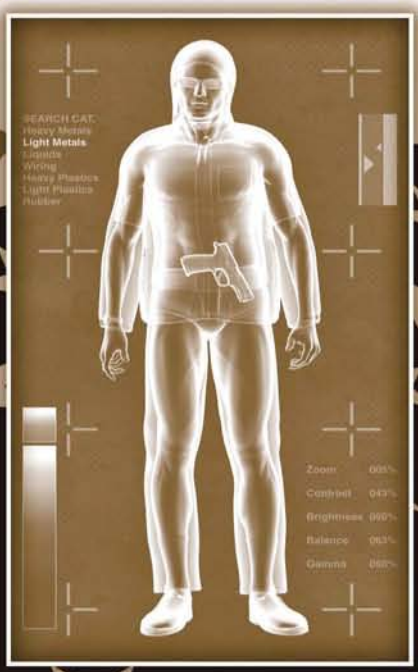
National Security Issues in Science, Law, and Technology

Edited by Thomas A. Johnson



CRC Press
Taylor & Francis Group

National Security Issues in Science, Law, and Technology

National Security Issues in Science, Law, and Technology

Edited by **Thomas A. Johnson**

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an informa business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 1-57444-908-7 (Hardcover)
International Standard Book Number-13: 978-1-57444-908-2 (Hardcover)

Library of Congress Cataloging-in-Publication Data

National security issues in science, law, and technology / [edited by] Thomas A. Johnson.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-57444-908-2 (alk. paper)
1. Intelligence service--United States. 2. National security--United States. 3. Terrorism--United States--Prevention. 4. Illegal arms transfers--Prevention. 5. Forensic sciences. I. Johnson, Thomas Alfred. II. Title. III. Series.

JK468.I6N38 2007
355'.033073--dc22 2006035229

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Table of Contents

Preface

Since the tragic attacks that occurred on September 11, 2001, our nation has focused its attention and resources on issues central to our homeland and national security. Particular focus has been directed to the prevention of any further terrorist attacks, especially an attack that may use chemical, biological, nuclear or radiological dispersal devices, or dirty bombs. Our nation's leaders also recognize that we are vulnerable to terrorists who would utilize agricultural terrorism and insect weaponization attack strategies. In short, our nation's critical infrastructure is at risk and in need of continued protection and vigilance.

To properly address these threats and weapons of terrorism, we must apply a very rigorous process of risk assessment, and learn how to best manage and mitigate the risk our nation now confronts. This also suggests that the structure of national security decisions should be premised on decision theory and science, while minimizing political posturing.

Our elected leaders and senior executives have been confronted with a range of issues never before faced with the intensity that is now occurring on a daily basis. The scope of national security policies and decisions required by our policymakers has called for an improved quality of all-source intelligence. Indeed, the overriding purpose of our intelligence community is to collect, analyze, and forecast patterns and trends that will enable our policymakers to make better informed decisions. To create effective policies that protect our national security, our decision makers and elected governmental officials must also possess a rich understanding and appreciation of science, law, and technology.

The range of legal issues and challenges that confront the very foundation of our democracy must be made by closely following the threads of our Constitution. We will continue to experience legal issues that call for dispassionate analysis of our intelligence, law enforcement and military operations actions. Both the Congress and the Courts will be further pressed to make new laws and interpret existing laws to protect our nation's heritage and future.

Finally, our nation's impressive national laboratory system is also at the crossroads of re-focusing its impressive array of talented people to address a

new and emerging role in homeland security. The administrators and managers within our national laboratory system will be called upon to redirect and refocus on the very problems terrorists can induce through their use of the weapons we have described, as well as weapons we have yet to confront.

Thomas A. Johnson

Acknowledgments

This book is the result of many people providing their insights and efforts in making it possible. First and foremost are the outstanding chapters prepared by each of my contributing authors. Their vision and insights as to how our nation can enhance our security is a testament to their expertise and individual leadership. Each of these outstanding colleagues gave considerable time from their schedules so that we might provide our readers with an overview of the important issues and challenges that confront our nation.

Dr. Michael Allswede, Dr. Simon Kenyon, and Dr. Fred Cohen are three of the most distinguished international scholars in their respective fields. Their groundbreaking work in bioterrorism, agroterrorism, and computer security and information assurance is among the most important in their respective fields. It is such an honor to work with each of these thoughtful and outstanding scholars.

Dr. Lucy Savitz, Roberta Lavin, and Elisabeth Root's work in Geographic Information Systems (GIS) is providing new and important tools that are being utilized by federal, state, and local agencies in their efforts to secure our nation. Dr. Savitz has provided our nation with a rich body of literature from her previous innovative and groundbreaking work in GIS, and we look to her leadership for additional writing and research.

David York's fascinating work on the illicit trafficking in nuclear and radiological materials promises to be one of the first of many important contributions we can expect to see from this innovative scientist.

Professor James Matschulat, who is now embarking on a new career in academia after a most impressive and successful career as a chief executive in the corporate world, has enriched our academic program beyond our expectations. His enthusiasm, writing skills, and gift for working with students clearly demonstrate that he belongs in academia. I would be remiss if I did not mention my deep gratitude to Robert Alvine and William Alvine for their encouragement and assistance in transforming this corporate executive into an academician.

Another important debt is owed to Justice George Nicholson of the California Court of Appeals for his encouragement and foresight to our nation's security. I am particularly indebted to Justice Nicholson as he was singularly

responsible for Professor Roy Shannon joining our team. Professor Shannon has not only excelled in the classroom, but also as an important contributor to this text. He promises to become one of our most prolific authors in this new emerging field of national security law.

Dr. Richard Neiser is truly one of our nation's leading scientists, and his thoughtful approach to the field of national security will be profound, not only for the manner in which he encourages other scientists to apply their discipline skills and knowledge to the security needs of our nation, but also for the vision he offers his colleagues.

Our publisher, Taylor & Francis Group, has provided excellent guidance and assistance throughout this project. Becky McEldowney, Carolyn Spence and, especially, Jill Jurgensen and Jay Margolis were so gracious in both their assistance and their patience. Each and, collectively, all four represent the best in the publishing world, and it is an author's dream to work with professionals such as these.

Finally, and most important of all, is the guidance and support offered by my wife, Colleen, who in addition to standing by my side and being my lifetime partner, has enabled our marriage to also include a working professional relationship. She has worked with each of our contributing authors and her editorial advice and skills have been reflected in the quality of this book. I am and will forever remain indebted to her for her wise counsel and sensitive support.

Thomas A. Johnson
Editor-in-Chief

Editor

Thomas A. Johnson

Dr. Thomas Johnson presently serves as dean of the Henry C. Lee College of Criminal Justice and Forensic Sciences and also dean and director of the University of New Haven, California Campus. He received his bachelor's and master's degrees from Michigan State University and completed his doctorate in criminology at the University of California, Berkeley. Dr. Johnson founded the Center for Cybercrime and Forensic Computer Investigation and serves as director of the Forensic Computer Investigation Graduate program. Additionally, he was responsible for developing the on-line program in Information Protection and Security at the University of New Haven. Dr. Johnson also founded the Graduate National Security program with campus offerings in Connecticut, Virginia, and two National Nuclear Security Administration laboratories in California and New Mexico.

Currently, Dr. Johnson serves as a member of the FBI Infraguard program and also a member of the Electronic Crime Task Force, New York Field Office, U.S. Secret Service. The U.S. Attorney General appointed him as a member of the Information Technology Working Group and he served as Chair, Task Force Group on Combating High Technology Crime for the National Institute of Justice. He was also appointed an advisor to the Judicial Council of California on the Court Technology Task Force by the California Supreme Court.

Dr. Johnson has published 4 books, 13 refereed articles; he holds copyright on 4 software programs and, in October 2000, his chapter on "Infrastructure Warriors: A Threat to the U.S. Homeland by Organized Crime," was published by the Strategic Studies Institute of the U.S. Army War College. In addition to lecturing at the U.S. Army War College, Carlisle Barracks, he has lectured at the Federal Law Enforcement Training Center and at numerous universities.

Dr. Johnson has appeared many times in both state and U.S. courts as an expert witness and was a member of the Select Ad Hoc Presidential Investigative Committee and consultant to the American Academy of Forensic Sciences in the case of Sirhan B. Sirhan regarding evaluation of ballistics and physical evidence concerning the assassination of U.S. Senator Robert F. Kennedy in June 1968.

Authors

Michael P. Allswede

Dr. Michael Allswede specializes in emergency medicine, critical care medicine, and medical toxicology and has devoted a career to improving medical response to disasters and terrorism. He has developed several operational programs in the areas that are in use today. Among these is the Strategic Medical Intelligence project that has taken its place in the Pittsburgh Field Office of the Federal Bureau of Investigation and has served as an organizing principle for Interpol efforts in worldwide terrorism. The RaPiD-T program is the educational program taught by the Pittsburgh Emergency Medical Services and serves to organize response to toxic, or infectious events. Lastly, the Rational Response Matrix project serves as a response modeling tool and modular disaster plan framework for several health systems.

Dr. Allswede is currently the program director at the Conemaugh Health System's Program in Emergency and Disaster Medicine, a residency that combines training in emergency medicine and disaster medicine to create physician leaders of tomorrow. Dr. Allswede also serves on several boards and advisory panels, including the informal advisory board to Interpol's Bioterrorism Unit and the Agency for Healthcare Research and Quality Altered Standards of Care in Mass Events. Dr. Allswede also serves as a tactical medicine asset for the Pennsylvania State Police.

Fred Cohen

Dr. Fred Cohen is best known as the inventor of computer virus defense techniques, the principal investigator whose team defined the information assurance problem as it relates to critical infrastructure protection today, as a seminal researcher in the use of deception for information protection, and as a topflight information protection consultant. But his work on information protection extends far beyond these areas. In the 1970s, he designed network

protocols for secure digital networks carrying voice, video, and data; he also helped to develop and prototype the electronic cash watch for implementing personal digital money systems. In the 1980s, he developed integrity mechanisms for secure operating systems, consulted for many major corporations, taught short courses in information protection to over 10,000 students worldwide, and in 1989, he won the prestigious international Information Technology Award for his work on integrity protection. In the 1990s, Dr. Cohen developed protection testing and audit techniques and systems, secure Internet servers and systems, defensive information warfare techniques and systems, early systems using deception for information protection, and bootable CDs designed for forensics and secure server applications. All told, the protection techniques he pioneered now help to defend more than three quarters of all the computers in the world.

Dr. Cohen has authored nearly 200 invited, refereed, and other scientific and management research articles. His most recently published books include: *World War 3: We are losing it and most of us didn't even know we were fighting in it — Information Warfare Basics,* ASP Press, 2006, and *Frauds, Spies, and Lies, and How to Defeat Them*, ASP Press, 2005. He received his M.S. in information science from the University of Pittsburgh in 1980 and his Ph.D. in electrical engineering from the University of Southern California in 1986. The reader is invited to find out more about Dr. Cohen at his website: http://all.net or his books at ASP-Press.com

Simon J. Kenyon

Dr. Simon J. Kenyon is an extension veterinarian and associate professor of population health at Purdue University's School of Veterinary Medicine. He teaches and practices dairy cow production medicine and teaches veterinary students about foreign animal diseases. He delivers farmer and public education programs on animal diseases and on health risk to humans from diseases, such as, bovine spongiform encephalopathy (BSE) and avian Influenza. He has studied foreign animal disease threats at the USDA's Foreign Animal Disease Diagnostic Laboratory on Plum Island and spent 10 years on assignment for the British Overseas Development Administration in Sudan and Indonesia dealing with epidemic disease diagnosis and disease reporting. He helped develop a nationally recognized program for aiding and rescuing animals after natural disasters and is a member of the Executive Committee of the Extension Disaster Education Network (EDEN). His publications include coauthorship of *Emergency Management of Disasters Involving Livestock in Developing Countries*, and the *Diagnostic Manual for Field Veterinarians*, which was published by the Veterinary Research Administration in Sudan and adopted as a training manual by the Food

and Agriculture Organization (FAO) of the United Nations Global Rinderpest Eradication Program. He received his veterinary degree from London University in 1969 and a Ph.D. in immunology from the University of Pennsylvania in 1976.

Roberta P. Lavin

Captain Roberta P. Lavin is currently working on a doctorate in nursing at the Uniformed Service University for the Health Science and also serves as the chief of staff to the Assistant Secretary for Public Health Emergency Preparedness at the Department of Health and Human Services. Prior to joining the Office of the Assistant Secretary, Captain Lavin was the director of the Secretary's Operations Center from October 2001 through March 2003. During her career, Captain Lavin has held a variety of positions including chief of field operations for the Division of Immigration Health Services, assistant health services administrator and clinical coordinator for the Federal Correctional Institution in Tuscon, Arizona, and nurse practitioner at St. Elizabeth Hospital in Washington, D.C. She holds a bachelor of science in psychology and a master of science degree in nursing as well as a master of arts in disaster and emergency management.

James O. Matschulat

James O. Matschulat**,** MBA, is a visiting associate professor in the Graduate National Security Program offered by The Henry C. Lee College of Criminal Justice and Forensic Sciences at the University of New Haven**.** Professor Matschulat's focus is on the administration of national security and he has been in the risk trade for over 40 years. He began his career as an insurance underwriter with Chubb & Son, Inc. and served as an adjunct associate professor at The College of Insurance (now St. John's School of Risk Management) and as a risk management consultant. He was also a principal at McKinsey & Company, Inc. and CEO of Middlesex Mutual Assurance Company, Inc.

Richard Neiser

Dr. Richard Neiser is currently manager of the Applied Systems and Materials Science Department in the Systems Assessment and Research Center at Sandia National Laboratories in Albuquerque, New Mexico. Born and raised in Pittsburgh, Pennsylvania he received his bachelor's and master's degrees in materials science and engineering from Virginia Tech in Blacksburg, Virginia.

Dr. Neiser performed his Ph.D. studies at the State University of New York at Stony Brook, Long Island. For 6 years, he worked at Brookhaven National Laboratory on Long Island operating x-ray facilities for the Naval Research Laboratory and Oak Ridge National Laboratory. Upon completing his doctorate, Dr. Neiser received an Alexander von Humboldt fellowship to study in Germany and performed post-doctoral research at Aachen Technical University and at the University of the Federal Armed Forces in Hamburg. Since moving to New Mexico in 1991, Dr. Neiser has worked at Sandia National Labs on a broad range of applied engineering projects in the area of national security. He is married and has three children.

Elisabeth Root

Elisabeth Root is a medical geographer specializing in modeling geographic information systems (GIS) data and cartographic analysis. Her current research involves the geographic analysis of the supply and demand of health services, specifically examining market characteristics and health outcomes in order to identify geographic areas with inadequate access to care or disparities in the quality of care. Root is also involved in research examining the relationship between the built environment and health behaviors and health outcomes. She uses GIS and spatial statistics software to examine geographic variation quality measure, health outcomes, and hospital services. Her work at RTI International in Durham, North Carolina includes data collection and database development activities, geographic analysis as well as project management and qualitative research. Prior to working at RTI, Root worked at the U.S. Census Bureau where she was responsible for the creation and design of county-level maps for the *Census 2000 Brief* publication series. She also acted as the lead geographic analyst in the development of the new Core Based Statistical Area (CBSA) Metro- and Micropolitan areas and assisted with final quality check activities for the Census 2000 public use files.

Lucy Savitz

Dr. Lucy Savitz holds a Ph.D. from the Department of Health Policy and Administration at the University of North Carolina and an MBA from the University of Denver. With more than 20 years experience in health-care delivery and health services research, she has worked as a financial planner at UNC Health Care, a researcher at the Cecil G. Sheps Center for Health Services Research, as a faculty member at the UNC School of Public Health, and most recently as a senior researcher at RTI International in Durham, North Carolina and now Abt Associates, based in Cambridge, Massachusetts.

Prior to relocating to North Carolina, Dr. Savitz served as an economist for the Colorado Legislative Council. Dr. Savitz's applied research has focused on preparedness, safety, and quality in health care. She is recognized as a thought leader in implementation and partnership science and is published extensively in the peer-reviewed literature and over a dozen book chapters as well as coediting *Geographic Methods for Health Service Research*. Dr. Savitz has been acknowledged as an examiner for the 2001 and 2002 Malcolm Baldrige National Quality Program, administered by the National Institute for Standards and Technology in the U.S. Department of Commerce and the American Society for Quality. She is also a senior scientist in the Intermountain Health Care Quality Institute and Research Fellow at the Cecil G. Sheps Center for Health Services Research (UNC).

