets were not simply bluffing when they threatened to intervene in Suez on the Egyptians' behalf.

Wright went on to recount that the Soviets helped their Egyptian allies by sweeping the London embassy for bugs, but when they discovered the device planted by MI5, they opted to leave it in place and not inform the Egyptians. By allowing MI5 to listen in to the Egyptian embassy, the Soviets were able to convey exactly where they stood on the Suez situation, and to do so in such a way that the British would know that they meant what they were saying.

Other phases. In later phases of Engulf, MI5 attempted to detect cipher noises in other contexts. In 1959, for instance, while the Soviet cruiser *Ordzhonikidze* was moored at Stockholm, Sweden, MI5 placed microphones in a nearby warehouse. This time, of course, there was no question of going aboard the ship under any pretext to plant a bug, and as it turned out, the warehouse was not close enough. Though MI5 did pick up what were apparently cipher machine noises, this did not lead to any usable intelligence.

From 1960 to 1963, in an operation known as Stockade, MI5 listened in to the French embassy in London. Unlike the Suez phase, however, reliable intelligence did not give the British any real diplomatic benefit. The United

Kingdom was attempting to join the European Economic Community (EEC) or Common Market, which in 1993 would become the European Union. France was attempting to keep Great Britain out of the EEC, and the bugging simply revealed that the French were not going to budge, without revealing any likely means of inducing them to do so. Wright, who also led Stockade, later recalled that the operation "was a graphic illustration of the limitations of intelligence."

FURTHER READING:

BOOKS:

Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence.* Woodstock, NY: Overlook Press, 2002.

Epstein, Leon D. *British Politics in the Suez Crisis.* Urbana: University of Illinois Press, 1964.

Kelly, Saul, and Anthony Gorst. *Whitehall and the Suez Crisis.* Portland, OR: Frank Cass, 2000.

Louis, William Roger, and Roger Owen. *Suez 1956: The Crisis and Its Consequences.* New York: Oxford University Press, 1989.

West, Nigel. *The Circus: MI5 Operations 1945–1972.* New York: Stein and Day, 1983.

Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer.* New York: Viking, 1987.

SEE ALSO

Cipher Machines
Egypt, Intelligence and Security
MI5 (British Security Service)
Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom
United Kingdom, Intelligence and Security

ENIAC Machine.

SEE *Ultra, Operation.*

Enigma

LARRY GILMAN

Enigma was a ciphering (code communication) system used by the German military from 1926 until the end of World War II, and by several other nations for some years after. Enigma was the first mechanized message-encryption system to see wide use. Enigma produced such thoroughly scrambled messages that for many years its cipher was considered unbreakable both by the German military and its foes. Polish and British mathematicians, however, cracked the Enigma cipher in time to give the Allies access to most German military communications throughout World War II. The German government never knew that the Enigma cipher had been broken and that its military communications were often transparent, giving a significant advantage to the Allies on many occasions. The Japanese military also used a cipher related to Enigma during World War II. The Japanese version of Enigma was cracked by American cryptographers, providing a crucial advantage to the Allies in the Pacific theater. U.S. knowledge of secrete Japanese transmissions was essential, for example, to victory at the crucial battle at Midway, the Japanese navy's first major defeat in several centuries. Many military strategists and historians hold that Allied success in cracking the Enigma and related ciphers helped significantly shorten World War II.

Origin of Enigma. During World War I, cumbersome paper-and-pencil ciphers were still the rule, as they had been for centuries past. (A *cipher* is any scheme for transforming ordinary written language—*plaintext*—into a coded, but apparently random string of characters, *ciphertext*.) After World War I, several inventors turned their attention to the mechanization of ciphering, seeking to increase accuracy, speed, and security. The most successful of these inventors was German engineer Arthur Scherbius, who in 1918, created a cipher machine he named the Enigma. (This is not a translation; the word "enigma" is the same in German and English). Scherbius was unsuccessful in selling Enigma to commercial buyers. It was not until 1923 that Enigma was chosen by the German government as its standard ciphering system, as Germany had only just learned how much damage had been done by the breaking of its ciphers by the Allies in World War I. Between 1925 and 1945, the German military bought over 30,000 Enigma machines, deploying slightly different systems to its European armies, its army in North Africa, its air force, and its navy.

The Enigma cipher. The Enigma cipher is built upon the simplest of all cipher types, the substitution cipher. In a substitution cipher, one letter of the alphabet is substituted directly for another. A substitution cipher for a six-letter alphabet might appear as:

Plaintext:	A B C D E F
Ciphertext:	F C A B D E

Using this cipher, the plaintext word BAD (for example) would produce the ciphertext word CFB. Such ciphers are easy to implement, but also contain easily broken code, as their ciphertext contains all the regularities of

A four-rotor Enigma machine, right, which was used by the crews of German U-boats in World War II to send coded messages. AP/WIDE WORLD PHOTOS.

ordinary language: that is, double letters in plaintext appear as double letters in ciphertext, the ciphertext letter for "e" will appear in the ciphertext just as often as "e" appears in plaintext, and so forth. Such codes are weak because analyzing regularities is one of the primary means by which codebreakers attack codes.

However, by adding complications to this simple idea, a powerful code can be devised. Consider the following substitution cipher for a three-letter alphabet:

Plaintext:	A B C
Ciphertext:	A C B

In this simple example, A is enciphered as itself. This cipher can be imagined as a physical device consisting of three disks or dials arranged in a row. The first (left-hand) and third (right-hand) disks, each of which has the alphabet ABC spaced evenly around its edge, are identical, and are aligned so that their letters are in the same positions; the third disk, which sandwiched between the other two, is different. It contains three wires that pass from its left side right through to its right, connecting the two alphabet disks so that the A of the left-hand disk is wired to the A of the right-hand disk, the B of the left-hand disk to the C of the right-hand disk, and the C of the left-hand disk to the B of the right-hand disk. In effect, the middle disk scrambles the alphabet. The result is a simple substitution cipher. If the middle disk, (the scrambler) is rotated, however, so that the wire which touched A on the plaintext disk now touches C on that disk, all the other letters on the plaintext and ciphertext disks will also be connected differently by the scrambler, producing the following substitution cipher:

Plaintext:	A B C
Ciphertext:	B A C

This can be verified by describing the wires in the scrambler as a set of input-output rules, one for each wire:

1) Connect input position 1 to output position 1.

2) Connect input position 2 to output position 3.

3) Connect input position 3 to output position 2.

By rule 1, when scrambler input position 1 is lined up with the letter A on the left-hand (plaintext) disk, it is connected to output position 1, which is lined up with the

letter A on the right-hand (ciphertext) disk. The other two substitutions are produced by the other two wires: B → C, C → B. When the scrambler is rotated so that its input 1 moves from A to C on the plaintext disk, its output 1 moves from A to C on the ciphertext disk. Now, instead of producing A → A, wire 1 produces C → C. The other two wires now produce the substitutions A → B, B → A. Thus, each time the scrambler is rotated by one letter position, a new different substitution code is produced. This continues until the scrambler returns to its starting position, whereupon the substitution codes produced by the device begin to repeat. In this example, repetition begins with the third shift of the scrambler.

Rotation of the scrambler can be used to make a cipher that is more formidable than a straightforward substitution. Consider a three-letter plaintext message is to be sent: ABA. First, A is enciphered with the scrambler in the first position described above: A → A. Before the second letter is encrypted, the scrambler disk is rotated by one letter-position. The second plaintext letter is then enciphered: B → A. The disk is rotated, and A is enciphered again: A → C. Although in this case one would start repeating substitutions after only three letters, the resulting cipher is significantly more complex, and thus harder to crack, than a static substitution cipher.

Decryption in this system is simple as long as the receiving party possesses an identical machine; the wires in the scrambler disk work equally well in either direction, so decryption is simply encryption run backwards. The receiver must, however, begin decrypting with their scrambler set to the same position as the sender's at the start of transmission, otherwise the substitution codes used by the receiver to decipher the message will be out of step with those used by the sender to encipher it, and decipherment will fail.

The Enigma system was based upon the scrambler-disk principle described above. Enigma used not a 3-letter, but a 26-character alphabet and not one, but four scrambler disks. The first scrambler scrambled plaintext or ciphertext, the second scrambler scrambled the outputs of the first scrambler, the third scrambled the outputs of the second, and the fourth fed back, or "reflected," the outputs of the third so that messages passed through the other three scramblers before the encrypted ciphertext (or decrypted plaintext) was read. Each letter was thus scrambled a total of seven times during its passage through the machine. Three of the scrambler disks could be rotated freely, but the fourth, the "reflector," was stationary.

In order to use an Enigma unit, its operator typed plaintext or ciphertext into a keyboard. For each keystroke typed, Enigma automatically shifted one or more of its scramblers and lit up a letter on a display board. The letter on the display board showed the output text for the typed input letter: ciphertext if plaintext was input, plaintext if ciphertext was input. To produce further scrambling between ciphertext and plaintext, each Enigma also had a built-in commutator or "plugboard" that enabled the operator to crisscross paired letters of the alphabet before their signals fed into the first scrambler disk. The result was that Enigma had over 10^{20} different "keys" or distinct settings of scramblers and plugboard. Simply guessing the correct key for a given message was, therefore, essentially impossible. Every day at midnight, all operators of a given Enigma system would switch to a new key; these initial daily keys were printed in a codebook that was distributed to the operators. For added security, the scrambler-disks part of the key was changed for every single message sent; this message-key information was transmitted twice at the beginning of every message. This technique was intended to prevent message loss due to transmission errors, but in fact reduced Enigma's effectiveness by introducing an element of predictability.

The defeat of Enigma. Enigma was long considered impossible to crack. However, in 1931, a disgruntled German ex-officer gave drawings for the machine to the French secret service. The French, who considered Enigma too tough to crack even with this information in their possession, gave it to the Polish government. Polish mathematician Marian Rejewski (1905–1980) used it to devise automatic devices (specialized electromechanical calculators) for re-cracking the ever-changing Enigma cipher on a daily basis. Just before the fall of Poland in 1939, Rejewski's findings were transferred to the British government, which continued to improve them.

During World War II, the German military modified the Enigma system at intervals, requiring the British to continue re-cracking the cipher throughout the war. With the help of a motley team of crossword-puzzle experts, bridge devotees, chess champions, mathematicians, and linguists led by British mathematician and computing pioneer Alan Turing (1912–1954), the group succeeded. Tragically, however, Turing was persecuted after the war for his homosexuality. His security clearance was revoked, he was forced to undergo debilitating hormone treatments, and he was banned from the development of the digital computer. Turing committed suicide in 1954, some 20 years before his crucial contribution to the cracking of Enigma, and thus, to the Allied victory, was declassified.

FURTHER READING:

BOOKS:

Churchouse, Robert. *Codes and Ciphers.* Cambridge, England: Cambridge University Press, 2002.

Singh, Simon. *The Code Book.* New York: Doubleday, 1999.

SEE ALSO

Cipher Machines
Codes and Ciphers

Entry-Exit Registration System, United States National Security

The U.S. National Security Entry-Exit Registration System (NEERS) is a program whereby persons whose nationality identifies them as a possible security risk are required to submit to control processes governed by the U.S. Department of Justice. Established in June, 2002, the system is a response to the September 11, 2001, terrorist attacks and the increased awareness of terrorism and homeland security that emerged in their wake. Despite these concerns, some critics have charged that NEERS is unconstitutional.

On June 5, 2002, the Justice Department introduced the new system that focused on citizens of Iran, Iraq, Libya, Sudan, and Syria. In addition, "certain nationals of other countries whom the State Department and the INS [Immigration and Naturalization Service] determine to be an elevated national security risk" would be placed under the program, which required these individuals to undergo fingerprinting, photographing, and registration. Exit controls built into the system would make it easier for law-enforcement officials to monitor foreign nationals as to the length of their visas, and to ensure the removal of those who had overstayed theirs.

In the first year, NEERS would track some 100,000 foreigners, but over time it would be expanded to include the more than 35 million who visit the United States every year. Though the program's original regulations made little reference to gender, it was clear that males from teen age to middle age were the focus. By early 2003, this had been spelled out in regulations that cited males 16 and over from some 25 countries.

Almost immediately, the program invoked the ire of groups representing civil liberties interests, foreigners, or other constituencies. In December, 2002, the *Financial Times* reported that some 700 men and boys in southern California had been detained for several days on suspicion of criminal activity. Such actions, the British paper warned, could deter foreign nationals from registering with the program.

This was one legitimate concern with the program that law-abiding foreigners would register, while those for whom NEERS was created would manage to avoid the system. Some workers fled to other countries, as the *Washington Post* showed in a report on Pakistanis making their way north to Canada—only to be met with an unfriendly reception there. As for the claim that the program unfairly singled out Middle Easterners or Muslims, defenders of NEERS pointed out at least three-quarters of the terrorist attacks worldwide over the past quarter-century—including the most violent attack in September, 2001, had been perpetrated by males from the Islamic world.

FURTHER READING:

PERIODICALS:

Brown, DeNeen L. "Pakistanis Find Cool Reception in Canada." *Washington Post.* (March 19, 2003): A24.

Lardner, George, Jr. "Congress Funds INS Registration System but Demands Details." *Washington Post.* (February 15, 2003): A18.

Parkes, Christopher. "Anti-Terror Programme in U.S. Runs into Controversy." *Financial Times.* (December 20, 2002): 8.

ELECTRONIC:

Attorney General Prepared Remarks on the National Security Entry-Exit Registration System. U.S. Department of Justice. <http://www.usdoj.gov/ag/speeches/2002/060502agpreparedremarks.htm> (March 24, 2003).

Fact Sheet: National Security Entry-Exit Registration System. U.S. Department of State International Information Programs. <http://usinfo.state.gov/topical/pol/terror/02060509.htm> (March 24, 2003).

National Security Entry-Exit Registration System (NEERS). <http://fpc.state.gov/16739.htm> (March 24, 2003).

SEE ALSO

INS (United States Immigration and Naturalization Service) Profiling
September 11 Terrorist Attacks on the United States

Environmental Issues Impact on Security

WILLIAM C. HANEBERG

The relationship between environmental issues and national security includes the possibility of conflict over scarce resources such as fresh water and arable land, the influence of global climate changes on the types and locations of future conflicts, and the degree to which the environmental consequences of domestic military and security activities should be open to public scrutiny. Although there is no standardized definition, aspects of national security that are driven by or that address environmental issues can be collectively described by the term environmental security. Because environmental security issues are tied as closely to public policy, politics, and economics as they are to science and engineering, discussions of either are often contentious and highly polarized.

Increasing concerns about environmental quality and degradation during the past several decades have led to the incorporation of environmental elements into national security policy. Some policy scenarios, for example, discuss the possibility of United States troops invading South American countries to enforce bans against logging in rainforests or to quell violence arising from competition

for arable land and fresh water in African regions undergoing desertification. It has also been suggested that potential global warming may shrink the northern polar ice cap and open parts of the Arctic Ocean as a military theatre for surface ships as well as an avenue of commerce.

With regard to their potential for political upheaval or war as a consequence of environmental problems, the least stable parts of the world have been identified as North Africa, the sub-Saharan Sahel region of Africa (including Ethiopia, Sudan, Somalia, Mali, Niger, and Chad), the island nations of the western Pacific Ocean, the Ganges River basin (principally northeastern India and Bangladesh), and some parts of Central and South America. Some portions of Africa, in particular, do not possess resources (especially food, water, and energy) adequate to support the current population under existing conditions. Other areas are those in which climate change or continuing population growth may cause the carrying capacity of the environment to be exceeded. In either case, regional deprivation and political unrest may have global consequences if they provide an atmosphere that allows extremist or terrorist groups to flourish. Environmental security concerns will likely require the shaping of events through diplomatic efforts to promote regional stability (including the equitable provision of foreign aid); limited military response in cases where diplomatic efforts to promote stability have failed; and continuing preparation of diplomatic, military, and civilian personnel to deal with environmental security issues.

The environmental impacts of military activities and the effects of domestic environmental laws on military readiness are also evolving concerns. Like other federal agencies, the Department of Defense has historically complied with the National Environmental Policy Act (NEPA) that requires, for example, the preparation of Environmental Impact Statements (EIS) or Environmental Assessments (EA) prior to many activities. Military facilities are also required to develop Integrated Natural Resources Management Plans (INRMPs) that must be revised every five years. In order to decrease the operational and budgetary impacts of environmental laws on military activities deemed essential to national security, the Strategic Environmental Research and Development Program (SERDP), a Department of Defense program, was established in 1990. Its focus areas include the development of more effective methods and technologies for the cleanup of contaminated military sites, compliance with environmental laws and regulations, conservation of natural resources, pollution prevention, and identification and destruction of unexploded ordnance. More recently, the Department of Defense has sought military exemptions from environmental laws that include the Endangered Species Act, the Clean Air Act, the Clean Water Act, and the Marine Mammal Protection Act. The House Armed Services Committee voted in 2002 to allow the Department of Defense to ignore some environmental laws, but compromise legislation passed several months later in the Senate limited this to a temporary exemption from the Migratory Bird Treaty Act. The legislation also directed the secretary of the interior to draft within one year regulations that would permanently exempt many military activities from environmental laws.

FURTHER READING:

BOOKS:

King, Chris. *Understanding International Environmental Security: A Strategic Military Perspective*. AEPI-IFP-1100A. Atlanta, GA: Army Environmental Policy Institute, 2000.

Petzold-Bradley, E., A. Carius, and A. Vincze (editors). *Responding to Environmental Conflicts: Implications for Theory and Practice*. Dordrecht, The Netherlands: Kluwer Academic Publishers, 2001 .

Price-Smith, A. T. *The Health of Nations: Infectious Diseases, Environmental Change, and Their Effects on National Security and Development.* Cambridge, MA: MIT Press, 2001 .

ELECTRONIC:

Benjamin, Paul. "Green Wars: Making Environmental Degradation a National Security Issue Puts Peace and Security at Risk." The Cato Institute, Policy Analysis No. 369. April 20, 2000. <http://www.cato.org/pubs/pas/pa-369es.html> (14 March 2003).

Pacific Institute. "Environment and Security." <http://www.pacinst.org/environment_and_security/>(14 March 2003).

Pike, John. "Environmental Issues." December 12, 2002. <http://www.globalsecurity.org/military/facility/environment.htm>(14 March 2003).

Strategic Environmental Research & Development Program. "Welcome to SERDP." March 10, 2003. <http://www.serdp.org/>(14 March 2003).