Roy Shannon

Roy Shannon is a Distinguished Special Lecturer at the University of New Haven, National Security Program, Sandia National Laboratory campus. He is a member of the prosecution team, San Joaquin County District Attorney's Office, Homicide and Gang Unit–California District Attorneys Association Legislative Office. Shannon served as a judicial extern in the California Third Appellate District Court of Appeal, Chamber of Associate Justice George Nicholson, and is a United States Department of Defense and Intelligence Community consultant and contractor (executive director of Katabatics and ArdRI systems). He received his J.D. from the McGeorge School of Law, 2005, and is a Governmental Affairs Certificate Holder. Twice published in *McGeorge Law Review* (35 McGeorge L. Rev 606, 36 McGeorge L. Rev. 727), he also is the research editor for *Journal of National Security Law & Policy*, Vols. 1-2. Shannon received his B.A. from Texas Christian University (TCU), 1989 summa cum laude in research psychology and foreign languages (Russian, German). He is a member of Phi Beta Kappa and is currently pursuing Arabic language coursework at California State University in Sacramento.

David York

David York received his undergraduate education in molecular genetics from the University of New Mexico (UNM) in 2003 and a master's of national security and information protection and security from the University of New Haven (UNH) in 2005. York began his career in international security at Sandia National Laboratories during his senior year at UNM. He was involved in biological monitoring of feedlots to combat agroterrorism. He also assisted on projects involving nuclear and radiological terrorism, which introduced him to the international nuclear security scene.

Currently, York is participating on several international projects involving nuclear transparency and remote monitoring of nuclear fuel cycles. He also directs the Illicit Nuclear Trafficking Framework at Sandia for the modeling and analysis of nuclear and radiological trafficking at the International Nuclear Safeguards Conference and the International Workshop on Radiological Sciences and Applications held at the International Atomic Energy Agency (IAEA). He has also presented at the International Nuclear Materials Management Conference and the American Nuclear Society Conference on nuclear transparency. In addition, York is a member of the Generation IV Reactor International Nuclear Experts Group for Proliferation Resistance and Physical Protection (GenIV-PRPP) where he specializes in providing physical protection analyses of nuclear fuel cycle facilities.

York is married to Jennifer York D. O., and has two rottweilers, Lilly and Roxy.

Section I

Terrorism: Threats, Vulnerabilities, and Weapons

1 An Introduction to the Intelligence Process for Addressing National Security Threats and Vulnerabilities

THOMAS A. JOHNSON

Contents

A significant range of issues in science, law, and technology are all a part of our nation's National Security challenges. The decision makers we hold responsible for protecting our nation require a vast amount of information to base their policy judgments upon. Our nation must have at its disposal the most current defensive weapons systems based on the latest advances in science and technology. At the same time, our nation's leaders must have current information about potential threats that could harm our nation or our people. Since 1947, our nation has benefited from both a Department of Defense and an intelligence community. We look to our intelligence community to provide information to our president for the formulation of policies that will result in greater protection of our nation.

Since the close of the Cold War with the Soviet Union in 1991, there have been tremendous changes in our intelligence community and in its responsibilities.

These changes were all part of a "peace dividend" that had an enormous impact on how congressional support for our intelligence community had diminished. In fairness to the position of Congress, there was a shaping of this environment by the mistakes made in the mid-1970s by our intelligence community, which necessitated the greatest degree of congressional oversight ever experienced in the history of our nation's intelligence community.

The attack on our nation on September 11, 2001 refocused our nation's attention to our intelligence community, both in terms of the mistakes made and to the new set of challenges and expectations we have of our entire intelligence community. While there have been major reorganizations of the Central Intelligence Agency (CIA), and a new Director of National Intelligence (DNI), along with major reporting modifications and budgetary reallocations, the one thing that has not changed is the need for our intelligence community to provide current and accurate information on the potential threats our nation confronts. Today our concerns focus on how terrorist organizations might use biological, chemical, or nuclear weapons to attack us. Other modalities of attack range from radiological dispersal devices, commonly known as dirty bombs, to several forms of agricultural terrorism caused by the weaponization of insects.

This chapter will describe the intelligence process for collecting and analyzing information, which our intelligence community uses to provide to our nation's leaders, so they might formulate the policies and make the decisions that ultimately become our strategy for defending and protecting our nation. To place into perspective how the intelligence process works, it will be useful to understand how the President of the U.S. communicates and receives national security information to assist his office in formulating national security policy. This will entail a brief description of both the National Security Council and the White House Situation Room.

The National Security Council consists of the President, Vice President, Secretaries of State and Defense, Chairman of the Joint Chiefs of Staff, and the National Security Advisor to the President. The DNI serves as the Intelligence Advisor to the National Security Council. The National Security Staff reports to the National Security Advisor and consists of military officers, career civil servants, and political appointees who have day-to-day responsibility for conveying the wishes of the President to the intelligence community and for coordinating among the various departments and agencies. In essence, the National Security Council Staff is primarily interested in the execution of policy as defined by the President and senior presidential appointees.[1]

The White House Situation Room's (WHSR) important daily role with the National Security Council is basic to how the White House and the National Security Council function in providing current intelligence information to key decision makers, including the President.

> The White House Situation Room (WHSR) was established by President Kennedy after the Bay of Pigs disaster in 1961. That crisis revealed a need for rapid and secure Presidential communications and for the White House coordination of the many external communications channels of national security information, which led to the President. Since then, the mission of the White House Situation Room has been to provide current intelligence and crisis support to the National Security Council Staff, the National Security Advisor and the President. The SIT room is composed of approximately 30 personnel, organized around 5 watch teams who provide 7-day, 24-hour monitoring of international events.[2]

The Watch Team within the WHSR prepares a "Morning Book," which contains the Senior Executive Intelligence Brief, the State Department Morning Summary, and diplomatic cables and intelligence reports. These reports are transmitted to the National Security Advisor who presents them to the president.[3] The president's daily brief was formerly prepared and presented by the CIA, but now is presented to the president by the DNI. The intelligence process that typically begins by a request from the "customer," which may emanate from the president, the National Security Council, or very senior leadership executives of the government will begin a series of events that ultimately will entail the preparation of a series of intelligence products. The dissemination of these intelligence reports will eventually be routed to the DNI and to the National Security Council and WHSR's external channel operations. However, not all intelligence products will follow this pathway, as the Department of Defense is also both a producer and consumer of intelligence information at levels of the Pentagon through to senior battlefield commanders.

The intelligence community will be discussed in a variety of roles and activities throughout this chapter, therefore, the 16-member agencies of our intelligence community are presented in alphabetical order as follows:

- Air Force Intelligence, Surveillance, and Reconnaissance
- Army Military Intelligence
- Central Intelligence Agency
- Coast Guard Intelligence
- Defense Intelligence Agency
- Department of Energy — Office of Intelligence
- Department of Homeland Security — Information Analysis and Infrastructure Protection Directorate
- Department of State — Bureau of Intelligence and Research
- Department of Treasury — Office of Intelligence and Analysis
- Drug Enforcement Administration — Office of National Security Intelligence

- Federal Bureau of Investigation
- Marine Corp Intelligence
- National Geospatial Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- Navy Intelligence — Office of Naval Intelligence

The Intelligence Process

For purposes of best understanding how our intelligence process provides our decision makers with the information they can use to frame their policies, the balance of this chapter will follow the outline of the actual intelligence process as follows:

1. Customer Requirements
2. Collection Disciplines
3. Processing and Exploitation of Data
4. Analysis and Production
5. Covert Action/Special Activities
6. Counter Intelligence
7. Dissemination of Intelligence Products
8. Policy
9. Evaluation

Customer Requirements

This is a critical phase in the entire intelligence process since there must be a clear understanding of what the intelligence problem is before one can begin the collection and analysis stages. Therefore, customer "needs," particularly if they are complex and time sensitive, require a very careful assessment before being expressed as intelligence requirements. Lisa Krizan observes that the "five Ws" (who, what, when, where, and why) are a good starting point for translating intelligence needs into requirements. A sixth related question, "how," may also be important to the analysis.[4] In short, the intelligence requirements translate the customer needs into an intelligence action plan, which in turn guides the collection strategy and the entire production of the intelligence product.

At the national level, it is the National Security Council that establishes our nation's policy and intelligence priorities. The National Security Advisor and the DNI must establish a clear understanding as to articulating intelligence priorities in such a manner that the entire intelligence community comprehends the specific nature of the intelligence problem or problems.

Collection Disciplines

Once the process for translating the customers' intelligence needs into a set of intelligence requirements with senior officials establishing an intelligence action plan is completed, then the process for selection of collection methodologies can take place. The intelligence need defines the collection requirement and ultimately the selection of collection sources. The collection strategy can use one or more of the collection disciplines. The four major collection disciplines are:

1. SIGINT — signals intelligence
2. GEOINT — geospatial intelligence
3. MASINT — measurement and signature intelligence
4. HUMINT — human intelligence

For the intelligence process to work at its best level, the intelligence community seeks to produce all-source intelligence or, as it is oftentimes referred to, fusion intelligence. In other words, the intelligence that is collected comes from as many collection sources and subdisciplines as possible. To appreciate the role and function each collection discipline plays in providing all-source intelligence, a brief description of each of the five collection disciplines and their subdisciplines will be presented.

The first major collection discipline, signals intelligence (SIGINT), is collected by satellites and by ships and planes. SIGINT consists of multiple types of intercepts: one type refers to the interception of communication between two parties; this is the subdiscipline of communications intelligence (COMINT). Another type of intercept of signals is the capture of data relayed by weapons during a test; this is the subdiscipline of telemetry intelligence (TELINT). A third type of intercept is with electronic emissions from military and civilian weapons and tracking systems; this is within the subdiscipline electronic intelligence (ELINT).[5]

The National Security Agency (NSA) is responsible for both the collection of our signals activities and the subdisciplines of COMINT, TELINT, and ELINT. The National Security Agency also has the responsibility of defending our nation against any nation–state who would use signals intelligence against us. From a technological point of view, life was not as difficult for the National Security Agency at its creation in 1952, as there were only 5000 computers in the entire world and no fax machines or cellular telephones.

> Fifty years later in 2002 there were over 180 billion minutes of international phone conversations from some 2.8 billion cellular phones and 1.2 billion fixed telephones. Instant messaging generates 530 billion messages daily. As communications switch to fiber optic cable, the available volume will increase. Also, more phone calls are going over the Internet using the voice-over Internet-protocol (VOIP) technology.[6]

As of 1995, the National Security Agency was capable of intercepting the equivalent of the entire collection of the U.S. Library of Congress (1 quadrillion bits of information every 3 hours). By 1997, new high tech collection systems produced even a more massive volume of intercepts; however, the NSA was swamped with intercepts and only able to process approximately 1% of the intercepts.[7] This problem came to a head on September 11, 2001 with our inability to capture intercepts that might have alerted our intelligence community to Al-Qaeda attack plans. Of course, there were additional reasons for our inability to capture and process the communication patterns of Al-Qaeda cells, among these reasons were the media's public disclosure of our earlier capture of cell phone and fax intercepts that alerted Al-Qaeda to avoid using these devices. Another reason centered on the 20% cut in intelligence personnel mandated by Congress as a result of the "peace dividend" at the close of the Cold War in 1991. Still another reason focused on our inability to translate the different Arabic languages from the Middle East, which include Farsi, Pashto, Dari, Hindi, and Urdu.

The war against terrorism has created additional problems for the capture of SIGINT. Our SIGINT collection discipline was designed to collect intelligence on the Soviet Union and other nations. Terrorist cells offer much smaller signatures that may not be susceptible to interception by remote SIGINT sensors. Therefore, we may have to rely on sensors that have been placed close to the target by human agents. In effect, HUMINT will become the enabler for SIGINT.[8] Signals intelligence will continue to play a very prominent role in providing fusion intelligence to the finished intelligence products produced by our intelligence community.

The second major collection discipline, geospatial intelligence (GEOINT), used to be referred to as imagery intelligence (IMINT); the current terminology has been renamed and the National Imagery and Mapping Agency that was responsible for processing and assessing images now falls under the National Geospatial Intelligence Agency. Geospatial intelligence is defined as "information about any object — natural or manmade — that can be observed or referenced to the Earth and has national security implications."[9]

Images can be acquired by satellite over flights and electronically captured and sent to satellite collecting stations. Electro-optical (E-O) cameras are a camera type of satellite imaging sensor and provides high-resolution images. These E-O sensors can only capture images in the day and cannot effectively operate through cloud cover or heavy fog. Another sensing device on some satellites is synthetic aperture radar, which does permit the capture of images of earth through clouds, fog, haze, and darkness, but does not have the high resolution that is provided by E-O sensors.[10]

Imagery is a most compelling form of collected intelligence and this was appropriately documented in the Cuban Missile Crisis in which President Kennedy was able to provide clear and convincing proof to the world as to the intentions of the Soviet Union by displaying photos and images of Soviet missiles on Soviet ships and in Cuba itself.

Another method of capturing images is provided by unmanned aerial vehicles (UAVs), which unlike satellites fly closer to areas of interest instead of making the high altitude orbital pass. The advantage of UAVs centers on producing real-time images and images that can be gathered by pursuit directional systems from the ground, thus offering an immediate capture of intelligence. Another advantage is found in the ability to incorporate missiles on the UAV.

> The United States currently relies on two UAVs, the Predator and the Global Hawk. Predator operates at up to 25,000 feet, flying at the relatively slow speed of 84 to 140 miles per hour. It can be based as far as 450 miles from a target for 16 to 24 hours. Predator provides real time imagery and has been mated with air-to-ground missiles, allowing immediate attacks on identified targets instead of having to relay the information to nearby air or ground units . . . Global Hawk operates at up to 65,000 feet at a speed of up to 400 miles per hour. It can be based 3000 miles from the target and can operate over the target for 24 hours.[11]

Other forms of images are captured by infrared (IR) imagery, which produces an image based on the heat reflected by the surfaces being recorded. This provides the ability to detect warm objects such as tanks or planes being camouflaged or inside hangers. Also, it provides the ability to detect humans camouflaged under a heavy jungle canopy.[12]

The third major collection discipline, measurement and signature intelligence (MASINT), is technically derived intelligence that detects and identifies the "signature" or distinctive characteristics of targeted sources. MASINT uses a wide variety of sensors to detect and differentiate specific signatures that permit one to identify the presence of particular materials, such as molecules, types of crops, soil composition, industrial pollutants, chemical composition, and numerous other types of signatures. By detecting these "signatures," MASINT can make very important contributions to the intelligence community. MASINT collection systems include radar, spectroradiometric, electrical optical, acoustic, radio frequency, nuclear detection, and seismic sensors, as well as techniques for gathering chemical, biological, nuclear, and other material samples.[13]

There exist six subdisciplines to this very important and scientific collection system. The six subdisciplines to the measurement and signature intelligence collection system are:

1. Materials intelligence
2. Radar intelligence
3. Radio frequency intelligence
4. Geophysical intelligence
5. Electro-optical intelligence
6. Nuclear intelligence

Following is a brief description of three of these subdisciplines.

Materials intelligence is the collection, processing, and scientific analysis of gas, liquid, or soil samples. Material intelligence is critical to the collection against chemical, biological, and nuclear warfare threats. This subdiscipline is also crucial to our assessment of weapons of mass destruction (WMD). The inclusion of computerized databases of established signatures of gas, liquid, and soil samples permits identification of these items. *Radio frequency intelligence* consists of the collection and assessment of electromagnetic emissions, which assists in the identification of various weapon systems and also nuclear testing because of the ability to measure electromagnetic pulses, which are measurable bursts of energy. *Geophysical intelligence* captures through its sensors and permits analysis of emitted or reflected sounds, pressure waves, vibrations, and magnetic or ionospheric disturbances.[14]

Spectroradiometric sensors are critical to intelligence collection as any object with a temperature above absolute zero emits electromagnetic energy. The higher the temperature, the shorter the mean wavelength of the radiation. This scientific principle is what permits multi- or hyperspectral E-O/IR sensors to remotely determine material composition. This is how NASA was able to perform and analyze the chemical and mineral composition of the soil on Mars over 119 million miles from Earth.[15] This capability of utilizing sensors for our intelligence community provides a base of scientific richness that is invaluable. For example, hyperspectral imaging can differentiate one crop from another or one type of soil from another as well as measuring water and industrial pollutants, all capabilities useful to the intelligence community.