U.S. Army Corps of Engineers. "NEPA and Army Management." September 10, 2002. <http://aec.army.mil/usaec/nepa/compliance00.html>(14 March 2003).

SEE ALSO

EPA (Environmental Protection Agency)
Food supply, Counter-Terrorism
Natural Resources and National Security
Water Supply: Counter-Terrorism

Environmental Measurements Laboratory

K. LEE LERNER

The Environmental Measurements Laboratory (EML) is a research laboratory located in New York City, first established in 1947, that is operated by the United States

government. Research at the facility is coordinated by the Science and Technology (S&T) Directorate of the Department of Homeland Security. EML scientists are an integral part of the nation's radiological incident emergency response plans.

As a federal laboratory, EML supports the United States Department of Energy (DOE) National Security objectives. EML responsibilities include monitoring international compliance with nonproliferation treaties. EML is a part of the Homeland Security Monitoring Network (HSMN) and is also an official U.S. Radionuclide Laboratory with facilities dedicated to support of the International Monitoring System.

EML programs are designed to develop and train personnel in instruments and technologies capable of detecting radioactive substances and identifying nuclear threats. EML has advanced programs in radiation survey planning, radiological monitoring and assessment, and radiation measurements (including dosimetry measurements). EML also hosts high resolution gamma sensors and equipment dedicated to measuring environmental radiation and radioactivity.

Unique EML research capabilities include the ability to generate atmospheric conditions that allow experimental evaluation of instrumentation. EML scientific programs include collaborative research with global meteorological groups dedicated to developing more accurate atmospheric modeling programs. Since the Cold War, EML has maintained the International Environmental International Environmental Sample Archive (IESA), a collection of atmospheric and other environmental samples containing isotopes present in the atmosphere during periods when nations still engaged in atmospheric testing of nuclear weapons. These samples can be used to test current samples for signs of nuclear testing and are a part of nonproliferation monitoring. The samples can also allow quantitative and qualitative standardization of monitoring instrumentation.

As part of HSMN implementation, EML scientists constructed a prototype monitoring platform on top the GSA building in New York city that is capable of detecting radiological anomalies. Radiation levels can be measured by instruments utilizing a pressurized ionization chambers (PIC), comprehensive radiation sensors (CRS), and direct analysis of trapping filters via high-resolution gamma-ray analysis. The instruments are capable of distinguishing between natural radioactive sources and artificial or man-made sources.

EML programs include surface, air, and high altitude sampling programs, soil and sediment sampling programs, and fallout measurement programs.

EML scientists have developed particulate collection systems that utilize sodium iodide gamma detectors, and RAMPSCAN, a highly portable battery-operated gamma radiation detector.

Other EML facilities include pulse ionization chambers capable of measuring radon levels, a gamma ray analysis laboratory, and a thermoluminescent dosimeter reader facility.

FURTHER READING:

ELECTRONIC:

Environmental Measurements Laboratory. National Security. <http://www.eml.doe.gov/> (March 16, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <http://www.dhs.gov/dhspublic/display?theme=27&content=374> (March 23, 2003).

SEE ALSO

Argonne National Laboratory
Brookhaven National Laboratory
DOE (United States Department of Energy)
Lawrence Berkeley National Laboratory
Lawrence Livermore National Laboratory (LLNL)
Los Alamos National Laboratory
NNSA (United States National Nuclear Security Administration)
Oak Ridge National Laboratory (ORNL)
Pacific Northwest National Laboratory
Plum Island Animal Disease Center
Sandia National Laboratories

EPA (Environmental Protection Agency)

ROBERT G. BEST

The Environmental Protection Agency (EPA) was founded for the specific purpose of protecting human health and safeguarding the natural environment. Until the establishment of the EPA in 1970, there were no federal agencies or programs designed to deal with environmental pollution in the United States in a coordinated fashion. The EPA was assigned the unenviable task of reversing pollution that resulted from many years of unregulated environmental practices that preceded the establishment of the EPA.

Even before its inception as an agency within the federal government, it was recognized that no single entity could govern all practices and activities that had significant potential impact on the environment. Thus, the EPA was designed as an interactive agency providing direction, oversight, and assistance to many other agencies and groups whose activities bear directly and indirectly on the quality of the air, water, and land.

The EPA provides advice to the president of the United States on matters of environmental policy, and is charged with the responsibility of establishing and enforcing laws

and regulations to control the quality of the environment. The chief officer of the EPA is the administrator who is appointed by the president. EPA employs 18,000 people and operates 17 laboratories across the United States. The country is divided into ten regions, each with its own regional EPA office. The total annual budget for the EPA is nearly $8 billion.

The EPA plays a leadership role in various aspects of environmental science including research, education and environmental evaluation and assessment. EPA works closely with other federal, state and local agencies as well as Native American tribal governments to develop environmental programs and regulations and to enforce existing laws pertaining to air, water, and land quality and purity. There are also a number of voluntary programs administered by the EPA that go beyond laws and regulations to encourage individuals and organizations to prevent pollution and conserve energy.

Research in environmental science is conducted directly by laboratories within the EPA. In addition, EPA serves as a funding source and planning resource for state governments and researchers outside of the agency. Over $1 billion from the overall EPA budget goes to categorical grants to state and local governments. Grants are also made for the purposes of enforcement, response preparedness, information exchange networks, assistance with Native American environmental issues, and counter-terrorism.

Cleanup of existing toxic waste facilities remains one of the largest and most difficult tasks for the EPA. The nation's biggest and most technically complex properties affected by toxic waste are prioritized on the National Priorities List to reverse, minimize, or prevent environmental disasters related to toxic waste. These include private and federal properties many of which have been abandoned by their owners. The Superfund was created to fund these complicated and expensive cleanup activities. EPA provides outreach and educational activities for communities surrounding the toxic waste sites to raise awareness of risks, prevention and avoidance strategies, and to promote direct involvement in cleanup activities.

EPA and the Federal Counter-Terrorism program. The EPA supports the federal counter-terrorism program by helping state and local agencies plan for emergencies, training first responders, providing necessary resources in the event of terrorist actions, and coordinating with key federal agencies. Three offices within the EPA participate in the counter-terrorist Program: the Chemical Emergency Preparedness and Prevention Office (CEPPO), the Office of Emergency and Remedial Response (OERR), and the Office of Air and Radiation (OAR).

Following the World Trade Center terrorist attacks in September, 2001, the EPA assumed responsibility for monitoring air and water purity at ground zero, provided decontamination operations for on-site workers, monitored key pollutants at the Staten Island landfill site, and participated in clean up of sidewalks, streets, and buildings in the surrounding area.

FURTHER READING:

BOOKS:

Binns, Tristan Boyer. *The Environmental Protection Agency.* Woburn, MA: Heineman Publishers, 2002.

ELECTRONIC:

United States Environmental Protection Agency. "EPA's Role and Authority in Counter Terrorism" Chemical Emergency Preparedness and Prevention <http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/ct-epro.htm#epa> (February 15, 2003).

———. "Protecting Human Health, Safeguarding the Natural Environment" Home Page<http://www.epa.gov/> (February 15, 2003).

SEE ALSO

Air and Water Purification, Security Issues
Chemical Warfare
Emergency Response Teams
Environmental Issues Impact on Security
FEMA (United States Federal Emergency Management Agency)
Radiological Emergency Response Plan, United States Federal
September 11 Terrorist Attacks on the United States
Toxicology
Toxins
Water Supply: Counter-Terrorism

Epidemiology

ANTONIO FARINA/BRIAN D. HOYLE

Epidemiology is the study of the various factors that influence the occurrence, distribution, prevention, and control of disease, injury, and other health-related events in a defined human population. By the application of various analytical techniques including mathematical analysis of the data, the probable cause of an infectious outbreak can be pinpointed. This connection between epidemiology and infection makes microorganisms an important facet of epidemiology, and gives epidemiologists a vital link in emergency planning for public health response to a biological attack.

Molecular epidemiology has been used to trace the cause of bacterial, viral, and parasitic diseases. This knowledge is valuable in developing a strategy to prevent further outbreaks of the microbial illness, since the probable source of a disease can be identified.

Furthermore, in the era of biological weapons use by individuals, organizations, and governments, epidemiological studies of the effect of exposure to infectious microbes has become more urgently important. Knowledge of the effect of a bioweapon on the battlefield may not extend to the civilian population that might also be secondarily affected by the weapons. Thus, epidemiology is an important tool in identifying and tracing the course of an infection.

Molecular and genetic basis of epidemiology. Genetic epidemiology studies could result in data that would enable forensic investigators to rapidly identify bioterrorism or biological warfare agents specifically engineered or vectored to affect certain subgroups within a larger population.

Molecular epidemiology arises from varied scientific disciplines, including genetics, epidemiology and statistics. The strategies involved in genetic epidemiology encompass population studies and family studies. Sophisticated mathematical tools are now involved, and computer technology is playing a predominant role in the development of the discipline. Multidisciplinary collaboration is crucial to understanding the role of genetic and environmental factors in disease processes.

Much information can come from molecular epidemiology even if the exact genetic cause of the malady is not known. For example, the identification of a malady in generations of related people can trace the genetic characteristic, and even help identify the original source of the trait. This approach is commonly referred to as genetic screening. The knowledge of why a particular malady appears in certain people, or why such people are more prone to a microbial infection than other members of the population, can reveal much about the nature of the disease in the absence of the actual gene whose defect causes the disease.