Macartney also observes that some of the more useful applications of MASINT include the following:

- Spectral analysis of jet or rocket exhaust that identifies the type of fuel and the specific type of vehicle, and even the throttle setting.
- F-15 Fire control radar can count the number of compressor blades on an approaching aircraft and the number of blades constitutes a "signature," thus identifying the engine itself and the type of aircraft.
- Laser remote sensing: Since WMD (chemical, biological, and nuclear) give off distinctive signatures (or their manufacture or storage involves signatures), and since WMD proliferation is one of the top priorities for the intelligence community, much of the MASINT effort has been pointed toward WMD detection.[16]

The fourth major type of collection discipline is human intelligence or HUMINT. This collection discipline was substantially impacted when President Carter appointed Admiral Stansfield Turner to assume the Director of Central Intelligence and, on assuming this role, Admiral Turner de-emphasized

the role of human intelligence in what was then known as the "Day of the Long Knife" in which our human intelligence capability was severely curtailed. The Carter Administration decided to pursue the more technological collection disciplines previously described. Also, as previously noted, the "peace dividend" of the 1990s as a result of the Cold War with the Soviet Union ending saw a further decline and retrenchment of our human intelligence capability. In fact, John E. McLaughlin, CIA deputy director of intelligence, noted that the reduction in intelligence community personnel was over 22% as a result of congressionally mandated action during the 1990s.

Human intelligence consists of espionage or spying and special activities, which include clandestine and covert operations. Also included within the operational subset of human collection activities will be counter-intelligence roles and responsibilities. Human intelligence becomes quite important in collecting information that the other collection disciplines are not fully capable of acquiring. Human intelligence requires agents to become proficient in a number of skill sets, such as evasion techniques, communications equipment, weapons, recruiting skills, knowledge of foreign countries, human asset management, and a general understanding of the tradecraft. After September 11, 2001, it became quite clear to the Congress and the nation that our intelligence community had to make a greater investment in our human intelligence capabilities. The collection systems, which were designed to work against large nation–states, were not functional against smaller terrorist nonstate operations, such as Al-Qaeda. The need to penetrate these terrorist organizations or to acquire information on their planned activities requires human intelligence capabilities. This process is a very difficult endeavor, as one has to identify individuals who will have information or access to information that is needed by the intelligence community. These individuals have to be managed in such a manner that the information acquired has value and is not part of a counter-intelligence activity or a plan for planting false information.

Human intelligence agents have to maintain cover stories or plausible reasons for being in a foreign nation. There are two types of cover: official and nonofficial. Agents with official cover hold other government jobs, such as a posting within an embassy. Nonofficial cover (NOC) avoids any overt connection between the agent and the government and makes the operation of this human intelligence agent very difficult since no overt contact can be made between the NOC agent and the agency. The use of NOCs is more complex and difficult, as they must maintain full-time jobs to fully explain their presence.[17]

Other forms of human intelligence activities may include paramilitary actions, covert special operational activities, and clandestine operations that may not be focused on collection activities, but in the process of fulfilling these responsibilities, information of value may be found that should be processed to the Directorate of Intelligence for further analysis.

In describing these four major collection disciplines, one major factor that one hopes to achieve is a fusion of information from all collection sources possible. Therefore, collection disciplines really are producing information, and the next step in processing this information goes to the stage of processing and exploitation, at which time this complex data and scientific information are further refined into information sets that ultimately are transmitted to the analysis and production stage for review by intelligence analysts.

Processing and Exploitation of Data

The processing and exploitation of data collected from the previously described collection disciplines reveal that much of the scientific data collected in signal intelligence, geospatial intelligence, and measurement and signature intelligence are simply not ready for submission to the analysis and production stage of this intelligence process. In other words, complex digital signals, foreign language that requires translation, and signature intelligence must be processed and converted into usable symbols or language that can be transmitted to the analysis and production stage. This is a very important phase of the intelligence process and if the data are not converted to useful information, it will minimize or preclude the intelligence analyst from producing usable intelligence reports or products. In short, the processing and exploitation phase of the intelligence cycle is critical to converting very technical collected data into information that will ultimately become processed into intelligence.

Analysis and Production

This important phase of the intelligence process is dependent on well-trained intelligence analysts. Analysis is not simply reorganizing data and information into a new format. The intelligence analyst's responsibility is to fully describe and provide as much usable and explanatory information about the intelligence target as possible. Intelligence assessments are based on the data and information captured by the collection disciplines and are refined by research methodologies used by the intelligence analyst. If the analysis of the data can reach beyond the descriptive and explanatory levels to a synthesis, which then results in an estimation, this will be of value and may be produced as an intelligence report or part of an intelligence product.

The purpose of intelligence analysis is to reveal to the ultimate policymakers the underlying significance of selected target information. Intelligence analysis involves estimating the likelihood of one possible outcome given the numerous possibilities that exist. Therefore, intelligence analysis involves forecasting and requires the analyst to provide a statement as to the degree of confidence held in a certain set of judgments, which are based on a certain set of explicit facts or assumptions.[18]

The intelligence analyst will deal with facts, findings, and forecasts in preparing the intelligence report.

- Facts: Verified information related to an intelligence issue.
- Findings: Expert knowledge based on organized information that indicates, for example, what is increasing, decreasing, changing, or taking on a pattern.
- Forecasts: Judgments (interpretations, predictions) based on facts and findings and defended by sound and clear argumentation.[19]

The intelligence analyst has the responsibility of reviewing the collected information and going beyond the descriptive and explanatory levels of analysis and to synthesize the facts by verification of information. The findings must be presented to the policymaker in such a fashion that the analyst forecast reduces the uncertainty that confronts decision makers and policymakers.

To effectively produce intelligence forecasts, estimates, warnings, or trends, the intelligence analyst must be able to apply the rigors of the scientific method to the intelligence analysis. To minimize error and institute proper controls, the intelligence analyst must clearly employ a research methodology and, where possible, statistical tests to provide for validated levels of statistical confidence. When decision makers are confronted with a range of difficult choices, they will demand as much confidence in the intelligence assessment or report as possible.

There are a number of analytical methods that intelligence analysts can employ in assessing a body of collected information that is presented to them for their review. Several of these methods of analysis have been designed and implemented because of past failures of intelligence estimates and reports. Some of the methods of analysis that intelligence analysts will use are:

1. Scientific method
   - Induction
   - Deduction
   - Abduction
2. Lynch pin analysis
3. Opportunity analysis
4. Competitive vs. cooperative analysis
5. Alternative analysis
6. Red cell analysis
7. Contingency analysis
8. High impact/low probability analysis
9. Scenario development
10. Indications and warnings
11. Computer and database analysis
12. Data mining analysis
13. Numerous other classified analytical bases for analysis

Ironically, until September 11, 2001 there existed little formal training for intelligence analysts within the intelligence community. Furthermore, university-based programs in preparing graduates to assume intelligence analyst positions were almost nonexistent. Given the incredible scientific detail that each of the previously described collection disciplines produces, our nation needs intelligence analysts that not only fully appreciate and can apply the scientific method, but they also are educated in a richness of calculus, physics, mathematics, biology, chemistry, and, in general, the hard sciences.

Covert Action/Special Activities

The CIA's principle role is in providing both clandestine and covert strategic services. The CIA's Directorate of Operations is responsible for providing both service and, in the process, the clandestine service operates to support military operations, law enforcement, and renders support to diplomatic/policy operations. Thus, the clandestine service is a very unique and versatile instrument of national power. Norman Imler best distinguishes the difference between clandestine and covert.

> Clandestine regards activities crafted, conducted, and intended to remain secret. Clandestine HUMINT activities use special means (tradecraft, in CIA parlances) to accomplish a collection task against a target, to produce information unobtainable by other means. This is espionage, more often referred to as spying. It is subdivided into foreign or positive intelligence, operational intelligence, and counterintelligence, which initially was referred to as negative intelligence.
>
> Covert regards activities crafted and conducted to keep the sponsor's hand hidden or plausibly deniable.[20]

In summary, covert action is an activity of the U.S. government designed to influence governments, events, organizations, or persons in support of U.S. foreign policy in a manner that is not attributable to the United States covert actions may require use of political, economic, propaganda, or paramilitary activities. Under current U.S. law, covert actions or special activities as they are now officially termed must be approved by the President of the U.S. in the form of a Memorandum of Notification and termed as a "finding." The Memorandum of Notification is transmitted to the Intelligence Oversight Committees of both the U.S. Senate and the U.S. House of Representatives. Covert actions are typically carried out by the CIA's Directorate of Operations, with the assistance as may be required from the Department of Defense and other members of the intelligence community.

In assessing other activities performed by both the clandestine service and covert operations, there has been a growing reliance on specialized intelligence

disciplines to counter the numerous security threats aimed at our nation. These six counter strategies are:

1. Counter-intelligence
2. Counter-terrorism
3. Covert action
4. Counter-proliferation
5. Counter-narcotics and counter-crime
6. Counter-denial and deception

While all six of the above counter strategies are very important, the counter-proliferation is probably the one area that best represents how all collection disciplines and the human intelligence areas could best work together, especially since the September 11, 2001 attacks.

> Counter-proliferation includes programs and activities designed to identify, monitor, and thwart efforts by foreign countries and groups that seek to possess weapons capable of causing mass casualties — radiological, chemical, biological, and nuclear arms often referred to as Weapons of Mass Destruction (WMD) . . . WMD are in many cases, accessible to foreign states and groups for little investment, but require networks of individuals to weaponize a capability . . . Counter-proliferation . . . is heavily dependent on science and technology and HUMINT — enabled access for success, particularly in the growing MASINT arena.[21]

In our nation's effort to combat terrorism, we are relying more on our clandestine services and especially our covert operations to neutralize and perform counter terrorist activities. The expectation of Congress and many critics of the performance of our intelligence agencies, particularly the CIA centered on the expectation that the intelligence community would have been able to detect the September 11, 2001 terrorist plot in time for measures to be taken to eliminate the threat. However, people have to appreciate that specific intelligence on terrorist threats are very rare, simply because we need the sources that could provide the information. Human assets are required to provide this information and since Congress and several Administrations (Carter and Clinton) severely cut back on our human intelligence capabilities, it has become almost impossible to acquire this information from natural sources.

> An additional complication in recruiting terrorist assets is that the individuals with the most information to offer tend to have considerable baggage, including possible involvement in past terrorist acts. Any use of such persons as intelligence assets requires additional

> checks and safeguards, including approval at high levels (up to the Director of Central Intelligence) and notification as appropriate to the Congressional Intelligence Committee. If the person may have violated U.S. law, the Department of Justice must also review the case and decide whether to seek or to waive prosecution. The National Commission on Terrorism stated that the CIA's guidelines for using such people as sources has hindered the recruitment of terrorist informants by making Intelligence Officers "risk aversive."[22]

Former Director of Central Intelligence, John Deutch, mandated the most restrictive use of CIA informants and this coupled with the language and religious views of Al-Qaeda provided almost insurmountable problems for penetrating this terrorist cell.

As Mark Lowenthal observes, the war on terrorism has focused attention on covert activity that does not fall into the customary range of actions — renditions. Renditions are the seizure of individuals wanted by the U.S. These individuals are living in countries where the U.S. cannot use legal processes to take them into custody. However, after the fugitive terrorist is captured and formally delivered to U.S. custody, the U.S. may retain custody of the individual or send the individual to the home nation of origin.[23] The issue of rendition has become a very sensitive matter for the U.S. government, engaging the Secretary of State and requiring explanation to officials of the European Union. Ultimately, the issue of maintaining custodial facilities in foreign countries or sending these individuals to the U.S. for custody and trial will pivot on the decision as to whether to use the criminal law process or the status of enemy combatants.

Of course, there are numerous forms of other special activities performed by the clandestine service and covert operations, but the previously described activities clearly portrays the role for enhancing the collection process in cooperation with the collection disciplines of SIGINT, GEOINT, and MASINT.

Counter-Intelligence

As discussed previously, the intelligence process consists of four major activities, three of which have been described: the collection process, the analysis and production process, and the covert action/special activities process. Counter-intelligence is the fourth of these major activities within the intelligence process and its responsibilities center on conducting activities and exploiting information collected on a nation's adversaries. This entails the identification, monitoring, manipulating, or neutralizing of any foreign intelligence threat to our nation. Currently, there are more than 45 countries that are attempting to commit some form of espionage on our nation. Counter-intelligence operations are designed to collect information on these activities and to affect appropriate action in response to these challenges.

Another major activity of our counter-intelligence process centers on internal monitoring of our Intelligence Agents, so that we preclude repeat episodes of former agents, such as Aldrich Ames and Robert Hanson, who provided information on our nation's secrets to the Soviet KGB. This role of internal affairs is quite different from the other activity of monitoring the Intelligence Agents of those groups or nations seeking to perform espionage acts against us; the collection methods are similar, but the process requires careful implementation as the potential for creating internal morale problems is very large.

Dissemination of Intelligence Products

The intelligence community has the responsibility of preparing and transmitting intelligence reports to the customer. The defined intelligence problem, which has been targeted by the appropriate collection disciplines and which has been processed by the analysis and production phase of the process will result in the form of an intelligence product moving from the intelligence producer to the consumer. The traditional intelligence products include the following reports:

- *The President's Daily Brief* is a daily report prepared by the CIA, but now delivered by the new DNI. It provides information as to any event that has national security ramifications and has occurred within the past 24 hours, anywhere in the world.
- *The Senior Executive Intelligence Brief* is prepared by the CIA in coordination with other intelligence agencies and provides a briefing of national security issues to senior executives and members of the Senate and House Intelligence Oversight Committees.
- *The National Intelligence Estimates* are the responsibility of National Intelligence Officers, who are members of the National Intelligence Council, which is now under the DNI. National Intelligence Estimates represent the opinion of the entire intelligence community and are presented to the president and the National Security Council by the DNI. National Intelligence Estimates are long-term intelligence products that estimate the likely events or direction an issue will take in the future. These are very important products that have the ability to shape the views of our policymakers. However, as with any intelligence product, the recipient may choose to follow its parameters, ignore it, or accept certain portions of the estimate.

Intelligence products or reports can also be presented in briefings to the president or senior officials. Intelligence reports can be transmitted via secure video conferencing methods, secure telephone calls, and secure and encrypted computer messages to senior government officials and to other intelligence agencies.

There are five categories of finished intelligence, and the three agencies responsible for producing all-source intelligence are the CIA's Directorate of Intelligence, the DIA's Directorate of Intelligence, and the State Departments Bureau of Intelligence and Research. Within the Department of Defense, there are four service agencies (Navy, Marine, Army, and Air Force) that also produce finished intelligence.

The finished intelligence categories available are:

1. *Current intelligence* addresses day-to-day events, seeking to apprise consumers of new developments and related background, to assess their significance, to warn of their near-term consequences, and to signal potential dangerous situations in the near future.
2. *Estimative intelligence* deals with what might be or what might happen. Its main purpose is to provide informed assessments of the range and likelihood of possible outcomes.
3. *Warning intelligence* sounds an alarm or gives notice to policymakers. This includes identifying or forecasting events that could cause the engagement of U.S. military forces. Warning intelligence also identifies events that could impact U.S. foreign policy.
4. *Research intelligence* consists of in-depth studies that underpin both current and estimative intelligence. Two categories of research are included: basic intelligence that consists primarily of the structured compilation of geographic, demographic, social, military, and political data on foreign countries; and intelligence for operational support incorporating all types of intelligence production and is tailored, focused, and produced for planners and operators.
5. *Scientific and technical intelligence* includes information on technical developments and characteristics, performance, and capabilities of foreign technologies. It covers the entire spectrum of sciences, technologies, weapon systems, and integrated operations.[24]

The dissemination of intelligence reports is an important phase of this entire process; however, one of the difficulties centers on the protection of sources and methods. Frequently, the recipient of such intelligence reports wants the assurance of the factual and objective veracity of the intelligence report, while at the same time, the intelligence-producing agency must be vigilant to protect sources and methods and may be limited in providing a full suite of information.

Policy

The entire intelligence process exists to provide the policymaker carefully analyzed and informed judgments on the particular problem under review so as to assist the policymaker in the decision-making process. It is imperative that

the Intelligence Officer and intelligence process maintain objectivity and not push for specific outcomes or choices. The intelligence process has a supporting role and should not cross over into advocacy of policies or positions. In short, the goal of the entire intelligence process is to put the policymaker in the best position available to make the best informed decision possible.

Evaluation

The intelligence process should undergo self-evaluation of the intelligence activities, reports, and products it produces. Lisa Krizan provides a very useful framework for intelligence product evaluation and customer feedback where the following constructs are suggested for use.

Accuracy: Were all sources and data free of technical error, misperception, and no attempt to mislead?

Objectivity: Were all judgments free of deliberate distortions and manipulations due to self-interest?

Usability: Was all production issued in a form that facilitated ready comprehension and immediate application?

Relevance: Was information selected and organized for its applicability to a customer's requirements, with potential consequences and significance of the information made explicit to the customer's circumstances?

Readiness: Are intelligence systems responsive to the existing and contingent intelligence requirements of customers at all levels of command?

Timeliness: Was intelligence delivered while the content was still actionable under the customer's circumstance?[25]

Conclusion

This chapter has focused attention on how our intelligence process works to protect our nation from national security threats and vulnerabilities. As earlier observed, the manner in which we have organized our intelligence system to confront the challenges posed by large nation–states is not as fully applicable and useful to the challenges we now confront from terrorist organizations. We must continue to improve on our collection disciplines, but especially engaging them in more of a "jointness" with the Human Intelligence discipline. Another area that must be substantially improved is in our intelligence analysis training. We should not rely or depend on our intelligence community to share this burden by itself. Our universities can play a role in offering assistance in the preparation of intelligence analysts as well as in the development and refinement of additional analytical tools. This chapter has provided a framework and described our nation's intelligence processing capability. Hopefully, it will provide insight as to how we can continue to gather information to protect our nation from the threats we will encounter from terrorist organizations in the future.

The remaining chapters in this book will focus on our vulnerabilities to bioterrorism, chemical weapons, nuclear dispersal devices, agricultural terrorism and weaponization, cyber risks, and our critical infrastructure. The risks and the management of how we confront these challenges, along with the structure of our national security decisions, will be referenced within our legal system.

References

1. Lowenthal, M.M., *Intelligence from Secrets to Policy*, CQ Press: A Division of Congressional Quarterly Inc., Washington, D.C., 2006, 175–176.
2. Donley, M.B., O'Leary, C., and Montgomery, J., Inside the White House situation room, in George, R.Z. and Kline, R.D., Eds., *Intelligence and the National Security Strategist: Enduring Issues and Challenges*. Published for the Sherman Kent Center for Intelligence Studies; National War College by National Defense University Press, Washington, D.C., 2004, 447–448.
3. Ibid., p. 448.
4. Krizan, L., *Intelligence Essentials for Everyone, Occasional Paper Number Six*, Joint Military Intelligence College, Washington, D.C., 1999, 13–14.
5. Lowenthal, M.M., *Intelligence from Secrets to Policy* pp. 89–90.
6. Lowenthal, M.M., *Intelligence from Secrets to Policy*, p. 91.
7. Aid, M.M., The time of troubles: the U.S. National Security Agency in the 21st century, in George, R.Z. and Kline, R.D., Eds., *Intelligence and the National Security Strategist: Enduring Issues and Challenges.* Published for the Sherman Kent Center for Intelligence Studies; National War College by National Defense University Press, Washington, D.C., 2004, 195.
8. Lowenthal, M.M., *Intelligence from Secrets to Policy*, p. 92.
9. Lowenthal, M.M., *Intelligence from Secrets to Policy*, p. 80.
10. Goodman, G.W., Jr., Unclassified space eyes, in George, R.Z. and Kline, R.D., Eds., *Intelligence and the National Security Strategist: Enduring Issues and Challenges.* Published for the Sherman Kent Center for Intelligence Studies; National War College by National Defense University Press, Washington, D.C., 2004, 154.
11. Lowenthal, M.M., *Intelligence from Secrets to Policy*, pp. 85–86.
12. Lowenthal, M.M., *Intelligence from Secrets to Policy*, p. 80.
13. Macartney, J.D., How should we explain MASINT, in George, R.Z. and Kline, R.D., Eds., *Intelligence and the National Security Strategist: Enduring Issues and Challenges.* Published for the Sherman Kent Center for Intelligence Studies; National War College by National Defense University Press, Washington, D.C., 2004, 172.
14. Ibid., pp. 172–174.
15. Ibid. p. 175.
16. Ibid., p. 177.
17. Lowenthal, M.M., *Intelligence from Secrets to Policy*, p. 95.

18. Krizan, L., *Intelligence Essentials for Everyone*, p. 29.
19. Davis, J., Defining the analytic mission: facts, findings, forecasts, and fortunetelling, in George, R.Z. and Kline, R.D., Eds., *Intelligence and National Security Strategist: Enduring Issues and Challenges*. Published for the Sherman Kent Center for Intelligence Studies; National War College by National Defense University Press, Washington, D.C., 2004, 298.
20. Imler, N.B., Espionage in an age of change: optimizing strategic intelligence services for the future, in George, R.Z. and Kline, R.D. Eds., *Intelligence and National Security Strategist: Enduring Issues and Challenges*. Published for the Sherman Kent Center for Intelligence Studies; National War College by National Defense University Press, Washington, D.C., 2004, 221.
21. Imler, N.B., *Espionage in an Age of Change*, pp. 226–227.
22. Pillar, P.R., *Terrorism and U.S. Foreign Policy*, Brookings Institution Press, Washington, D.C., 2001, 111.
23. Lowenthal, M.M., *Intelligence from Secrets to Policy*, p. 164.
24. Lowenthal, M.M., *Intelligence from Secrets to Policy*, p. 37.
25. Krizan, L., *Intelligence Essentials for Everyone*, p. 47.

Medical Response to Chemical and Biological Terrorism

2

MICHAEL P. ALLSWEDE

Contents

No matter whether the event is terrorism or natural disaster, all roads eventually lead to a hospital for the victims.

Introduction

In the past, medical systems could be reasonably relied upon to adequately respond to a disaster event, such as a fire, bombing, or flood, through community response planning. However, new threats, such as chemical,

biological, and radiological terrorism, increase the burden on medical systems. In addition to potentially large volumes of victims, medical systems must also be responsible for *recognition* of insidious disease or unfamiliar syndromes. Recognition of unusual disease or chemical exposure must occur prior to rendering care for these victims. If unrecognized, these infectious and toxic threats may place the medical system and its personnel at risk by contamination of the facility. The need to detect, respond, and protect simultaneously creates a unique burden on health-care systems that is difficult to address in this modern era of terrorism. Despite the need to take on added responsibilities for community safety, medical systems today face financial, regulatory, and liability pressures that are significant and will impede their function in time of national crisis. This chapter will discuss specific problems and potential solutions for medical systems in the modern era of chemical and biological terrorism.

Medical systems are a vitally important, but neglected component of the nation's homeland defense strategy. Though a great deal of money has been spent on homeland security in a variety of departments and agencies, medical systems have been mostly left out of the partnership for preparedness. There are a number of reasons why medical systems are not yet included as full and equal partners in the national preparedness architecture. First, most U.S. medical systems are not government agencies, but are independent private businesses. These businesses compete with one another in the health-care market and are not always predisposed to cooperate with one another. In addition, each medical system represents a unique organization ranging from single-proprietor clinics to major university medical centers. It is difficult, therefore, to find a single organization that represents "medical care." Lastly, there is a perception that disaster or a terrorist incident is mostly "scene" management. This is true in explosives, building collapse, hazardous materials (HAZMAT), and firearms incidents. However, if an event is a covert release of a biological or chemical weapon, the "scene" is the hospital, as recognition and management is primarily a medical function with first responders in support.

The Incident Command System (ICS), which provides the guidelines used to respond to catastrophic events, endeavors to blend the capabilities of different local services and numerous local jurisdictions into an integrated team. The ICS scales upward toward the National Incident Management System (NIMS), which integrates multiple state and federal agencies to coordinate the overall national response to major disasters and other incidents of national significance. With few exceptions, these multiple agencies do not actually render definitive care to victims, medical systems do. In events in which medical systems detect and are the primary responders, the ICS system may have difficulty due to the variety of medical systems with which to integrate and the business nature of their organizations. ICS systems are unfamiliar to most medical practitioners and medical personnel and they

may have difficulty accepting ICS authority about medical matters. An example may be in the ICS designation of a facility as a "contaminated" hospital, which may have severe financial repercussions on the business of that facility. Whether people will choose to go to have their future care at the "smallpox hospital" is a significant concern for medical systems to consider.

A key disability for organization of medical systems with homeland security efforts is the lack of an overarching national organization of medical systems that is specifically responsible for defining the role and creating the capacity. In addition — and unlike police or fire departments, many, if not all, are designed to have extra capacity available if needed — medical systems are designed for maximum efficiency. Finally, because most cash inflows to medical systems consist of reimbursement for medical care and very little if any financial support for preparedness planning is available, any training drills or exercises, equipment, or personnel costs related to disaster training must be paid for from the medical system's own capital or operating funds. Diverting patient revenues that otherwise could be directed to hiring more nurses or adding specialty services in favor of creating nonrevenue-generating civic "surge" capacity is a significant ethical question. No other civilian private business is expected to be such a central part of community response for free.

Quantifying Medical System Response to the Threat

The threat of chemical–biological weapons creates situations where recognition and response must occur simultaneously; therefore, information collection, analysis, decision support, needed medications, and rapid surge capacity must rapidly and accurately occur for the event to be characterized and the victims saved. Chemical and biological events are recognized by the symptoms that they produce in victims, which must be discriminated from the background of normal disease. There are hundreds of potential biological weapons and toxins and thousands of chemicals that may be used for terrorist purposes. In a covert or unannounced attack, the recognition of chemical and biological terrorism will likely start with ill victims, the medical system is the initial data collector and analyzer for disease recognition. The anthrax events of 2001 and 2002 were initially recognized within the medical system,[1] as was West Nile encephalitis,[2] as was Hantavirus Pulmonary Syndrome.[3] In each of these events, detection of the disease was medical and the initial determination of the event as bioterrorism or not was based on medical judgment.

Terrorism, however, is fundamentally different from infectious disease outbreaks because it is under the willful control of a malevolent individual. The manipulation of a disease or toxic chemical allows the attacker to pick targets, repeat attacks, and alter strategies at will. The best medical and public

health management of a disease or toxicological event cannot stop the next attack. Only interdiction can stop biological or chemical terrorism. Despite these realities, the lead law enforcement agency, the Federal Bureau of Investigation (FBI), and the overall manager of the event, the Department of Homeland Security, have a rather informal connection to the medical community. Formal connections do exist between the FBI and various public health agencies. Public health[4] agencies are the designated organizations responsible for managing infectious disease or toxic threats to the populace. Public health departments, however, are neither law enforcement agencies nor health-care providers for most people. Epidemic investigation, quarantine, and preventative measures, such as prophylaxis and vaccination, are the primary mission of most public health departments within the U.S. Recent events of bioterrorism and emerging disease have strained the existing system, often to its limits.[5] The reason is that, like medical systems, public health agencies are generally not funded or trained to be emergency response agencies. It is also important to understand that "public health" refers to a patchwork of municipal, county, state, and federal agencies and departments that are of differing structure and capability. The connection of medical systems to this patchwork quilt of public health authorities leaves significant questions of authority and information flow, and renders a highly variable medical public health structure throughout the U.S.

Though the FBI is the designated lead federal agency to investigate and determine the criminal aspects of bioterrorism, and clinical medical providers are the professionals that primarily see the victims of terrorism, there exists very little formal connection between the FBI and clinical medicine. The result of these variable but not integrated systems of authority, can be expected to produce parallel criminal, health care, and epidemiological investigations of the same event. Separate but incomplete investigations are not a prudent strategy.[6] There are several reasons for this lack of integration. Medical privacy and public safety concerns are common when the investigations of crimes involve medical evidence. Without forward-looking policies and processes, issues of privacy[7] and national security will collide when medical events are converted to criminal investigations and issues of national security. Neither medical privacy nor public safety will be supported by this organizational flaw.

To improve the ability of medical systems to do their part in chemical and biological terrorism detection and response, a series of key questions should be addressed. These questions are:

- How should an event of chemical or biological terrorism be detected?
- What are the resources needed to contend with the event?
- How should medical systems prepare for terrorism?
- How should an event of chemical or biological terrorism be reported?

- What safeguards are there for privacy?
- How should the event be investigated?
- How can the national security be maintained and improved?

The following sections will develop these seven questions and suggest methods of rational integration of the medical community in the management of terrorism. Specific recommendations will be made for application and usage by the reader.

How Should an Event of Chemical or Biological Terrorism Be Detected?

Chemical Terrorism

Chemical terrorism refers to the use of toxic chemicals to disrupt normal functions and to sicken or kill victims within the zone of release. Chemical weapon attacks differ from chemical spills by the intent of the terrorist, the use of dissemination devices, and the choice of chemical for maximum impact. There are thousands of available toxic industrial chemicals (TICs) that are toxic to man, but the common "war agents" are:

- Organophosphate nerve agents, such as Sarin
- Vesicants, such as mustard gas
- Chemical asphyxiates, such as cyanide
- Pulmonary irritants, such as phosgene
- Riot control agents, such as tear gas

The chemical war agents as well as many toxic chemicals have distinctive odors or produce distinctive physiologic signs and symptoms in exposed victims. While there are many instances of war agents being used during World War I and in various conflicts since, the most instructive example for U.S. preparedness is the use of Sarin by the Aum Shinrikyo in Japan in 1994 and again in 1995. The Sarin attack in Matsumoto in 1994 and the Tokyo subway in 1995 each created a significant influx of victims prior to accurate information from the scene. Most of the victims were minimally exposed and needed no medical treatment to survive, but some required hospitalizations and aggressive care. Due to a general lack of familiarity with nerve agents, this care was either delayed or insufficiently aggressive until physicians were educated during the ongoing crisis. In addition, up to 23% of hospital staff was contaminated by the victims with Sarin and became incapacitated.[8]

Should an organophosphate nerve agent be released into a U.S. city, the U.S. medical system can be expected to respond with similar results. Cholinergic symptoms, such as those produced by Sarin, are unusual in the day-to-day practice of medicine. Without some "just in time" information or readily available references, it is likely that delays in recognition would occur.

Delays in diagnosis would cascade similar delays in protective measures and in decontamination. These delays will contaminate the facility, the staff, and the emergency patients who are ill, but not primary victims.

To be designated as a fully functional emergency department, U.S. medical facilities must possess a decontamination room. The intent of this room is to wash a contaminated victim and to prevent secondary contamination of the medical staff and facility; however, the state or readiness of most medical personnel with respect to decontamination and proper use of personal protective equipment is suspect. In most facilities, the decontamination room will typically service a single victim at a time, which is sufficient for small volume chemical spills and accidents. The release of a war agent, however, may produce hundreds or thousands of victims, rendering the single service room insufficient. For these reasons, most experts would agree that the medical facilities most accessible to the public would be overrun by a chemical weapon release on a populated venue.

Chemical testing devices do exist to detect various chemical weapons and can be used by staff familiar with the testing devices. The conduct of the test and interpretation of the results are outside the typical scope of practice for most medical facilities and, therefore, may cause confusion due to the cross reactivity of many common compounds with chemical weapons detection systems. In addition, there is no simple test to differentiate the thousands of toxic industrial chemicals (TICs) from one another. Lastly, there is generally an inverse relationship between speed and accuracy in testing materials. While reference laboratory testing may be important for evidentiary purposes, rapid patient symptom recognition and decision-support information geared to the probable agent class are most efficient.

> Recommendation: U.S. medical facilities must expand training of emergency personnel to include recognition, protection, decontamination, triage, and treatment of chemical weapons syndromes.