Differences in response to pathogens is often a complex interplay of various environmental and genetic factors that require sophisticated analytical tools and techniques to identify. Aided by advances in computer technology, scientists develop complex mathematical formulas for the analysis of epidemiological models, the description of the transmission of the disease, and genetic-environmental interactions. Sophisticated mathematical techniques are now used for assessing classification, diagnosis, prognosis and treatment of many diseases.

Population studies provide data that greatly impact public health programs and emergency responses. By means of several statistical tools, genetic epidemiologic studies evaluate risk factors, inheritance and possible models of inheritance. Different kinds of studies are based upon the number of people who participate and the method of sample collection (i.e., at the time of an outbreak or after an outbreak has occurred). A challenge for the investigator is to achieve a result able to be applied with as low a bias as possible to the general population. In other words, the goal of an epidemiological study of an infectious outbreak is to make the results from a few individuals applicable to the whole population.

A fundamental underpinning of infectious epidemiology is the confirmation that a disease outbreak has occurred. Once this is done, the disease is followed with time. The pattern of appearance of cases of the disease can be tracked by developing what is known as an epidemic curve. This information is vital in distinguishing a natural outbreak from a deliberate and hostile act, for example. In a natural outbreak the number of cases increases over time to a peak, after which the cases subside as immunity develops in the population. A deliberate release of organisms will be evident as a sudden appearance of a large number of cases at the same time.

Tracking diseases with technology. Many illnesses of epidemiological concern are caused by microorganisms. Examples include hemorrhagic fevers such as that caused by the Ebola virus. The determination of the nature of illness outbreaks due to these and other microorganisms involve microbiological and immunological techniques.

Various routes can spread infections (i.e., contact, air borne, insect borne, food and water intake, etc.). Likewise, the route of entry of an infectious microbe can also vary from microbe to microbe.

If an outbreak is recognized early enough, samples of the suspected cause as well as samples from the afflicted (i.e., sputum, feces) can be gathered for analysis. The analysis will depend on the symptoms. For example, in the case of a food poisoning, symptoms such as the rapid development of cramping, nausea with vomiting, and diarrhea after eating a hamburger would be grounds to consider *Escherichia coli* O157:H7 as the culprit. Analyses would likely include the examination for other known microbes associated with food poisoning (i.e., *Salmonella*) in order to save time in identifying the organism.

Analysis can involve the use of conventional laboratory techniques (e.g., use of nonselective and selective growth media to detect bacteria). As well, more recent technological innovations can be employed. An example is the use of antibodies to a known microorganism that are complexed with a fluorescent particle. The binding of the antibody to the microbes can be detected by the examination of a sample using fluorescence microscopy or flow cytometry. Molecular techniques such as the polymerase chain reaction are employed to detect genetic material from a target organism. However, the expense of the techniques such as PCR tends to limit its use to more of a confirmatory role, rather than as an initial tool of an investigation. A considerable research effort is ongoing at U.S. National Laboratories to develop quicker, less expensive, and more portable PCR equipment that can be used by inspectors and investigators.

Another epidemiological tool is the determination of the antibiotic susceptibility and resistance of bacteria.

Such laboratory techniques can be combined with other techniques to provide information related to the spread of an outbreak. For example, microbiological data can be combined with geographic information systems (GIS). GIS information has helped pinpoint the source of outbreaks. In addition to geographic based information, epidemiologists will use information including the weather on the days preceding an outbreak, mass transit travel schedules and schedules of mass-participation events that occurred around the time of an outbreak to try and establish a pattern of movement or behavior to those who have been affected by the outbreak. Use of credit cards and bank debit cards can also help piece together the movements of those who subsequently became infected.

Reconstructing the movements of people is especially important when the outbreak is an infectious disease. The occurrence of the disease over time can yield information as to the source of an outbreak. For example, the appearance of a few cases at first with the number of cases increasing over time to a peak is indicative of a natural outbreak. The number of cases usually begins to subside as the population develops immunity to the infection (e.g., influenza). However, if a large number of cases occur in the same area at the same time, the source of the infection might not be natural. Examples include a food poisoning or a bioterrorist action.

Epidemiologists were among the first scientists to effectively utilize the Internet and email capabilities to effectively communicate regarding disease outbreaks. The International Society for Infectious Diseases sponsors PROMED, the global email based electronic reporting system for outbreaks of emerging infectious diseases and toxins, is open to all sources.

■ FURTHER READING:

BOOKS:

Trestrail, John H. *Forensic Epidemiology.* Loue, Sana, 1999.

PERIODICALS:

Epidemiology Program Office, CDC. "CDC's 50th Anniversary: History of CDC." *Morbidity and Mortality Weekly Report* no. 45 (1996): 525–30.

ELECTRONIC:

Centers for Disease Control and Prevention. "About CDC." November 2, 2002. <http://www.cdc.gov/aboutcdc.htm> (28 December 2002).

International Society for Infectious Diseases. ProMED-mail. May, 2003. <http://www.promedmail.org/pls/askus/f?p=2400:1000'>(May 12, 2003).

SEE ALSO

Biological Weapons, Genetic Identification
Bioshield Project
Bioterrorism, Protective Measures
CDC (United States Centers for Disease Control and Prevention)
Communicable Diseases, Isolation, and Quarantine
Public Health Service (PHS), United States
World Health Organization (WHO)

Espionage

Espionage is the use of spies, or the practice of spying, for the purpose of obtaining information about the plans, activities, capabilities, or resources of a competitor or enemy. It is closely related to intelligence, but is often distinguished from it by virtue of the clandestine, aggressive, and dangerous nature of the espionage trade.

The term *espionage* comes from a French word meaning *to spy.* The Middle French *espionner* appears to be related to the Old Italian *spione,* which in turn is linguistically akin to the Old High German *spehon.* This is interesting philologically, since French, Italian, and German have very different historic roots: the first two derived from the Latin of the Roman Empire, while the third comes from the language of the Romans' "barbarian" foes across the Rhine. It is perhaps fitting that the very etymology of *espionage* would reflect surreptitious connections.

A brief history. Though the word itself entered the English language from the French in 1793, at a time when the foundations of modern espionage were being laid, the concept of espionage is as old as civilization. Ancient and classical era scripts often mention spies and the use of espionage (e.g., the Bible mentions spies some 100 times) while the Greek legend of the Trojan horse suggests that covert operations and "dirty tricks" are nothing new. The roots of espionage in the East are likewise very deep: in the third century B.C., both the Mauryan empire of India and the China's Ch'in dynasty ensured control over their vast realms with the help of spy networks.

Despite this early evidence of organized spying in east Asia, espionage tended to be an ad hoc enterprise until the late eighteenth century. The reign of terror that followed the French Revolution—significantly, in 1793—marked the beginnings of the modern totalitarian police state, while the American Revolution a few years earlier saw the beginnings of a consistent interface between military operations and intelligence. Military intelligence came into its own during the American Civil War, while the late nineteenth century saw the birth of the first U.S. military intelligence organizations.

The twentieth century and beyond. Espionage reached a new level of maturity in World War I. Although Mata Hari may

United States attorney general for the southern district of Florida Thomas Scott shows a diagram illustrating a Cuban espionage network operating illegally in the U.S. as foreign agents of the Cuban government in 1998. AP/WIDE WORLD PHOTOS.

have been the most visible, and romantic, spy of the war, there were many others on both sides. The war also gave birth to the first true totalitarian state, in Russia, and this was followed soon afterward by the establishment of fascism in Italy. Totalitarianism spawned its own elaborate spy networks, and increased the requirements for espionage activities on the part of democracies, as evidenced by the U.S. experience with Nazi and later Soviet infiltrators on American shores.

The era that perhaps most commonly comes to mind at the mention of the word *espionage* is the Cold War, which lasted from the end of World War II to the fall of the Berlin Wall and the Soviet empire. Yet the end of Soviet communism was certainly not the end of espionage, a fact that became dramatically apparent as new U.S. enemies emerged among Islamist terrorists and their supporters.

In any case, espionage is not solely the enterprise of governments: companies have long sought to gain the advantage over competitors through the use of economic or industrial espionage. In a world increasingly dominated by huge corporations, economic espionage is not likely to disappear. Nor is espionage only undertaken against enemies: the United States has captured, and punished, spies who passed U.S. secrets to such allies as Israel and South Korea.

FURTHER READING:

BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

Dulles, Allen Welsh. *The Craft of Intelligence.* New York: Harper & Row, 1963.

Haynes, John Earl. *Venona: Decoding Soviet Espionage in America.* New Haven, CT: Yale University Press, 1999.

Martin, David C. *Wilderness of Mirrors.* New York: Harper & Row, 1980.

Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer.* New York: Viking, 1987.

SEE ALSO

Civil War, Espionage and Intelligence
Economic Espionage
Espionage and Intelligence, Early Historical Foundations
Intelligence
Napoleonic Wars, Espionage During

Espionage Act of 1917

ADRIENNE WILMOTH LERNER

The Espionage Act, passed in 1917 after the United States entered the World War I, prohibited the disclosure of government and industrial information regarding national defense. The act also criminalized refusal to perform military service if conscripted.