Biological Terrorism

Biological weapons are used for by the intentional spread of disease-causing microbes and toxins. They produce disease that may be nondescript as in the initial flu-like illness associated with anthrax, or they may cause clearly abnormal disease presentations like the descending paralysis associated with botulinum toxicity. From the medical detection perspective, there are three basic characteristics available to the clinician to differentiate bioterrorism-associated disease from background illness. The three characteristics are:

- Detecting case clusters
- Syndrome recognition
- Abnormal test results/unusual disease presentations

Detecting a case cluster refers to the observation of nonspecific disease occurring in a greater than expected frequency among persons of a given demographic. Terrorists are associated with victims by ideological disagreements or by the victim's attendance at a targeted venue. Because clinicians are focused on patient care, not observation of trends, the ability to detect case clusters should be augmented by using some form of syndromic surveillance. Syndromic surveillance can be as simple as reviewing the daily log of patients seen or as complex as dedicated computer systems.[9] Should there be an anticipated threat to a segment of the population, involving medical systems prospectively to survey for potential victims will likely speed recognition.

Syndromic detection strategies are somewhat limited for a number of reasons. Among the more significant limitations of syndromic surveillance include: the data monitored are nonspecific and may be de-identified due to privacy concerns. Individuals who are ill, but who do not seek medical attention or seek alternative treatments are not monitored. Natural variations in disease presentation are a challenge as other factors influence disease occurrence, such as ill family members and friends, communal living, and mass transit. Lastly, syndromic detection systems only compare the number of ill individuals' relative historical averages, not the total population served. Changes in population will change the number of ill individuals presenting to health-care facilities. Thus, case clusters detection must also have some form of directed clinical investigations to support or refute the trends in syndromic data. That stated, once a given syndrome is detected, syndromic surveillance processes can greatly enhance the characterization of an infectious outbreak. Case findings and the scale of the event are key components of response and an electronic syndromic data system can be a significant aid to these tasks.

Disease recognition refers either to definitive case presentations or unusually severe disease that warrants further workup. For example, the first case of anthrax in 2001, Bob Stevens of American Media[10] presented with unusually severe meningitis that was later proven to be anthrax. The detection of these cases rests on alert and astute clinicians, with appropriate laboratory backup. Because many bioterrorism diseases are also naturally occurring diseases, the detection of an unusual syndrome should initiate a coordinated epidemiological and law enforcement investigation. The recovery of bioterrorism-related microbes from routine culture or the presentation of unusual test findings is the last method of medical detection. The culture of *Yersinia pestis,* the causative bacteria of the plague, from the lungs of a person with pneumonia would be an indicator that the pneumonia may be evidence of bioterrorism. Because plague can also occur naturally in rare cases,[11] bioterrorism must be considered and investigated along with the infectious nature of the disease. The detection of a bioterrorism-related microbe should initiate a coordinated epidemiological and law enforcement investigation.[12]

The clinical detection of bioterrorism is clearly imperfect and requires a number of seldom-used associations.[13] It should be noted that the role of law enforcement intelligence may be significant in determining the proper response to a worrisome medical anomaly that has yet to be characterized. Knowledge about given targets or likely attack scenarios in association with medical anomalies can be used to guide crisis decisions. Intelligence from law enforcement can potentially identify likely agents, likely target demographics, likely targets and venues of attack, and likely time frames for an attack to occur. Combining law enforcement intelligence with clinical investigations is probably the strongest detection-support strategy for the detection of bioterrorism.

> Recommendation: The U.S. medical system should develop active interfaces between public health and law enforcement to speed recognition, and improve accuracy of bioterrorism detection.

What Are the Resources Needed to Contend with the Event?

Chemical Terrorism

One of the greater challenges of a medical facility in responding to a chemical weapon attack is the prevention of contamination. It is likely that the initial victims of a chemical weapon attack will present without warning or scene information and potentially contaminate the medical facility. Thus, medical facilities must be able to respond by limiting access, enforcing decontamination, and surety testing those victims admitted to the facility. By limiting access, a facility may opt to initially deny entry to the contaminated victims until the facility can be configured for decontamination. This response may seem a bit irresponsible, but it is a reasonable option. The medical facility has an obligation to its staff and existing patients not to contaminate them. The victims presenting early from a scene are largely those individuals who are minimally exposed and do not need extrication of scene resuscitation. In many cases, the treatment for minimally exposed chemical casualties is fresh air. Lastly, by allowing staff and the facility to become contaminated, medical resources are removed and victims are added.

Once properly configured, the medical facility should decontaminate the victims with surety testing. Surety testing refers to the assurance of complete decontamination and the absence of any chemical residue. Gaseous or vapor exposures cause minimal exterior contamination and are most efficiently decontaminated by disrobing the individual of their exterior garments. Liquid or solid chemical exposure requires more significant cleansing of the skin surfaces and may be related to more significant exposures. Given the large number of potential victims, significant thought must be given to the ability to engage mass decontamination. Some strategies include: augmentation of hospital capacity by local hazardous material teams, augmentation of hospital

capacity by purchasing additional tents or other structures, and making physical changes to the medical facility entrance to ensure no contaminated victim may enter inadvertently. Given the potential deployment of hazardous materials teams during a crisis, the medical facility should develop larger volume endogenous decontamination capability.

> Recommendation: U.S. medical facilities must improve decontamination facilities to accommodate larger numbers of victims, limit entry to only those who are ill, and provide surety testing for workplace safety.

Once victims are decontaminated, the next challenge is to triage and deliver medical treatment. An open air gaseous or vapor exposure causes a larger number of minimally exposed victims relative to severely exposed victims due to the dilution of the contaminated air in three dimensions. In contrast, the same amount of contamination within a structure could produce a larger number of severe exposures due to the containment of the contaminated air and its recirculation. A structural contamination can be expected to generate more significant exposures than an open air venue due to the containment and recirculation of the toxin by the building's heating ventilation and air conditioning system, as well as the movement of structure inhabitants and elevators.

There are a series of challenges to treating victims of chemical exposure. Some chemical weapons have specific antidotes, such as organophosphate nerve agents and cyanide. These antidotes are "narrow" in their spectrum as they are not useful in other sorts of chemical exposures. Many chemical weapon victims require only supportive measures, such as ventilator support for pulmonary irritants. If a hospital stocks antidotal medications for chemical weapons, it is difficult to stock all of the potential antidotes in sufficient volume and in a readily available form to reverse rapidly acting toxins. Most incidents involving chemical exposure of this sort are small volume industrial or home accidents. Urban emergency medical service (EMS) systems typically will carry a small amount of antidotes intended for use by the EMS crew in the event of inadvertent exposure. Civic stockpiles of antidotes for victims are often placed in central locations for ease of inventory and security. This "stockpile strategy" emphasizes EMS provider care and administrative maintenance, but does not maximize victim care. To rapidly deliver needed antidotes to large numbers of victims requires predeployment. Predeployment is possible if a threat is known and communicated to the medical system. Not all threats can be anticipated, however. For this reason, a "disseminated strategy" is employed by the U.S. military in which every soldier or sailor carries a potentially life-saving dosage of medication. This strategy has also been applied to civilian response in Israel with rather minimal health effects.[14] The correct strategy depends upon

anticipating the size, frequency, and toxicity of the chemical attack. Large, highly toxic events favor a disseminated strategy.

Regardless of predeployment strategy, rapidly available education must also be provided to the treating individual as antidotes are seldom-used medications, or medications used in doses different from their common usage. For these reasons, antidote stockpiles should be accompanied with decision-support material that can be easily disseminated. The following example is taken from the RaPiD-T Program.[15] RaPiD-T is the educational and management tool for the City of Pittsburgh EMS and the University of Pittsburgh Medical Center.

> Recommendation: Antidotal stockpiles and associated decision-support tools be readily available to medical and EMS systems preparing for chemical terrorism. Consideration should be given to disseminated antidote strategy with educational material for higher severity and frequency threat areas.

Selected Portion of RaPiD-T Manual

Organophosphate Nerve Poisons

Recognition: **Vapor** **Liquid**
Miosis Fasciculations, sweating

Protection: Level C minimum

Decontamination: 0.5% hypochlorite

Triage: Based upon symptom complex as depicted below

Severity	Vapor-onset in 1-2 minutes	Liquid-onset in several minutes
Mild	Miosis, Rhinorrhea, Dim Vision,	Local fasciculations, Local sweating
Moderate	All above with Nausea, Vomiting	All above with Nausea, Vomiting
Severe	Convulsions, Apnea, Death	Convulsions, Apnea, Death

Treatment: Based upon triage category as depicted below

Severity	Vapor	Liquid
Mild	Observation only	2mg atropine, 600mg 2-PAM, Observation
Moderate	2 mg atropine, 600 mg 2-PAM, Observation	2-4 mg atropine, 600-1200 mg 20PAM Observation
Severe	6 mg atropine, 1800 mg 2-PAM, 10 mg Diazepam	6 mg atropine, 1800 mg 2-PAM, 10 mg, Diazepam

The now infamous Sarin gas belongs to the group of super toxic organophosphate compounds, termed "nerve agents". Included in this group are

the following compounds: Tabun (designated GA), Sarin (designated GB), Soman (designated GD), and VX. The nerve agent compounds are odorless and tasteless, and are readily absorbed through the skin, or by inhalation. They are highly toxic by either route. When inhaled, toxicity is determined by a concentration time product in which the milligram concentration per cubic meter is multiplied by the time of contact. Sarin, for example, has a LCt_{50} of 100 mg-min/m^3. This means that 50% mortality is achieved when adult subjects are exposed to 100 mg total exposure. It is important to recognize that the cumulative dose may be achieved by inspiring a low concentration for a longer period of time. It is this feature of nerve agent toxicity that mandates decontamination. In the Tokyo example, a significant number of health personnel were overcome by breathing the vapor contained on victims clothing. Simply disrobing the patients, and setting up a triage post in open air would have alleviated a number of casualties.

Nerve agents are liquids at room temperature and have relatively low vapor pressures. Sarin (GB) is the most volatile at 2 mm. Hg, which is similar to water's vapor pressure. The photo to the left demonstrates the physical appearance of common chemical weapons. Note that the compound is an oily brownish liquid. When heated, as in the Matsumoto incident, Sarin will come out of solution at a faster rate and produce a highly toxic concentration of agent. The nerve agents are also about 4 times heavier than air so they collect in low-lying areas. The Tokyo subway attack utilized this property by allowing the unheated vapor to accumulate in the lower reaches of the subway with obvious lethal consequences. The other "G" nerve agents are less volatile than Sarin and the agent VX is only considered a contact risk. It is important to note that some of the victims of the Subway attack included individuals who attempted to pick up the packets of agent and sustained a subsequent liquid exposure. Liquid exposure presents its own problems in management as the agent VX could be laid down at a location prior to occupation by the intended victims. An understanding of the effect the route of exposure has on the presentation of the clinical toxidrome is critical to the management of the victim.

The toxic effects of nerve agent compounds are achieved through the inhibition of acetylcholinesterase, and the subsequent over-stimulation of the acetylcholine receptor. Muscarinic, Nicotinic, and CNS subtypes of receptors are affected. Muscarinic receptors, when stimulated, increase the activity of salivary glands, lacrimal glands, smooth muscle, and pupillary constriction (miosis). The muscarinic syndrome is best remembered by the SLUDGE acronym; S (salivation), L (lacrimation), U (urination), D (diarrhea/diaphoresis), G (general weakness), E (emesis). Of specific concern for medical personnel is the effect upon bronchial smooth muscle and bronchial mucous glands. Nicotinic receptors are found primarily on skeletal muscle as well as certain ganglia, most significantly, the adrenal medulla. Stimulation of nicotinic receptors results in fasciculation and ultimate paralysis of the affected

skeletal muscle. The CNS effects of these compounds are sedation, seizure, apnea, and ultimate death.

Biological Terrorism

If one were to believe the media, bioterrorism consists only of a smallpox or anthrax release in a stadium resulting in thousands and hundreds of thousands of dead and dying.[16] While these scenarios are motivating for certain, there has not been a single instance of that level of attack succeeding,[17] though it has been attempted. The anthrax events of latter 2001, for example, were a small volume, tightly targeted attack more resembling assassination attempts than a population-based attack.[18] Although initially lumped together with Al-Qaeda, the anthrax terrorist actually provided the opportunity to prevent deaths from anthrax by taking the detection problem away from authorities.[19] Twenty-two individuals developed some form of anthrax, five died, but the number of treated individuals is estimated to be 10,000 to 20,000.[20] Consider for a moment, how much more difficult for health-care systems the fall/winter of 2001 would have been had the attack been larger or anonymous. Who was exposed? Where were they exposed? Who needs treatment? Which flu-like syndrome is anthrax and which is not? The inability to answer these questions, the disorganization of response, and the resultant panic would have caused significantly more social problems and potentially more deaths.

In responding to bioterrorism, the scale of the attack and the time of detection of the attack are critical components. For example, the mortality of those who acted on the anthrax exposure at the time of the receipt of the letter had a 0% death rate from anthrax, but those who waited for a hospital diagnosis had a 70% death rate.[21] As America invests in detection technology with better intelligence analysis,[22] biosensors,[23] and syndromic detection,[24] medical interventions may change and survivorship increased as bioterrorism-related disease is detected earlier. Detection of a bioterrorism attack may occur prior to release (through law enforcement and intelligence services), at the time of release (as in fall/winter 2001), at the time of nonspecific symptom occurrence in the exposed population (by a syndromic detection system), at the time of hospital diagnosis of ill individuals, or at the time of deaths/epidemic occurrence. Unfortunately, prior to these events, detection of unusual disease events occurred only *after* deaths of the intended victims, if at all.[25]

The potential stages in which a disease may be detected are represented by the following timeline.

- *Prerelease* X
- *Release* X
- *Symptom Occurrence* X
- *Illness Occurrence* X
- *Deaths/Epidemic* X

The stage at which disease detection occurs will alter the possible actions of the hospital or health-care system. Prophylaxis, for example, would be of primary importance early in the timeline, but wane in its effectiveness later in the timeline of an individual victim.

The size of a quarantine effort would also markedly change when the later on the timeline one detects the bioterrorism event, as more secondary victims could potentially be exposed. The critical concept is that medical response varies with the timeline and scale that an event may be detected.

A model for quantification of a health-care system response to bioterrorism should include both scalar effects and timeline of detection. The critical actions and priorities of a hospital or medical system will be primarily effected by these two assessments, as much as pathogen identification. A representative matrix, termed "the Pittsburgh Matrix"[26] after the location of its development, has been developed to characterize medical response to bioterrorism combining these two variables as seen below.

Pittsburgh Matrix

Above all capacity					
Augmented capacity					
Surge capacity					
Current capacity					
	Prerelease	Release	Symptom occurrence	Illness occurrence	Epidemic

"Current capacity" would be defined by the number of victims that a hospital or system could absorb without altering normal operations. "Surge capacity" refers to maximal crisis mode capacity. "Augmented capacity" refers to capacity derived with external resources and "Above all capacity" refers to "battlefield" triage in which maximum good is done for the maximum number.

As a hospital or health system adds resources in terms of better organization and increased capacity, a given numerical scenario will be plotted successively lower on the vertical access. Early recognition and good early decision making can move a given scenario from right to left on the horizontal access. Poor decision making and inadequate planning will move the scenario management to the upper right. Mortality can be expected to increase by moving up and right on the matrix.

Specific resources apply well in certain cells and for certain pathogens but not in others. For example, antibiotic stockpiling of oral antibiotics for anthrax is useful in the Release and Symptom occurrence columns, but loses its effectiveness after severe illness occurs. Likewise, education of physicians to recognize bioterrorism-related diseases is only effective after the disease is recognizable in the illness column.

The confusion of fall/winter 2001 can largely be explained by the supposition on the part of most leaders that we were preparing for a "Deaths/ Epidemic Triage of Resources" problem when in fact we were in the "Release-Current Capacity" cell. As a decision-support tool, each box can be constructed to contain critical decision and resources identified along with agent specific recommendations.

Hospitals do not take care of matrix cells, they take care of real patients with real infections. Pathogens have a multitude of characteristics that are of medical relevance, but from the planning and response perspective, the three primary concerns are:

1. *Communicability/quarantine needs*: This agent characteristic defines quarantine and isolation needs not only for patients but also for exposed but asymptomatic individuals. This is a critical characteristic, as quarantine will be a difficult civic–medical effort.
2. *Effectiveness of medical treatment*: Some bioterrorism diseases are not amenable to treatment, others have unproven treatments, and others have highly effective treatments. The urgency of pharmaceutical intervention and staff can be determined by this analysis. Example: Botulism treatment must be given prior to symptom onset to be effective.
3. *Availability of medical treatment*: Certain bioterrorism agents have obscure treatments available only in small amounts. Examples may be antitoxins, heavy metal chelators, or vaccines. The availability of a given treatment may potentially change management strategy from treatment to palliation.

Using a tool like the Pittsburgh Matrix, an accurate assessment of the primary difficulties in managing communicability, effectiveness of treatments, and availability supplies and space can be mapped to matrix cells by the system preparing for the event. By identifying gaps or shortfalls within a cell, improving preparedness on the local level is possible. Armed with these matrices, it is possible for a hospital or medical system to rapidly identify critical needs, estimate casualties, as well as predict future needs as time progresses. By combining mortality expected within each cell, the value in terms of lives saved per dollar spent can be estimated for new detection technologies, such as syndromic surveillance technology or deploying bioaerosol detectors in various scenarios involving real agents and real events. The value of pre-emptive law enforcement interdiction, a vaccination program, or a new medication can also be evaluated in similar fashion.

> Recommendation: Resource planning must be coordinated with an overall understanding of bioterrorism in both timeline of detection and scale of response. Resource planning for bioterrorism must consist of a "defense in depth" with multiple options and strategies for each stage of the epidemic.

How Should Medical Systems Prepare for Terrorism?

An old adage in medicine is "the eye does not see what the mind does not know." The purpose of educating the mind is to recognize disease, but most chemical and biological weapons agents are not part of a medical education. There is a need for an integrated, sustainable, comprehensive educational process for clinical practitioners in addition to providing them with new resources. Medical facilities must train their personnel on how to use new decontamination systems, access stockpiles of medications, and treat unfamiliar illness. New skills are needed.

Disaster drills have been used in the past to practice mass care, but that care is largely within the normal practice of medicine. While there are a number of good training courses available on chemical and biological weapons, how personnel adapt that knowledge and apply it in practice remains a challenge. In times of crisis, additional personnel are added and more work is accomplished. Training these personnel to adapt to terrorist threats is difficult because hospitals function like a ship underway, with every person having an assigned job. To train for disaster, a hospital cannot stop its daily work. Disaster training and response capacity are simply not funded by private, municipal, county, state, or federal authorities. When confronted with the need for additional drilling, some hospitals do choose to spend money on additional staffing for drill players. While this strategy allows unencumbered drill play, it is expensive and, for many hospitals, training a shift at a time is inefficient use of money, time, and personnel. Other hospitals ask for volunteers to avoid the expense of drill pay. While volunteerism is laudable, it only trains those who self-select for training. This lack of a comprehensive approach to training may show the hospital disaster function at its best, but it does not give an accurate picture of how the hospital would function under normal circumstances. Still other hospitals refuse to play in a disaster drill as they are focused and paid to do their health-care jobs, not to treat moulage patients.

No matter what skills may be taught during a disaster drill, they will degrade in time if not used. A key component to responding to high consequence but low frequency events is practice. In the case of caring for victims of hazardous materials events, rendering care in protective gear is an entirely new experience for many. In addition, heat stress, claustrophobia, and attenuation of the senses are just a few challenges of working with personal protective gear. Though blood and body fluid infection control methods are common practice in the U.S., management of airborne pathogens is not. These skills must be reinforced if the hospital is to respond efficiently on the day of the event.

> Recommendation: Develop a sustainable educational program focused not only on chemical and biological weapons, but also application of that knowledge to hospital operations. Develop a sustainable skill acquisition program focused on training unique new skill sets for response to chemical and biological weapons.

A model training program would be sustainable, focused upon individual jobs, contain skill acquisition and knowledge acquisition strategies, and have associated knowledge retention tools. Fortunately, most medical practitioners have periodic continuing medical educational (CME) requirements. By adding new skills and knowledge to the ongoing CME process, all can benefit from the training, not just those who participate in the drills. A model of skill acquisition taken from military training programs is the FAPV or "familiarize," "acquire," "practice," and "validate" sequence. This is similar to the "crawl," walk," and "run" euphemism that often characterizes training efforts.

Familiarization with new knowledge and skills should maximize ease of access for the student. Smaller units of knowledge, testing, and evaluation that one could accomplish during downtime or on a training day may work better than a larger and more comprehensive program. Distance learning is ideal for this sort of knowledge dissemination. Acquisition of skills requires an experiential component. A "training room" experience in which the student wears protective garments and uses equipment is the goal. An example of a training room experience is the cardiopulmonary resuscitation training in which a mannequin is used to acquire skills. Medical simulation is in its early development, but holds significant promise in this area. An opportunity to practice the new knowledge and skills can be created by standard drilling. Validation of response can be assessed in real events or by using unannounced drills. By developing an educational strategy for new knowledge and skill acquisition and by integrating with existing educational programs, the entire staff performance cannot only be improved, it can also be measured.

> Recommendation: Integrate new training methodologies with existing educational programming to create a sustainable and general improvement in personal response to chemical or biological weapons response.

Finally, most U.S. medical facilities are private businesses that employ private citizens for medical jobs. In response to a chemical or biological event, personnel of a medical facility may become alarmed by caring for potentially hazardous patients. Also, should the event alarm the community, one's concerns may be with one's dependents. The choice between professional duty, personal safety, and responsibility to dependents is a difficult one. It is important that some institutional guidance be given to those personnel who would be in that potential position. A family emergency plan is the base document that should be completed by the staff. In addition, some provision for caring

for dependents must be made by the institution should a valuable staff member be equally needed at home. In a perfect situation, a sense of duty, purpose, and common bond should be instilled in employees to complete the medical mission, despite its challenges. "Psychological immunization" of the workforce by outreach and motivational programming is needed to mitigate the natural response to crisis.

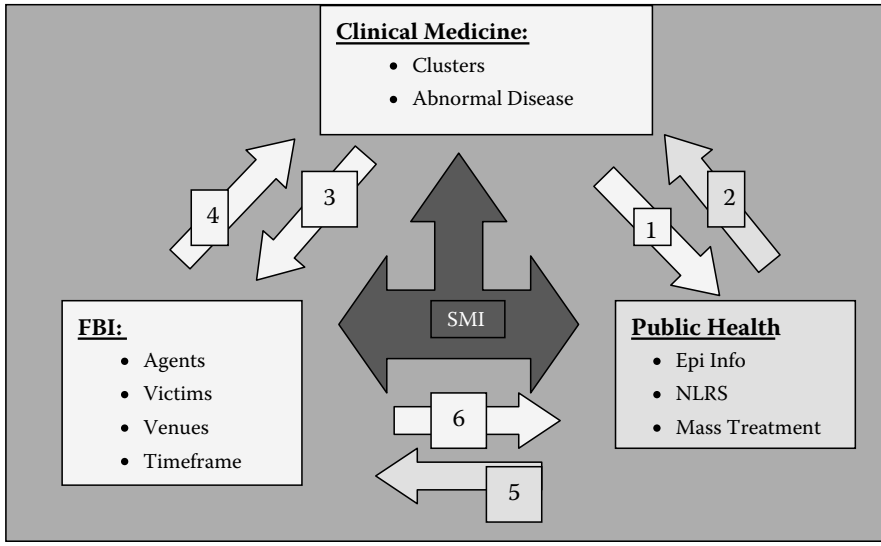
> Recommendation: Medical facilities engage employees in discussions of needs and develop programs for employee support and motivation.

How Should an Event of Chemical or Biological Terrorism Be Reported?

Should an anomalous medical event occur and be recognized, the specifics and parameters of the event should be reported to the managing authorities. Specific characteristics of bioterrorism that should be scrutinized are:

1. Medical inputs, such as:
   (a) Clusters of demographics within ill populations
   (b) Clusters of a nonspecific disease that can be traced to a point of exposure
   (c) Disease recognition of bioterrorism pathogens
   (d) Abnormal laboratory or testing results
2. Law enforcement inputs would include
   (a) Likely victims as determined by annunciated threats
   (b) Likely venues as determined by threat analysis
   (c) Likely timelines as determined by surveillance techniques
   (d) Likely agents as determined by threat analysis
3. Public health inputs would include
   (a) Syndromic detection systems to include active and passive data collection
   (b) The National Laboratory Response System (NLRS)

As previously stated, the FBI has jurisdiction of the law enforcement investigation, the public health has responsibility for the epidemiologic investigation, and the medical system has responsibility to care for the victims. Criminal and epidemiological investigations depend on medical information. There are many impediments to communication including medical privacy concerns, "need to know" thresholds for sharing intelligence, and institutional rivalry. The specific communication can be characterized by the diagram below.



Legend:
1. Normal disease reporting
2. Public health advisement
3. Law enforcement reporting
4. Law enforcement investigations
5-6. Interagency communication

Normal disease reporting is best characterized by the normal reporting of specific diseases to the public health authority by clinicians. Most of these reports consist of culture reports or definitive clinical diagnosis of disease submitted by clinicians to local public health authorities. The reporting system is often by the mail and events are recorded, collected, and collated by hand. This laborious process is reasonable for nonserious disease or clearly recognizable disease, but may prove disastrously slow in times of infectious disease crisis.[27] Obtaining relevant, timely information has been an identified problem in most emerging diseases, most recently severe acute respiratory syndrome (SARS).

Public health advisement in times of crisis has been somewhat problematic as there are multiple public health authorities that must coordinate to send a uniform message. Public health authority is highly irregular across the U.S. and manifests as city departments of public health, county department of public health, state departments of public health, and various federal agencies to include the Centers for Disease Control (CDC), the Surgeon General, and the Office of Emergency Preparedness of the Health and Human Services Department.

Because of the irregular reporting of clinical disease, a certain level of ignorance of bioterrorism detection criteria and the irregular public health authority, bioterrorism and emerging disease detection and decision making is not

standardized. For example, the agencies and organizations involved in the U.S. Capitol anthrax response included: U.S. Capital Police, Architect of the U.S. Capitol, Sergeant at Arms, U.S. Senate, Office of the Attending Physician of the U.S. Senate, FBI, EPA, CDC, DARPA, HHS, NIOSH, USAMRIID, FEMA, the U.S. Coast Guard, U.S. Marines CBIRF, District of Columbia Department of Health, Office of the Mayor of District of Columbia, U.S. Army, U.S. Navy, and U.S. Air Force.[28]

Further, a casual review of recent bioterrorism and emerging infectious disease events shows that the most often used method of communication is the media. While commendable, the use of the media prior to information sharing by the major stakeholders in management of an infectious disease crisis can be expected to increase confusion, erode privacy, and alarm the public.

> Recommendation: The FBI, public health, and clinical medicine must improve the communication and decision-making systems to evaluate and respond to potential infectious events. The FBI, public health, and clinical medicine define and familiarize their organizations with the specific information they must contribute to decision making in a bioterrorism crisis.

What Safeguards Are There for Privacy?

Reporting of relevant medical information to the FBI is, at present, not governed by any statute or regulation. Instead, there are conflicting regulations that both mandate the reporting of infectious threats to the community and protecting patient privacy.[29] Clinical medicine is restrained in the sharing of clinical data by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA was intended to guide medical systems in the routine processing of medical information, not to guide the institution through a bioterrorism crisis response. For example, HIPAA allows the sharing of health information with the FBI under subpoena. To generate a subpoena, the FBI must first generate suspicion that a bio-crime has been committed. For this, they must have a reporting structure to receive concerns of the medical community. HIPAA creates a circular logic for the investigation of bio-crimes.

In response to the need for new models of information sharing, the Model State Emergency Health Powers Act[30] (MSEHPA) has been created as a framework under which information sharing should be regulated. Specific responsibilities, authority, and constraints must be analyzed for this communication to occur for each of the stakeholders.

1. Define *responsibilities* of clinical medicine, public health, and the FBI for use and sharing of data and decision making.
2. Define *authority* of clinical medicine, public health, and the FBI for use and sharing of data and decision making.
3. Define *constraints* on clinical medicine, public health, and the FBI for use and sharing of medical and intelligence data.

Though not yet in force in the U.S. and opposed by those representing privacy concerns, this analytical construct may prove useful in designing new legislation to guide and support the sharing of information to determine the nature of infectious disease emergencies and to guide the roles and responsibilities of the managing authorities. Because of the potential impact of bioterrorism, national executive authority can be expected to be invoked should a significant crisis occur. Thresholds for application of the HIPAA, MSEHPA, and National Command Authority are not well explored and, in practice, will be strongly tied to the context of the event. A suspicious medical anomaly may be treated differently if it occurs at a highly contentious political event such as the United Nations or a political convention.

Just as important as concerns for rapid detection and public safety, are concerns for privacy of the individual. Unregulated reporting of potential bioterrorism in the media "in the public interest" by concerned officials and medical providers has caused examples of privacy violations.

The Council for Excellence in Government has explored the views of the public in this area[31] and found that the public is willing to undergo intrusions of privacy in exchange for safety if the perceived threat is high.

- Sixty-five percent of Americans are satisfied with the government's job in protecting our civil liberties.
- Only 14% of Americans trust the government to use private information appropriately.
- Fifty-six percent of Americans believe that the Patriot Act is good for America.
- Thirty-three percent of Americans believe that the Patriot Act is bad for America.
- Confidence in local emergency responders to provide homeland security is 73%.
- Confidence in the FBI to fight terrorism is 49%.
- Confidence in the federal government as a whole to provide homeland security is 13%.

These various data points indicate that while the federal authorities have funding and strategic direction responsibilities, the local assets are where the public places its trust. For this reason, it is imperative that critical information be obtained, shared, and preserved by the managing FBI, public health, and clinical medicine professionals.

> Recommendation: Structures to share information and decision-making must be developed to include public health, the FBI, and local medical leaders.

How Should the Event Be Investigated?

The investigation of chemical and bioterrorism can take two forms. First and best from the perspective of the public interest is pre-event detection. Pre-event detection refers to detection and interdiction of a bioterrorism event prior to the exposure of the target population. Pre-event detection can take the form of surveillance of terrorist cells, "hardening"[32] of target venues, and detecting small medical events that indicate manufacture or acquisition of chemical or biological agents.

Because chemical and biological weapons are toxic or infectious in minute amounts and because terrorist cells must produce, store, and transport these weapons in a clandestine manner under austere conditions, there is a potential that small spills, leaks, and inadvertent releases can be detected by monitoring culture results, unusual toxidromes, and perhaps the health of the terrorists themselves.

Like medical reporting of child abuse, spousal abuse, elder abuse, and homicidal and suicidal ideation, the reporting of unusual medical events or significant medical events in potential terrorists is in the public interest. The seminal work in this area is detailed in the Tarasoff laws[33] in which the physician has a clear and proscribed "duty to warn" the public of imminent danger. While medical findings of abuse or psychiatric cases are well defined and taught to clinicians and the reporting structures are well defined and include "whistle-blower" protections to the reporting physician, medical terrorism markers are largely unexplored. Some events that would fall into this category would include:

- Unexplained blast injury indicating bomb-making
- Unexplained toxidromes of known chemical weapons agents
- Unexplained culture results of known biological weapons agents
- Unexplained findings of radiation illness
- Unusual cluster of illness in known terrorist cells

Should a medical terrorism marker occur, it may be unnoticed by an uneducated or overly busy physician. If recognized by a concerned physician, there is no clear reporting mechanism. By following the Tarasoff defined "duty to warn," the reporting individual may have violated HIPAA statutes depending on the eventual finding of the investigation. Finally, it is also a concern that in times of national crisis physicians may unwittingly report medical information inappropriately in their zeal to guard the public interest during times of attack.