In 1914, war began in Europe. The United States declared neutrality at the beginning of the war, attempting to avoid war in Europe and unrest within its own borders. Forging alliances was difficult not only because the United States' relatively small military at the time, but also because of its large immigrant population. In the three decades preceding World War I, several million people immigrated to America, many from various nations involved in the European conflict. Making alliances with Britain and France promised to upset scores of German and Austrian sympathizers, and vice versa. Though some elements of the population were divided on the opinion of European alliances, the government favored allegiance with Britain and France. While America maintained its neutrality until 1917, it became a major supplier of money, supplies, and munitions to British and French forces. American ships transported contraband weapons across the Atlantic and between European ports. Intelligence agents and merchant ships gathered reports on German vessels and informed the British Navy of fleet activity.

In retaliation for what was viewed as acts of war and signs of allegiance with their enemies, the German government sent saboteurs to destroy American factories, warehouses, and ships that produced or held munitions bound for the western front. Several high-profile terrorist acts, most especially the demolition of Black Tom Pier near Ellis Island, New York, helped to foster a genuine concern, and to some degree an hysteria, about the danger of spies and saboteurs. When America formally joined the Allies' fight against Germany and Austria-Hungary in 1917, the government enacted tough legislation intended to aid the war effort.

The Espionage Act was one of the first pieces of wartime legislation passed. It had overwhelming favor in the government, but was more controversial to the public, especially among political radicals opposed to war, conscription, and interference with civil liberties. The act had provisions for steep penalties, including a $10,000 fine and 20 years imprisonment. While the act was rarely questioned as a means of controlling enemy espionage, its broad application to silence anti-war protesters and left-wing sympathizers drew criticism. Socialist advocate Eugene V. Debs was sentenced to ten years in prison for claiming in a speech that the Espionage Act itself was unconstitutional. Over 450 conscientious objectors were jailed under the provisions of the act for refusing military service.

Congress amended the Espionage Act in 1918 with the passage of the Sedition Act. The act further extended prohibition on the expression of anti-war and unpatriotic sentiments. It imposed several penalties on those convicted of "disloyal, profane, scurrilous, or abusive language" against the government, its actions, or its symbols.

While the Espionage Act was intended as wartime legislation, it continued to be invoked following the end of the war. When the Bolshevik Revolution toppled the Russian monarchy in 1917, it sparked a widespread fear of communist revolts in other nations. The period, which lasted from 1919 to 1920, became known in America as the Red Scare. During the Red Scare, the attorney general, A. Mitchell Palmer, and his assistant, John Edgar Hoover, set up a special task force to prosecute radicals under the Espionage and Sedition Acts. Nearly 2,000 people were tried and imprisoned, but Palmer's increasing zeal for his cause began to draw criticism in 1920. Palmer claimed that communist agents had infiltrated American organizations and were planning to overthrow the government on May 1, 1920. When his predicted revolution failed to materialize, many turned away from his cause. Palmer and Hoover ordered the deportation of some people convicted during the Red Scare; however, most were simply jailed in the United States. Most of the prisoners sentenced during the Red Scare were freed in 1920.

FURTHER READING:

BOOKS:

Kennedy, David M. *Over Here: The First World War and American Society.* New York: Oxford University Press, 1986.

SEE ALSO

World War I

Espionage and Intelligence, Early Historical Foundations

ADRIENNE WILMOTH LERNER

Espionage is one of the oldest, and most well documented, political and military arts. The rise of the great

Belle Boyd was a spy for the Confederacy during the American Civil War. ©BETTMANN/CORBIS.

ancient civilizations, beginning 6,000 years ago in Mesopotamia, begat institutions and persons devoted to the security and preservation of their ruling regimes. Clandestine and covert operations garner the most intrigue, but the history of espionage is better described in terms of the evolution of its more mundane components of tradecraft. Throughout history, intelligence has been defined as the collection, culling, analysis, and dissemination of critical and strategic information. Its practice and implications, however, are widely diverse.

Espionage in the Ancient World

Historical and literary accounts of spies and acts of espionage appear in some of world's earliest recorded histories. Egyptian hieroglyphs reveal the presence of court spies, as do papyri describing ancient Egypt's extensive military and slave trade operations. Early Egyptian pharos employed agents of espionage to ferret-out disloyal subject and to locate tribes that could be conquered and enslaved. From 1,000 B.C. onwards, Egyptian espionage operations focused on foreign intelligence about the political and military strength of rivals Greece and Rome.

Egyptian spies made significant contributions to espionage tradecraft. As the ancient civilizations of Egypt, Greece, and Rome employed literate subjects in their civil services, many spies dealt with written communications. The use of written messages necessitated the development of codes, disguised writing, trick inks, and hidden compartments in clothing to his communications. Egyptian spies were the first to develop the extensive use of poisons, including toxins derived from plants and snakes, to carry-out assassinations or acts of sabotage.

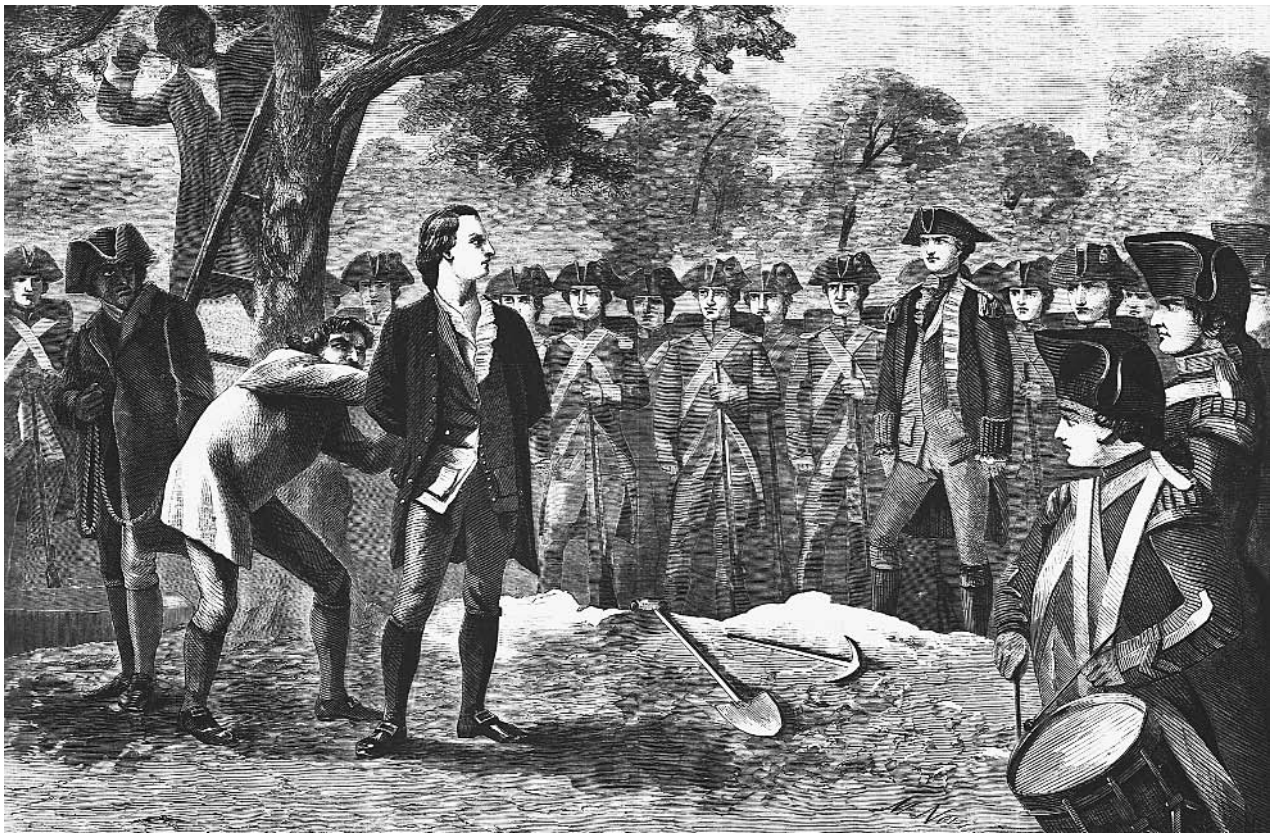
The rise of the Greek civilization brought forth new concepts of government and law enforcement. Between 1500 B.C. and 1200 B.C., Greece's many wars with its regional rivals led to the development of new military and intelligence strategies. The early Greeks relied on deception as a primary means of achieving surprise attacks on their enemies. So renowned were Greek employments of deceptive strategies, that Greek literature from antiquity celebrated its intelligence and espionage exploits. The legendary incident of the Trojan Horse, a wooden structure given to the city of Troy as gift, but which contained several hundred Greek soldiers seeking safe entrance into the heavily fortified rival city, became the symbol of Grecian intelligence prowess.

In the era of democratic Greek city-states, espionage was chiefly employed as a political tool. Agents of espionage spied on rival city-states, providing rulers with information on military strength and defenses. The most farsighted contribution of the ancient Greek intelligence community, however, was its creation of a complex and efficient means of communication between cities. Couriers delivered messages between cities, but important messages were also relayed between a series of outposts or towers using semaphore, a form of communication that utilized signals to convey messages. Greek communications were so efficient that they remained unparalleled until the modern era.