Medical markers of terrorism must also be interpreted correctly by public health officials and the FBI. It is not clear that either organization has a clear understanding of how to relate medical findings to syndromic data or intelligence data and how to share in that analysis. Should a concern be elevated due to corroborating threat information and medical or public health data, what is the most prudent course of action? Seemingly drastic responses, such

as quarantine or rapid law enforcement interdiction may be life saving if employed prior to spread of disease or execution of a planned attack. Political concerns of these decisions must be weighed not only in their medical context, but also in their political impact. Typically, elected officials are more cautious and require greater surety that a given action is correct if the action will be seen as disruptive to the electorate.

> Recommendation: Reporting of medical markers indicating terrorism must be supported by legal statutes and formalized similar to abuse reporting.

The second approach to investigation is reactive, in which an event has occurred to which the medical system must recognize and respond. Reactive investigation is primarily directed at characterizing the event and investigating its public health and criminal potential. Chemical weapons generally exert their symptoms rapidly; therefore, the detection issue is less complex as victims emerge from a venue with similar symptoms. Testing for chemical weapons is now available in most hazardous materials teams.

Biological events, particularly discrimination of bioterrorism from emerging disease is more difficult. In past events, there has typically been a significant delay between the detection of a medical anomaly and the accurate and complete characterization of the event. The New York West Nile outbreak, for example, took 6 weeks to fully characterize.[34] The interim time was fraught with confusion and misstatements. Intentional terrorism in which larger numbers of victims are exposed is considerably more difficult.

Investigations of a bioterrorism event must proceed simultaneously down several avenues. Medical investigations include the laboratory evaluation of the pathogen to include antibiotic resistance, the response of victims to treatment, the development of a "case definition" for unknown diseases, and analysis of virulence features. The medical assets needed to care for the event must be estimated and recruited. Public health must survey the event to determine the epidemiological cause, and the current size of the event. Victim location is a key for medical asset estimation and public heath has the mandate for this aspect. Further, the movement of national stockpiles, the development of mass treatment guidelines, and reference laboratory capability reside in the various levels of the public health system. The FBI must determine if the medical outbreak could be a crime and, if so, collect sufficient evidence to identify and apprehend the perpetrators and guide national command authority. Potentially this investigation may lead to national command authority action and result in military action.

The longer an event remains undetected or underappreciated, the more difficult will be the eventual investigation and response. Speed and accuracy

are essential for all investigations, but thresholds for the determination of event character and potential decisions are not well defined. A few sample questions would be:

- How is disease determined to be bioterrorism or an emerging disease?
- If two or more diseases are occurring in a population, how are they both managed?
- Can medical facilities, which are largely private businesses, be compelled to care for hazardous infectious patients by the public health authority?
- Can physicians, who are private citizens, be compelled to care for hazardous infectious patients by the public health authority?
- Can private citizens be compelled to receive medical care against their wishes by the public health authority?
- Who will manage civic unrest if infectious disease is threatening a community?
- Who determines who must be quarantined or treated, where they will be quarantined or treated, and what shall be the proper use of force for those resisting detention or treatment?

Forced quarantine has in the past resulted in civic unrest.[35] Quarantine has been inappropriately applied and has resulted in deaths.[36] Though we have yet to encounter bioterrorism challenges of this nature, imagine for a moment the anthrax events of 2001 and 2002 without the annunciated threat letter. If the anthrax terrorist used the spores to contaminate a mall or airport or stadium, these decisions may have confronted us and the resultant lack of organization[37] may have been disastrous.

> Recommendation: Structures to share information and decision-making must be developed to include public health, the FBI, local medical leaders, and political leadership to coordinate key decisions and assessments of potential terrorist events.

How Can the National Security Be Maintained and Improved?

The Japanese word for "crisis" is composed of two pictograms read vertically, one for "danger" and the other for "opportunity." This poignant combination of meanings is particularly applicable in describing the current U.S.'s preparation for bioterrorism. We all agree that we face a new danger in the potential of bioterrorism within our borders in the hands of terrorists. However, bioterrorism for all its great potential has only been responsible for five deaths in the last year. Bioterrorism represents our current national crisis, but we have been afforded the opportunity to prepare

the great resources of this nation prior to a more adept application of bioterrorism.

A key feature of our preparedness efforts must be to better understand and characterize the specific responsibilities and duties of the key stakeholders. No single entity holds the solution to terrorism challenges, but together, medical, public health, and law enforcement entities can combine to create a "defense in depth." Defense in depth refers to specific strategies employed by specific entities or organizations to mitigate specific threats. Roughly separated, the stages of defense and their attendant strategies are summarized by the following.

Pre-Event Detection and Mitigation

The FBI and intelligence agencies must be augmented in their detection mission by appropriate sharing of medical indicators of terrorism and public health surveillance for maximum effectiveness for pre-event interdiction.

Release Detection and Venue Protection

Technology-based detection systems and facility hardening should be deployed at high value venues by facility and municipal safety officers.

Symptomatic Recognition Strategy

Public health surveillance of nonspecific disease trends must be coordinated with directed medical investigations to determine at the earliest possible moment the presence of an unusual disease or syndrome. These findings must be corroborated to intelligence services and coordinated management plans developed between political leaders, the FBI, public health, and clinical medical leadership.

Disease Recognition Strategy

Training physicians to recognize unusual diseases or toxidromes must be supported and needed antidotes and medications stockpiled in accessible locations for maximal utility and life saving. Critical decisions involving mass

treatment and control of the population must be coordinated with public health, law enforcement, and political leadership.

To manage this defense in-depth strategy, a focused flexible system of local management is optimal. The components of such a system are surveillance, monitoring, reporting, synthesis/analysis, and response. Due to the highly technical nature of each component, it is not efficient to train every physician, medical facility, or public health official to a high degree of competence. It is, however, necessary to train a smaller group or team to respond to these challenges.[38] This team would respond to local threat changes and national threat levels by deploying different threat-based strategies for detection and response. Should evidence of bioterrorism occur, corroboration and analysis would be initially performed by this group and reported to the stakeholder communities. Strategy and decision making would then ensue and incorporate local, state, and federal partners as indicated. Response would be coordinated in a similar manner. Early detection, systematic preparations, and a defense in depth strategy are the key needs in developing a better system to respond to chemical and biological terrorism.

> Recommendation: Adopt a systematic approach to preparedness that is focused on increasing local competence in detection, evaluation, and response to terrorist threats.

Conclusion

If terrorism could be reasonably relied upon to produce a few victims per year, as bad as that would be, terrorism management would not be a priority. However, chemical and biological terrorism has the capability to overwhelm our resources and alter the course of this nation and potentially the world. Taking well-reasoned steps toward preparedness is the responsibility of medical systems and providers. Strengthening local medical systems will create better detection and response capability. Improved local recognition and response will make the nation safer, one community at a time.

In the development of a competent, flexible, system of making informed decisions to manage bioterrorism, the medical systems must understand its role in the recognition of these threats, the protection of its staff and patients, the need for nontraditional operations like decontamination, and finally train and guide its staff in the management of chemical and biological weapons events. This challenge takes resources and committed leadership, but it also requires the ability to characterize the new challenges and to create new organizational structure.

Similar to the intelligence community, information sharing under HIPAA has largely been governed by a "need to know" rationale. "Need to know" refers

to the general lack of information sharing unless it is determined that an individual has a need for that information. As this nation prepares for terrorist threats, information sharing will become a key for good decision making. A "need to share" paradigm should be adopted in which key bioterrorism or chemical terrorism-related information must be shared under proper controls. Shared information and decision making are in the best interest of the nation.

References

1. Bush, L.M., Abrams, B.H., Beall, A., and Johnson, C.C., Index case of fatal inhalational anthrax due to bioterrorism in the United States, *N. Engl. J. Med.* 2001.
2. New York City encephalitis outbreak of 1999.
3. Forty-two deaths of suspicious pneumonia in the Four Corners region of Southwest U.S., 1994.
4. Public health refers to municipal, county, state, and federal agencies.
5. *Bioterrorism: Public Health Response to Anthrax Incidents of 2001*, GAO-04-152, Washington, D.C., Oct. 15, 2003.
6. Ibid.
7. Health Insurance Portability and Accountability Act (HIPAA).
8. Okumura, T., Suzuki, K., Ishimatsu, S., Takasu, N., Fuiji, C., and Kohama, A., Lessons learned from the Tokyo subway Sarin attack, *Prehosp. Disast. Med.*, 15(3), s30, 2000.
9. Syndromic detection refers to the science of collecting and analyzing data to determine anomalous disease patterns. Examples would include the computer-based real-time outbreak detection system (RODS), the system in place during the Salt Lake City Winter Olympics (http://www.health.pitt.edu/ rods/) or clinical systems, such as standard public health sentinel physician networks.
10. Bush, L.M., Abrams, B.H., Beall, A., and Johnson, C.C., Index case of fatal inhalational anthrax due to bioterrorism in the United States, *N. Engl. J. Med.*, 2001.
11. Plague occurs in less than 10 cases per year in the U.S.
12. Henderson, D.A., Inglesby, T.V., and O'Toole, T., Bioterrorism: guidelines for medical and public health management, *JAMA Arch. J.*, 2002.
13. Committee on Assuring the Health of the Public in the 21st Century, Institute of Medicine, *The Future of the Public's Health in the 21st Century*, National Academy Press, Washington, D.C., 2003.
14. Amitai, Y., Almog, S., Singer, R., Hammer, R., Bentur, Y., and Danon, Y., Atropine poisoning in children during the Persian Gulf crisis: a national survey in Israel, *JAMA,* 268, 5, 1992.
15. Allswede, M., Suyama, J., and Stoy, W., RaPiD-T Program, Center for Emergency Medicine, University of Pittsburgh, in press, Prentice-Hall-Brady.

16. Example: "Dark Winter" Exercise, June 2001.
17. Example: In 1992, the Aum Shinrikyo released anthrax aerosol in downtown Tokyo for three days with no human deaths.
18. Limited dissemination, tightly targeted releases directed at famous people.
19. The letters contained an accurate description of the pathogen and suggested antibiotics that were also correct.
20. Henderson, D.A., Inglesby, T.V., and O'Toole, T., Bioterrorism: guidelines for medical and public health management, *JAMA Arch. J.*, 2002.
21. Heyman, D., Lessons from the anthrax attacks: implications for U.S. bioterrorism response, A Report on a National Forum on Biodefense, Center for Strategic Studies, Defense Threat Reduction Agency, Apr. 2002, DTRA01-02-C-0013.
22. Refers to current intelligence pooling initiatives.
23. Refers to detection of pathogenic biological aerosols.
24. Refers to detection of latent illness in the population by data mining and analysis.
25. Example: Sin Nombre virus 1992 and West Nile outbreak 2000.
26. Allswede, M. and Savitz, L., Pittsburgh Matrix Project, Agency for Healthcare Resources and Quality; Bioterrorism Toolbox Presentations, San Diego, Atlanta, 2003 and 2004.
27. Heyman, D., Lessons from the anthrax attacks: implications for U.S. bioterrorism response, *A Report on a National Forum on Biodefense*, Center for Strategic Studies, Defense Threat Reduction Agency, Apr. 2002, DTRA01-02-C-0013.
28. Ibid.
29. Fairchild, A. and Bayer, R., Ethics and the conduct of public health surveillance, *Science*, 303, 631, 2004.
30. Gostin, L.,The Model State Emergency Health Powers Act, The Center for Law and the Public's Health at Georgetown and Johns Hopkins Universities, Prepared for the CDC to assist National Governors Association, National Conference of State Legislatures, Association of State and Territorial Health Officials, and the National Association of County and City Health Officials, Dec. 2001, http://www.publichealthlaw.net/
31. The Council for Excellence in Government, *From the Home Front to the Front Lines: America Speaks Out about Homeland Security*; Mar. 2004.
32. Hardening is a term borrowed from the cold war in which the target venue is made more difficult to attack through making its heating ventilation and air conditioning systems more difficult to contaminate, creating better surveillance systems, or by placing early warning monitors in vulnerable locations.
33. Tarasoff *v.* Regents of the University of California, 17 Cal.3d 425, 1976.
34. Nash, D., Mostashari, F., Fine, A., Miller, J., O'Leary, D., Murray, K., Huang, A., Rosenberg, A., Greenberg, A., Sherman, M., Wong, S., and Layton, M.,

The outbreak of West Nile virus infection in the New York City area in 1999, 1999 West Nile Outbreak Response Working Group, *N. Engl. J. Med.,* 344 (24), 1807–1814, 2001.

35. Eidson, W., Confusion, controversy, and quarantine: the Muncie smallpox epidemic of 1893, *Indiana Mag. Hist.*, LXXXVI, 1990.
36. Markel, H., Knocking out the cholera: cholera, class, and quarantines in New York City, 1892, *Bull. Hist. Med.*, 69, 1995.
37. Heyman, D., Lessons from the anthrax attacks: implications for US bioterrorism response, *A Report on a National Forum on Biodefense*, Center for Strategic Studies, Defense Threat Reduction Agency, Apr. 2002, DTRA01-02-C-0013.
38. Joyce, G., Abarbanel, H., Block, S., Drell, S., Dyson, F., Henderson, R., Koonin, S., Lewis, N., Schwitters, R., Weinberg, P., and Williams, E., *Biodetection Architectures*, JASON JSR-02-330, Feb. 2003, The Mitre Corporation.

Agroterrorism

3

SIMON J. KENYON

Contents

> There is no terror in the bang, only in the anticipation of it.
>
> **Alfred Hitchcock**

> No one can terrorize a whole nation, unless we are all his accomplices.
>
> **Ed Murrow**

This chapter is about agricultural terrorism. I am writing from the perspective of a food animal veterinarian, perhaps more accurately described as a food systems veterinarian, who deals with animal health and the safety of food derived from animals, as part of the same job description. When we discuss acts of terrorism against either crop or animal agriculture, we are not just talking about the impact of a terrorist act on the agricultural economy, but also on the security of the food supply and the safety of food. The disruptions brought about by naturally occurring disease outbreaks, particularly in food animal species, such as cattle, sheep, and pigs, can be very large indeed, leading to disruption of the market system, movement restrictions on animals and sometimes humans, the shutting down of export markets,

and all the costs associated with bringing an outbreak under control. During the 10 years I spent as a veterinary officer in Africa and Southeast Asia, I worked on the control of epidemic diseases, such as foot and mouth disease (FMD) and rinderpest, and saw the devastation they can wreak on people's lives and livelihoods in developing countries. Epidemiological exercises and disease simulations, however, show that diseases such as FMD have the potential to cause just as great hardship and heartbreak to livestock owners in the developed world, as in Africa, and even greater economic loss. In fact, a General Accounting Office report in 2002 suggested that the cost of eradicating an FMD outbreak in the U.S. could be as high as $24 billion.[1]

The recent history of FMD and other diseases in Europe and the U.S. makes it clear that the risk of *unintentional* spread of animal and plant diseases is at least as great as the risk of *deliberate* attacks on agriculture and the food supply. The wake-up call for agriculture and the food system was not the terrorist attack on the World Trade Center in 2001, but the FMD outbreak in Britain earlier in the same year. It is not necessary to raise the specter of terrorism to justify beefing up agricultural security measures. The appearance of viruses new to the U.S., such as West Nile Virus, the recent appearance of mad cow disease in North America, outbreaks of exotic newcastle disease in poultry in California, and the possibility of a human pandemic caused by an avian influenza virus, is justification enough. Control of these diseases calls for education about their risks, for better surveillance, improved preparedness, improved diagnostic capacity, and swifter response. Preparation for natural disease events and the unintentional introduction of foreign animal diseases leads to improved preparedness for dealing with deliberate acts of terrorism.

The elevated political status of terrorism and the rhetoric of national security color our thinking on the critical issues involved in disease management. For instance, there is a tendency for the political status of terrorism to change the way we think about risk; in fact, the word "threat" is often substituted where the word "risk" would be more appropriate. Threats are to be confronted, and though from a political point of view this may be a useful idea, it does little to help in planning for disease events. Elevating all risks to the same status by referring to them as threats hinders a nuanced response to risk based on probability and potential impact. The "all hazards" approach to emergency management does not mean that all hazards have equal risk of occurring and should be confronted in the same way and with the same commitment of resources. The all hazards approach simply means that preparation is more effective if emergency management procedures are set up that can accommodate hazards of different types.