In the Middle East, and later Byzantium, the large government bureaucracy established one of the earliest civilian intelligence agencies. Civilian agents of espionage culled information abut foreign militaries and economic practices from traders, merchants, sailors, and other businessmen. Outside of the Mediterranean region, other civilizations utilized and contributed to the art of espionage. Written records from the fifth century mention the use of spies in the Indus Valley 2,500 years ago. In China, Sun Tzu penned the comprehensive military treatise, *The Art of War*, which contained several chapters devoted to the use of spies both on and off the battlefield.

No civilization in the ancient world relied more heavily on intelligence information, nor furthered the development of espionage more than ancient Rome. Over a millennium, the Romans created the largest empire of the ancient world, necessitating the governance of the most expansive infrastructure, military, and bureaucracy or the period.

Rome's most famous case of espionage and intrigue culminated in the assassination of Julius Caesar on March 15, 44 B.C. The exact details of the assassination conspiracy remain a mystery to historians, but records have established that the Roman intelligence community knew



British soldiers tie the hands of Nathan Hale (1755–1776), just before his execution for spying. ©CORBIS.

of the plot and even provided information to Caesar or his assistants providing the names of several conspirators. The information from the intelligence community was ignored.

The ever-expanding Roman Empire often spied on its neighbors. Not only did intelligence forces provide comprehensive reports on the military strength and resources of those outside the empire, but the Roman military also employed intelligence forces to infiltrate tribal organizations and convince leaders to join in alliance with Rome. If populations were judged hostile by informants, the military was informed, and engaged the opposing forces. This type of intelligence campaign was very successful in the Italian Peninsula during the fourth century B.C., but far less effective in the later campaigns to conquer North Africa and Northern Europe.

The Roman Empire possessed a fondness for the practice of political espionage. Spies engaged in both foreign and domestic political operations, gauging the political climate of the Empire and surrounding lands by eavesdropping in the Forum or in public market spaces. Several ancient accounts, especially those of the A.D. first century, mention the presence of a secret police force, the *frumentarii*. By the third century, Roman authors noted the pervasiveness and excessive censorship of the secret police forces, likening them to an authoritative force or an occupational army. Political espionage was not limited to the more contentious parts of the Roman periphery, but was also practiced in Rome itself by rival factions of the government. Some ministries even employed saboteurs. Concern about government rivalries necessitated the creation of the *agentes in rebus*, the first exclusive counterintelligence force.

The Middle Ages

After the collapse of the Roman Empire in Europe, espionage and intelligence activities were confined to wartime or local service. Warring factions under barbarian lords may have used strategic espionage to gauge the strength of their opposition or learn about enemy defenses, but no written records of such activities survive. The only considerable political force in Europe during the Dark Ages was the Catholic Church, but operations on the European periphery were confined to monastic outposts that struggled for survival.

In the Middle Ages, the birth of large nation-states, such as France and England, in the ninth and tenth centuries facilitated the need for intelligence in a diplomatic setting. Systems of couriers, translators, and royal messengers carried diplomatic messages between monarchs or feudal lords. Literacy was a rarity, even in the early royal

courts, so messages were carefully delivered verbatim by couriers, or clergy acted as scribes.

Espionage remained mostly limited to battlefield operations, but the development of the feudal system, in which lords swore fealty to monarchs, created a complicated allegiance network. The web of allegiances gave rise to laws prohibiting treason, double allegiances, and political espionage against allied lords.

In the eleventh century, the Catholic Church rose to the fore in European politics. With a large bureaucratic network, the resources of feudal military forces, and the largest treasury in the world, the Church formed policy that governed all of Europe. Throughout the course of the Middle Ages, two events, the Crusades and the Inquisition, solidified the power of the Church and created the only long-standing, medieval intelligence community.

In 1095, Pope Urban II called for the first Crusade, a military campaign to recapture Jerusalem and the Holy Lands from Muslim and Byzantine rule. The Church massed several large armies, and employed spies to report on defenses surrounding Constantinople and Jerusalem. Special intelligence agents also infiltrated prisons to free captured crusaders, or sabotage rival palaces, mosques, and military defenses. The Crusades continued for nearly four centuries, draining the military and intelligence resources of most of the European monarchs.

The Crusades also changed the tenor of espionage and intelligence work within Europe itself. Religious fervor, and the desire for political consolidation, prompted thirteenth century church councils to establish laws regarding the prosecution of heretics and anti-clerical political leaders. The ensuing movement became known as the Inquisition. Although the Church used its political force as impetus for the Inquisition, enforcement of religious edicts and prosecution of violators fell to local clergy and secular authorities. For this reason, the Inquisition took many forms throughout Europe. The same movement that was terror-filled and brutal in Spain, had little impact in England and Scandinavia.

Espionage was an essential component of the Inquisition. The Church relied on vast networks of informants to find and denounce suspected heretics and political dissidents. By the early fourteenth century, Rome and the Spanish monarchs both employed sizable secret police forces to carry out mass trials and public executions. In southern France, heretical groups relied on intelligence gathered from their own resistance networks to gauge the surrounding political climate, and assist in hiding refugees.

In 1542, the process of Inquisition was centralized within the Church. Pope Paul III established the Congregation of the Holy Office, a permanent council, composed of cardinals and other officials, whose mission was to maintain the political integrity of Church. The council relied on censure and excommunication to coerce problematic individuals, forsaking the brutal cloak and dagger methods of early Inquisitors. The council maintained spies and informants, but shifted their focus to scrutinizing the actions of Europe's monarchs and prominent aristocrats. The advent of the Renaissance in Italy in the mid-fifteenth century quelled much of the fervor and political fear that drove the Inquisition, and the movement faded.

The Renaissance

The Renaissance marked the eclipse of the Church dominated world. Europe transitioned to more localized, nationalistic models of government, with each nation or city-state employing its own intelligence force. As nations and city-states became wealthier and gained more power, espionage enjoyed a resurgence. Competition for dominance over trade and exploration of the New World changed the political climate of Europe, and forced regimes to adopt increasingly deft measures of protecting political, military, and economic interests.

In response to the changing world, Niccolo Machiavelli, a Florentine political philosopher, published a series of books detailing the qualities and actions of effective rulers. In his works, *The Prince*, and *The Art of War*, Machiavelli advocated that rulers routinely employ espionage tradecraft, engaging in deception and spying to insure protection of their power and interests. His advice, much of which was culled from rediscovered works of Aristotle and Cicero, was intended for the ruling Medici princes of Florence. However, the works gained popularity several centuries after their 1520 publication.

In the late 1500s, the English royal court developed the premier Renaissance era spy network. Religious reforms and a schism with the Catholic Church under the rule of Henry VIII, prompted the creation of a large secret police force, commanded by the military, to locate and infiltrate Catholic loyalist cells that threatened the English monarchy. When his daughter, Elizabeth I, ascended to the throne, political tensions threatened her reign. Elizabeth chose to rebuild the flagging military to rebuff opposition from disloyal lords and their forces, but especially lobbied for the expansion of the Navy and intelligence services. The new navy dispatched foreign threats, defeating the Spanish Armada in 1558, while the intelligence services dispatched several conspiracy plots that threatened to topple Elizabeth I's reign.

The Elizabethan court gained a reputation for the ruthlessness of its spies, several of whom double and triple crossed those with whom they dealt. The Elizabethan espionage system was highly effective, but its novel contribution to the development of espionage lay in its employment practices. Instead of relying on haphazard, ill-trained volunteers, or military men, the Elizabethan intelligence community employed linguists, scholars, authors, engineers, and scientists, relying on professional experts to seek and analyze intelligence information.

Technological development in the Renaissance altered the practice of espionage. The development of small

firearms, such the pistol, aided cloak and dagger operations. Chemists invested invisible inks, and the rebirth of complex mathematics revived encryption and code methods long dormant since Antiquity. Telescopes, magnifying glasses, the camera obscura, and clocks facilitated the remote surveillance and the effective use of "dead drops" to pass information between agents. Travel became easier, but that ease soon prompted territorial growth and the rebirth of vast empires.

The Birth of Modern Espionage: The Age of Empires, Industrial Revolution, and the Nineteenth Century

Espionage in the Age of Empires, a period that spanned from 1700 to almost 1900, saw its greatest development in the numerous conflicts and wars that occurred in Europe, and between rival colonial powers in Europe and abroad. Industrialization, economic and territorial expansion, the diversification of political philosophies and regimes, and immigration all transformed the world's intelligence communities.

During the French Revolution, in the 1790s, all factions relied heavily on espionage. However, the period marked by the dictatorship of Robespierre is most infamous. Informant networks denounced traitors to the new republic, and tracked down refugee aristocrats and clergy for trial and execution. The wide application of treason laws and charges marked one of the greatest abuses of intelligence powers in the modern era.

The American Revolution (1776–1783), and colonial wars for independence in South America in the 1820s and 1830s, marked the end of Europe's New World empires. European nations turned their attention to Africa and the Orient. The ensuing land grab inflamed tensions among European nations, changing the balance of European power and creating a complicated alliance system. Colonial rulers employed secret police and agents of espionage throughout their territorial holdings, hoping to quell anticolonial rebellions and separatist movements.

Imperialism not only changed the world political balance, but transformed economics. Modern industrial espionage was born in the pan-European revolutions of 1848. The series of regional conflicts pitted workers against landed gentry, liberals against conservatives, and monarchists against republicans, communists, and other political groups. Many governments, especially those of England, France, and Prussia, employed spies to infiltrate political and labor organizations and report on any antigovernment activities. Labor organizations often spied on each other, reporting on working conditions, factory operations, mining productivity, and other concerns. Many radical workers' organizations carried out acts of sabotage, destroying factories, mines, and government property. After armed conflict abated, many governments continued to conduct surveillance on dissident and workers' groups, within a decade, the same principals of industrial espionage were increasingly employed against foreign economic interests.

Industrialization revolutionized tradecraft with the proliferations of gadgets for the concealment, transcription, and analysis of intelligence information. The invention of dynamite aided saboteurs. Advances in chemistry and chemical production transformed everything from dyes and inks, to poisons and acids. Chemical weapons and poison gasses were developed during this time, but were considered too inhumane for strategic use until World War I. The discipline of forensic science added scientific methodology to the investigation of crimes and the analysis of intelligence information.

The collection of intelligence information forever changed in 1837, with the invention of the daguerreotype, the first practical form of photography. Though not able to be widely incorporated into intelligence practices until the 1860s, the photograph permitted agents of espionage to portray targets, documents, and other interests as they actually were. As soon as photo development became more practical with the advent of film, in lieu of glass plates, cameras were made smaller, disguised, or placed in mundane items for use in espionage. Until the advent of electronic data storage in the twentieth century, the photograph was the best means of copying and transmitting information.

Improvements in transportation and communications also transformed espionage operations. On May 24, 1844, Samuel Morse, sent the first message via telegraph. His code (Morse code) and the telegraph were able to send messages over lines in a matter of minutes, requiring only knowledge of the operational code. As soon as governments began to use telegraphs to send vital communications, rival intelligence services learned to tap the line, gaining access to secret communications and conducting detailed surveillance from a comfortable distance. Use of the telegraph necessitated the development of complex codes, and the creation of specialized cryptology departments. By the turn of the twentieth century, most national intelligence operations in Europe and the United States involved communications surveillance and the tapping of both wired, and wireless, telegraphs.

Just as the discovery of the New World, and the development of fast ships in the seventeenth century altered the scope of espionage, so to did the invention of the locomotive and the proliferation of railroads. Railroads also became primary targets of enemy sabotage, and one of the main protective objectives of counterintelligence personnel. Ease of travel facilitated communications and surveillance, permitting agents to travel to foreign destinations under the guise of tourists without arousing suspicion. Movement, travel, and immigration during the nineteenth century provided many nations,

especially the United States, with a field of language and culture experts.

By the dawn of the twentieth century, espionage had evolved into a highly specialized, technical field. Far from the battlefield and political intrigue of the ancient world, modern espionage involves more research and analysis than field operations. Specialized military units are still used for strategic intelligence, but most nations have developed large, centralized, civilian intelligence communities that conduct operations in wartime and peacetime with increasing technological sophistication.

FURTHER READING:

BOOKS:

Boardman, John, Jasper Griffen, and Oswyn Murray. *Oxford History of the Classical World.* New York: Oxford University Press, 1986.

Holmes, George. *Oxford History of Medieval Europe.* New York: Oxford University Press, 1988.

SEE ALSO

Cryptology, History
Napoleonic Wars, Espionage During
Revolutionary War, Espionage and Intelligence
War of 1812

Estonia, Intelligence and Security

Estonia maintains one central intelligence and security agency, the *Kaitsepolitseiamet* (KPol), Security Police Board. The KPol administers intelligence gathering and information analysis, and reports its findings to the executive branch of the government. KPol governs several operational divisions, including Counterintelligence, the Security Police, the Anti-terrorism Bureau, Constitutional Protection Bureau, and Anti-Corruption Bureau. The KPol's main objective is the protection of national interests and national sovereignty. The agency seeks both domestic and foreign intelligence.

Estonia emerged as a modern, independent nation in 1920. During World War II, however, the nation was invaded by both Soviet and German forces. After the war, Estonia fell in the Soviet sphere of influence. Estonia lost its sovereignty, becoming part of the Soviet Union for four decades. In 1988, the Estonian parliament decreed the nation autonomous, but Soviet forces kept the nation from seceding for over a year. After the fall of the Berlin Wall and the Iron Curtain in 1989, Estonia began the process of regaining its status as an independent nation. The collapse of the Soviet Union in 1991 allowed Estonia to finally reemerge as a democratic, independent nation.

The move to democracy in Estonia required extensive social, economic, and government reform. The new Estonian government sought to dissolve any remaining Soviet institutions, most especially those that were used as state-sponsored instruments of suppression, intended to quell nationalism. Estonia did not maintain its own intelligence community under Soviet rule, but had to distance its new, national intelligence agencies from the legacy of the KGB and Soviet secret police.

Corruption is a primary concern for the Estonia government. A legacy of Soviet occupation, government corruption was prevalent in the early 1990s. However, anti-crime and corruption task forces, as well as intelligence surveillance of government officials, has greatly reduced the problem. Business corruption, as well as incursions into the national economy by the Russian mafia, are also targeted by KPol intelligence operations.

Today, Estonia is actively pursuing membership in several international organizations. Reforms have aided a rapid transformation of the Estonian economy. Diplomatically, Estonia gravitates toward Europe, but maintains ties with neighboring Russia.

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
European Union

European Union

ADRIENNE WILMOTH LERNER

The European Union (EU) is a long-standing political and economic federation of autonomous European nations. With the consent of member states, the EU legislates a variety of issues by treaty, including trade, customs, travel, currency, and defense. Members choose to participate in various EU institutions, delegating sovereignty in order to achieve common goals.

The organization embraces democracy and the rule of law, requiring member states to possess some form of representative government, elected by universal adult suffrage of the adult citizenry. The mission of the EU is to promote economic growth in Europe, create a strong international market, lobby for European interests in the international community, raise standards of living, and promote peace.

History. European integration, the process that eventually yielded the EU, began on May 9, 1950, when France

proposed to create a European trade organization. Two years later, France and Germany established the European Coal and Steel Community. Both nations sought to solve disputes over coal mining territories and industry competition unresolved since the end of the Second World War. Belgium later joined France and Germany, uniting most of Western Europe's continental coal and steel industry.

Continued success of the European Coal and Steel Community prompted its president to lobby European governments for the establishment of a large-scale economic and trade union. In 1957, six nations (France, Germany, Belgium, the Netherlands, Luxembourg, and Italy) signed the Treaty of Rome, establishing the European Economic Community (EEC). The EEC standardized some tariffs, opened borders to free trade, promoted industry cooperation, regulated industry standards, and synchronized export practices.

In 1967, the member nations brought the European Coal and Steel Community and the European Atomic Energy Community (Euratom) into the fold of the EEC. The new unified organization was officially named the European Community (EC), though many continued to use to older designation, EEC, to refer to the new union.

Several nations in Europe chose not to join the original EEC, the most prominent of which was Great Britain. In January 1960, Britain formed a more loosely regulated economic union to rival the EC. The European Free Trade Association (EFTA), known colloquially as the "Seven," included Britain, Austria, Denmark, Norway, Portugal, Sweden, and Switzerland. A year later, Britain applied for membership in the EC, but France rejected their proposal to join the organization. The French government subsequently vetoed Britain's second application for membership in 1964.

Britain, along with Ireland, Denmark, and Norway, became members of the EC in 1973. In a series of accessions, six more nations joined the EC before 1995. The organization adopted a more ambitious mandate in the 1990s, establishing government and judiciary organizations in an attempt to closely unite European interests. Adoption of the new mandate by member states established the European Union.

Organization. Today's EU mission encompasses more than economic goals. The principal objectives of the EU are to establish European citizenship, ensure civil rights of European citizens, promote social progress, protect European security, and ensure justice. To these ends, the European Union maintains its own government and supporting agencies. These institutions are granted sovereignty by the member states to legislate European affairs and create international law. Final adoption of EU policy, however, is left to the individual member states.

Five primary institutions comprise the government of the EU. Its overall structure embraces the three-branch democratic model of government, with executive, legislative, and judicial bodies. The European Commission is the primary institution of the executive branch. Members are elected or appointed by the European Parliament. The Council of the Union is composed of representatives from the governments of the member states. The Council governs the EU as a collective, requiring majority support to set or endorse policy.

The European Parliament, the legislative body, is elected by the people of the member states. Committees within the European Parliament address specific concerns, such as health care, preservation of the environment, and trade regulation. The Court of Auditors, the committee responsible for overseeing and managing the EU budget, remains separate from every branch of the EU government, but works closely with the Parliament to appropriately allocate funds and resources.

The EU judiciary is the Court of Justice. The jurisdiction of the European court is somewhat dubious, and member states recognize its authority to varying degrees. The court is similar in structure and function to those of the United Nations, but is permitted to pursue only cases that affect member states.

A myriad of committees and support institutions comprise the rest of the EU government. The EU maintains its own central finance system, including the European Central Bank and the European Investment Bank. These contain funds used by the EU or granted to individual member states for various joint projects. In 1999, nine nations adopted a standard European currency, the Euro.

Membership. Fifteen member states currently comprise the European Union: Austria, Belgium, Denmark, Germany, Greece, Finland, France, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom of Great Britain and Northern Ireland. These member nations participate in the EU to varying degrees. For example, Britain participates in EU economic and trade associations, but uses its national currency, the pound, instead of the euro.

In 1998, the EU began negotiations with several eastern and southern European nations regarding EU expansion. Still recovering from decades of Soviet Communist domination, many of these nations possess fledgling free market economies. Introduction of former Eastern Block nations into the EU holds the potential for economic growth and expanded investment opportunities for European industry. However, expansion also poses liabilities to more economically robust EU nations.

The EU granted admission to the following candidate nations in 2002: Czech Republic, Cyprus, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovenia, and Slovakia. These nations officially join the EU on May 1, 2004, assuming that they ratify membership in a national, public referendum. Bulgaria and Romania are scheduled join the EU in 2007.

Some negotiations on expansion proved contentious. The EU denied Turkey's application to join the organization, despite the nation's numerous economic and trade associations with Europe. The EU will review Turkey's application again in 2004, if the nation furnishes evidence that it has met EU demands to improve human rights and maintain a stable democratic government. The nation of Cyprus, divided between Grecian southern Cyprus and nationalist Turkish Cypriots, failed to reunify before the EU accepted the national proposal to join the EU. Therefore, only the independent half of the nation will join the EU in 2004.

Some nations in Western Europe have chosen to remain outside of the European Union. Switzerland, and EFTA members, did not join the union on the grounds that membership in the EU threatened its national policy of declared neutrality. Norway also chose to exclude itself from EU membership.

Common defense and security: the future of the EU. A series of treaties in the 1980s and 1990s expanded the political, defense, and military role of the European Union. Formerly an instrument of economic and social policy, the EU adopted the Common Foreign and Security Policy (CFSP) in response to global instability and the rise or terrorism. The creation of the European Security and Defense Policy (ESDP) followed, outlining the EU's international responsibilities to defend European territory and interests while cooperating with organizations such as the North Atlantic Treaty Organization (NATO) and the United Nations.

Defense and security strategy remains one of the most contentious aspects of European Union policy. Some member states prefer to rely on their connections to NATO, or their own defenses, for protection. Others are wary of creating an EU military force under international command.

The EU established several crisis management tasks, known as the Petersberg Tasks, a foreign policy priority. For the purpose of humanitarian aid and rescue, peacekeeping, and crisis management, the EU created a military task force of 60,000 reserve troops. Member states can choose to contribute and deploy national military troops to EU operations on a case-by-case basis.

The EDSP launched its first operation, a police mission in Bosnia and Herzegovina, in January 2003. The first EU military operation commenced in Macedonia two months later.

With the aid of ESDP liaisons in 2002, the EU candidate nations signed a declaration warning Iraqi leader Saddam Hussein that military action was justified if United Nations weapons inspections were not permitted to freely proceed. The statement angered several EU members, causing a rift in EU foreign policy. Although the EU did not formally support the subsequent United States led action in Iraq, several member and candidate nations supported the Coalition military action. Some of the most influential EU nations, such as France and Germany, voiced strong opposition to the 2003 war in Iraq.

FURTHER READING:

ELECTRONIC:

European Union. <http://www.europa.eu.int> (May 9, 2003).

SEE ALSO

NATO (North Atlantic Treaty Organization)
United Nations Security Council

Executive Orders and Presidential Directives

Executive orders and presidential directives, as their name suggests, come from the president of the United States. Executive orders are unclassified, and in practice carry the force of law, though they remain controversial inasmuch as they amount to government by virtual edict. Presidential directives are classified, and thus the public is not even aware of their content. Both types of rules, along with directives from various security agencies, provide the guidelines by which the United States intelligence community operates.

Executive orders. President Theodore Roosevelt initiated the practice of issuing executive orders at the beginning of the twentieth century, and their numbers grew with each successive administration, until by the early twenty-first century they numbered more than 50,000. The actual numbers designating the orders are relatively low: for example, that of the order by which President George W. Bush froze terrorist organization assets in the aftermath of the September 11, 2001, attacks is only 13224. But these low numbers conceal the fact that many executive orders have been amended by number or letter extensions thus: xxxx-A, xxxx-B, and so on.

Among the executive orders of significance to the intelligence community are those dealing with classification and declassification of national security information. These go back at least to the time of President Richard M. Nixon, whose Executive Order 11652 (1972) stipulated that virtually all records would be declassified after 30 years. President Carter, in Executive Order 12065 (1978), called for a review of records after just 20 years with an eye toward declassification. In 1982, President Ronald Reagan bucked the trend, tightening the standards with Executive Order 12356, which favored continued classification and even provided conditions for the reclassification of previously declassified documents. With Executive Order 12958,

discussed elsewhere in the context of classified information, President Clinton returned to the earlier trend toward declassification.

Most administrations from the 1960s onward have also issued executive orders concerning the intelligence community, its operations, and/or specific aspects of security and intelligence. President Reagan, for instance, signed Executive Order 12333, "United States Intelligence Activities," in April 1981. President Clinton's Executive Order 12968, in 1995, provided conditions whereby security clearances would be granted.

The Supreme Court has ruled that executive orders have the force of law only if they are consistent with the provisions of the Constitution and/or receive congressional authorization. In practice, however, these orders have served as a means whereby presidents make law without recourse to the system prescribed in the Constitution.

Presidential directives and other guidelines. At least executive orders are unclassified; by contrast, presidential directives are not open to public knowledge. They exist, however, and have helped to guide security and intelligence policy since the administration of President John F. Kennedy.

Most administrations have their own names for presidential directives; thus under President George Bush (president, 1989–1993), they were known as national security directives (NSDs). President Clinton called them presidential decision directives, while President George W. Bush designated them national security presidential directives. An example of a known presidential directive is NSD 63, issued by George H. W. Bush in October 1991 to guide background checks for the issuance of Sensitive Compartmented Information (SCI) security clearances.

In addition to executive orders and presidential directives, other regulations guiding intelligence and security operations in the United States include National Security Council (NSC) intelligence directives (NSCIDs), Director of Central Intelligence (DCI) directives (DCIDs), and Department of Defense (DoD) directives. Whereas the guidelines from the president tend to be general, those from the NSC, DCI, and DoD are much more specific.

FURTHER READING:

BOOKS:

Mayer, Kenneth R. *With the Stroke of a Pen: Executive Orders and Presidential Power.* Princeton, NJ: Princeton University Press, 2001.

National Security: The Use of Presidential Directives to Make and Implement United States Policy: Report to the Chairman, Committee on Government Operations, House of Representatives. Washington, D.C.: Government Printing Office, 1988.

Richelson, Jeffrey T. *The United States Intelligence Community,* third edition. Boulder, CO: Westview Press, 1995.

ELECTRONIC:

Executive Orders. National Archives and Records Administration. <http://http://www.archives.gov/federal_register/executive_orders/executive_orders.html> (January 22, 2003).

SEE ALSO

Classified Information
Interagency Security Committee, United States
PFIAB (President's Foreign Intelligence Advisory Board)
President of the United States (Executive Command and control of Intelligence Agencies)
Security Clearance Investigations
Terrorist Organizations, Freezing of Assets

Explosive Coal

DAVID TULLOCH

Explosives disguised as coal were made in World War II by both the British Special Operations Executive (SOE) and the American Office of Strategic Services (OSS) to be used against such targets as steam locomotives, ships, and factory furnaces. Explosive coal allowed operatives to target relatively unguarded coal storage areas that supplied heavy security installations. Many other disguised explosives were also made.

The SOE's Section D made a number of disguised explosives. Their explosive coal design was a hollow shell in two halves that looked like coal and could be filled with plastic explosive and fitted with an igniter match, fuse, and detonator. The coal could then be hidden in enemy coal bins, and would be triggered when burned. Dead rats filled with plastic explosive were also used against the same targets. Like the coal, these could be casually tossed into coal stores by operatives, or left in factories, as the most common method of disposal of dead vermin was to burn them in the nearest furnace. After initial successes in Belgium, the Germans discovered a downed British plane containing a number of these vermin bombs, and so changed their rat disposal methods. The SOE also produced explosive logs, cow-pats, mule dung, and even explosive elephant dung.

The OSS Office of Science Research and Development went a step further with their explosive coal design by providing a Coal Camouflage Kit. Coal comes in many varieties, and there are significant differences in appearance depending on the region and grade of coal. Lignite coal, for example, is brown in color, while anthracite coal is a deep black. The Camouflage Kit contained paints, brushes, and other tools to enable operatives to match the explosive coal more exactly to the target type. Another

innovative OSS-disguised explosive looked identical to wheat flour and could even be added to milk or water and baked into a loaf before use. While having great novelty value, the actual operational value of weapons such as explosive coal was small in comparison to more conventional forms of explosives.

FURTHER READING:

BOOKS:

Ladd, James, and H. Keith Melton. *Clandestine Warfare: Weapons and Equipment of the SOE and OSS*. London: Blandford, 1988.

Melton, H. Keith. *OSS Special Weapons and Equipment: Spy Devices of World War Two*. New York: Sterling Publishing Co, Inc., 1991.

ELECTRONIC:

International Spy Museum, 800 F Street NW, Washington, D.C. <http://www.spymuseum.org.> (December 19, 2002).

Museum of World War II, 46 Eliot Street, Natick, MA, 2001. <http://www.museumofworldwarii.com.> (December 19, 2002).

SEE ALSO

OSS (United States Office of Strategic Services