One of the consequences of focusing on terrorism as an overriding threat is a loss of perspective on the likelihood of particular agents being used for an attack. When considering preparedness for terrorist attacks, a risk assessment of the suitability of agents must be a part of the planning process. The World

Organization for Animal Health (OIE)* maintains lists of animal diseases that are notifiable to the international community. They are reportable because introduction of these diseases to a new country would threaten the animal population and, in some cases, the human population; affect the agricultural economy; and risk the imposition of movement restrictions and trade sanctions. These disease agents, particularly the so-called List A diseases, have been considered as among most likely to be used in terrorist attacks against agricultural targets. However, just because the use of these agents is possible does not mean that it is likely.

In this chapter, I show where agricultural terrorism fits into the much broader field of agricultural security. I also discuss whether agriculture and the food system make attractive targets for terrorist activity and who would be likely to mount such an attack. Lastly, I ask what role disease control and food safety measures play in protecting and responding to deliberate interference with agriculture and the food system. My principal focus is on animal diseases and the safety of food of animal origin because that is my area of expertise, but I also address issues related to crop agriculture.

Agrosecurity and Agroterrorism

I am defining agroterrorism as a deliberate attack on agricultural production systems designed to cause economic injury, disruption of the production system, human disease, or political change. Agroterrorism falls under the general rubric of agrosecurity, which is the conceptual framework of a food system that is resistant to natural disasters, accidental introduction of disease agents or toxins, or deliberate mischief, and one that is economically self-sustaining. Preparation for, and mitigation of, terrorist attack is only one part of agrosecurity.

Agroterrorism is but one of many threats to a secure agricultural and food system. Agriculture is an industry that is fraught with risk from natural disasters such as drought, or the introduction of animal or plant diseases, as well as the business risks that other manufacturing businesses face, such as interest rate and currency fluctuations, or market competition. Naturally occurring disease outbreaks, and the appearance of contaminants in the food chain that might threaten human health, have always been a risk. The control of animal and plant diseases and the assurance of a safe food supply were concerns long before the current focus on agrosecurity and agroterrorism. Indeed, the predecessor of the U.S. Department of Agriculture, the Bureau of Animal Industry, was created in 1890 to inspect and certify that pork products for export were free of trichinosis, a parasite in the meat of pigs that can infect humans.

* The World Organization for Animal Health was previously known as the Office International des Épizooties, but has retained the acronym OIE.

Deliberate introduction of animal or plant diseases through criminal activity has historically been very rare, although deliberate contamination of food or the food chain has occurred with more frequency. Even so, the only documented case of casualties in the U.S. from an attack on the food system was from *Salmonella* food poisoning among restaurant patrons in Oregon in 1984, perpetrated by a religious cult.[2] Although a single act of agroterrorism could cause large economic loss, it is unlikely (except in the case of one or two infectious animal and plant diseases) to compete with the annual losses from natural disasters or unintentionally introduced diseases.

The possibility of a deliberate attack against agriculture must certainly be entertained, but it is also important to keep the risk in perspective. It is difficult to document examples of attacks on agricultural targets by terrorists, although crop destruction and the propagation of disease have been used by nation states in the conduct of warfare. Fortunately, developed economies already have systems in place to minimize naturally occurring and unintentional risk to plants, animals, and the food supply, and these may serve to contain the effects of deliberate attack. Even so, the outbreak of FMD that began in the U.K. in 2001, and the appearance of bovine spongiform encephalopathy (BSE) in North America in 2003, both of which received a vast amount of media coverage, focused attention on the vulnerability of both agriculture and the food system to disease risks. A broad reassessment of the ability of the animal health authorities to recognize and respond to epidemic disease outbreaks followed. The elevation of terrorism to a major political issue in the same time frame led to attempts to create a more responsive and integrated system for dealing with threats to agriculture and the food system, whether intentional or unintentional. As part of this process, U.S. agriculture has been declared a critical infrastructure industry in Homeland Security Presidential Directive No. 9 (HSPD-9), which establishes a national policy to protect agriculture and the food system against terrorist attacks, major disasters, and other emergencies.

The changes to the structure of government and commercial organizations involved in preparedness and response to agricultural and food system emergencies were still in process in 2006. A significant change in the approach to disease outbreak control during the past 10 years has been the recognition that large epidemic disease events have many of the characteristics of large natural disasters and that multiagency approaches, integrated into the emergency management incident command system, are appropriate. For instance, in a number of states a declaration of an animal health emergency by the state veterinarian leads to the declaration of an emergency by the governor, which in turn activates the state's Department of Homeland Security in a support role.

Agroterrorism Targets

Many nations have had biological weapons programs. These have generally focused on the weaponization of disease agents to improve their delivery and effectiveness as bioweapons directed against humans, animals, and plants. Large numbers of candidate pathogens have been examined for their suitability as bioweapons and there is evidence of occasional use for this purpose. Glanders, for instance, an infectious disease of horses that is transmissible to humans, was believed to have been used to infect large numbers of Russian horses and mules on the eastern front in World War I in an attempt to cripple the military transport system.[3]

It is not only infectious disease agents that have been used against plants and animals. Chemical weapons have been developed, particularly in the 20th century, by nation states for use in wartime. To give two examples: defoliant herbicides were used in Malaya by the British in the 1950s to remove vegetation from potential ambush sites and to destroy crops in order to deny food to insurgents. In the Vietnam, conflict defoliants were used by U.S. forces to improve visibility by reducing the forest canopy and also to attack agricultural crops in order to encourage the population to leave Viet Cong controlled areas.[4]

Besides the use of biological weapons in conventional warfare and counter-insurgency operations, similar agents could be used by terrorists. The following list attempts to identify the potential targets for terrorist use of biological weapons.

1. The agricultural economy by disruption of the production system or by causing the imposition of trade barriers by trading partners because of the presence of disease. For example, loss of export markets for live animals, meat, and meat products following an FMD outbreak.
2. The safety of the food supply by contamination of agricultural products or interference with the wholesomeness of food products, resulting in harm to humans or loss of confidence in the safety of the food supply.
3. The human population through the dissemination of zoonotic diseases, which are diseases transmitted from animals to man.
4. The human population directly using animal or plant pathogens, such as anthrax bacillus, or toxins, such as botulinum or ricin, used against the human population so as to cause sickness or disease. This contingency is outside the scope of this discussion and falls more properly into a discussion of bioterrorism directed at the human population.

Attacks on the Agricultural Economy

The agricultural economy is a huge and diffuse target, extraordinarily complex and very difficult to defend. The food system from the farm to the consumer's plate consists of a vast network of production facilities, material-handling

systems, food processing plants, transportation networks and product distribution systems, and a plethora of retail stores and restaurants. Because of its size and complexity, this immense and dispersed network is difficult to protect from interference and it is, at least potentially, vulnerable at every point.

At some points, however, production agriculture is more vulnerable than at others. Infectious diseases are more likely to spread when there is large, high density, susceptible populations of plants or animals in close proximity. Modern agricultural production in the U.S. is characterized partly by concentration of production. There are 10,000 cow dairies and 50,000-head beef feedlots, crops concentrated in distinct geographical areas, such as the intensive farming of corn and soybeans in the Midwest, or of wheat in the Upper Plains states. The concentration of production in large units means that infectious diseases can spread rapidly on the same farm and to neighboring farms. In animal agriculture, at least, the means of disease spread from an initial infected premises to other farms lies in the patterns of livestock movement that are also characteristic of the U.S. livestock industry. Large numbers of young feeder pigs, up to 20,000 per day, move from breeding facilities in North Carolina to contract feeding operations in the Midwestern states where the feed, based on corn and soybeans, is cheaper. During a 2002 emergency planning exercise carried out by the National Defense University, a putative FMD infection centered on five farms in North Carolina spread to 35 states within 10 days.[5] Similarly, large dairies send their female calves to specialist calf growers and heifer raisers, who may raise the calves received from a large number of dairies before sending them back, as pregnant heifers 2 years later. These calf and heifer-raising operations may have thousands of animals, move large numbers of them in and out every week, and be two or three states away from the dairy farms with which they have contracts.

Chalk has suggested that the tendency to breed out differences in populations of animals or plants, combined with modern husbandry practices, may increase their vulnerability to disease by limiting the protective effect of genetic diversity and by subjecting them to additional stress.[6] In plants, this has taken the form of monocropping species or varieties, and in animal agriculture, particularly in the pig and poultry industry, of breeding genetically specialized animals to meet the demands of the market for faster maturity or uniform size. Although the introduction of disease-resistant genes has been widely carried out (particularly in plants), allowing for increased intensity of production, the increased animal or plant density within a farm or region puts them at risk of more rapid spread of new diseases.

Attacks on crops may be less dramatic than deliberately caused outbreaks of animal disease, but still have severe economic consequences. Karnal bunt is a fungal disease of wheat, which causes only small losses of crop yield, but affects the quality of grain. Generally, wheat containing more than 3% bunted

kernels is considered unfit for human consumption because of its effect on the odor and taste of flour made from the grains. The greatest impact of widespread Karnal bunt infection in the U.S. would most likely be on grain exports because the U.S. is the world's leading exporter of wheat, accounting for one third of total wheat exports worldwide. The U.S. prohibits the import of wheat and materials, such as straw and wheat chaff, from countries where Karnal bunt is known to occur, but its presence was detected in Arizona in 1996 and, subsequently, in Texas and California. Fortunately, the countries that import grain from the U.S. have continued to accept imports as long as they are certified as coming from areas in which Karnal bunt is not known to occur. But clearly, a major outbreak of a crop disease, whether naturally occurring or deliberately introduced, could result in both domestic losses and loss of important export markets.

Attacks on the agricultural sector can be purely economic in effect or can have the effect of disrupting society by causing interruptions in the operation of markets, restrictions on people's daily lives, or, in some cases, by putting the public health at risk.

Although attacks on commercial agricultural crops can have massive economic consequences, they are less likely to fulfill terrorist aspirations for public outrage, fear, or political disquiet than attacks that affect animals or humans directly. This may not be true for attacks on some agricultural crops in which the public invests social value, such as Christmas tree farms or grape crops in the Napa Valley of California. Attacks on these operations could well be viewed much more as an attack on people's way of life than on the crop itself.

In general, though, the consequences of an economic attack on agricultural production would be inconvenience for the public through supply interruption or added expense because of higher prices for scarce agricultural commodities. In 1996, citrus canker, a bacterial disease of grapefruit, limes, oranges and other citrus fruit, thought to have originated in Asia, appeared in a residential area close to Miami International Airport. In 2006, after an unsuccessful 10-year effort to eradicate the disease, the U.S. Department of Agriculture (USDA) banned the shipment of fresh Florida oranges to 11 other citrus-growing states.[7]

The effects of a direct attack on agricultural production are mitigated by the fact that it is relatively difficult to disrupt the domestic supply of food raw materials because the U.S. has such a massive agricultural industry and a large surplus of most agricultural products. Of all the U.S. industrial sectors that produce trade goods, agriculture is the only one that is a net exporter. For instance, the U.S. produces 40% of the world's maize supply and 6% of the world's meat. However, this very commodity surplus has buried within it a vulnerability of its own: The threat of losing export markets because of bans on the export of these commodities under international phytosanitary rules designed to protect importing countries.

Except for certain activist groups, production agriculture itself, whether crop or animal agriculture, does not make an attractive target for terrorists wishing to use terrorism to communicate in "symbolic ways."[8] Economic attacks on the agricultural industry lack the iconic impact and visible and dramatic results that attacks on other targets, such as landmark buildings, may have. The introduction of a disease, such as FMD, resulting in the destruction of millions of domestic animals, restricted access to the countryside, and upsetting visual images, could have such an impact. On the other hand, it is difficult to imagine other animal diseases or (even more so) crop diseases that would have this effect. However, issue-based activist groups, such as environmental or animal rights, or antigenetically modified (anti-GM) crops groups, whose target issue is closely related to agriculture itself, may find farm targets attractive and symbolic.

The British experience of a major animal disease epidemic in 2001 showed that the "collateral damage" to the economy caused by outbreaks of diseases, such as FMD or classical swine fever, may exceed the direct economic losses to agriculture from the disease and from the costs to contain it. The closure of the British countryside to hiking and other country pursuits, such as hunting, was used as a biosecurity measure to prevent the spread of FMD from one farm to another. The restrictions were aimed at preventing people from carrying the virus to another part of the country on vehicles, clothing, and footwear and resulted in the tourist industry bearing the economic brunt of the outbreak. The Cumbria region of Britain is thought to have lost 31% of its tourist revenue in 2001, and Gross Domestic Product in Britain fell by 2.5 billion pounds of which 1.93 billion was accounted for by reduction in tourism expenditure.[9] The restrictions imposed on people's daily lives by, for instance, restricting access to the countryside, forced government agencies to make controversial decisions that can affect public confidence in political institutions and cause profound changes in government policy toward agriculture and the use of the countryside. The British Prime Minister was prompted to delay national elections by 1 month, and the renaming of the British *Ministry* of Agriculture, Fisheries, and Food (MAFF) in the aftermath of the 2001 FMD outbreak to the *Department* of the Environment, Food, and Rural Affairs (DEFRA) is emblematic of the political downgrading of production agriculture and the rethinking of government policy toward rural areas. In Britain, the loss of rural tourism and restriction of public access to both private and public land accelerated a change in attitudes to land use. Policy decisions and public attitudes attributable in large part to the effects of the 2001 FMD outbreak are making the countryside less a primarily agricultural production area and more an amenity for the general population maintained for the public good by the agricultural community. In the U.S., the current social contract with agriculture is that rural areas are primarily agricultural production areas and public parklands and wildlife areas are

more clearly demarcated from production areas than they are in Europe. In many parts of the U.S., however, farming communities are in close proximity to urban areas, and there are already clear tensions over farming operations close to suburban and exurban homes. A disruptive disease incident could exacerbate these tensions. A major disease outbreak could have major impact on public access and tourism in such areas as Lancaster County, Pennsylvania, home to a large Amish community, or to the Central Valley of California, site of many large dairies on the edge of a densely populated area.

The U.S. has not had an outbreak of FMD since 1929. FMD virus is the most infectious virus of either humans or animals. The U.S. public has seen televised images from Britain of domestic livestock being slaughtered *en masse*, pictures of heaps of carcasses lying in farm yards and fields, and of cattle and sheep burning on funeral pyres, but public reaction to the reality of a major disease outbreak at home is difficult to predict. The public may question, as they did in Britain, whether a disease that kills relatively few animals itself should result in the slaughter of millions. They may also query the competence of animal health authorities and question policies, both disease control policy and wider agricultural policy that appear to put the interests of commercial agriculture and agribusiness ahead of the public good.

Attack on the Food System

The food industry, which is supplied by agriculture, is much more vulnerable. There is a certain fragility to public trust and confidence in the safety of the food supply. A good example is the Alar episode of 1989. Alar was a chemical used to make crops of apples ripen at the same time, and the contention that caused the scare was that it was carcinogenic and posed particular risks to children. Apple producers suffered large losses and eventually the Environmental Protection Agency (EPA) banned the use of the chemical.* There is ample evidence that the public is sensitive to the risks of food-borne illness, although not necessarily well informed.[10] The susceptibility of the public to food scares may make contamination of the food supply a more attractive option for terrorists than direct attacks on agricultural production.

It certainly seems that agriculture is a much more attractive target in the postharvest phase of production; the bulk ingredients leaving farms to processing plants, and the processing plants themselves, where large batches of products, often in the hundreds of thousands of pounds, make their way into products packaged for the consumer, into stores across the nation, and onto the kitchen tables of millions of homes across the country. Thus, the security, not only of the farms and orchards that produce the foodstuffs, but also of the transportation, processing, and distribution system that prepares and delivers the food for

* "Daminozide (Alar) Pesticide Canceled for Food Uses," EPA Press Release, Nov. 7, 1989.

the consumer, is a matter of great concern. In many ways, the postharvest phase of food production, between the farm and final packaging when food material is often handled in bulk, is the most vulnerable to intentional interference. It is also technically much easier to contaminate a tanker load of milk or a grain bin than it is to infect or poison cattle or fields of wheat, in the hope of causing harm to humans that consume products made from them.

In 1999, the U.S. was responsible for 46% of world soybean production and about 32% of the world's soybean oil. A semitrailer holds 24 tons of soybeans, enough to make nearly 5000 pounds of oil. Processing plants handling many truckloads of soybeans for processing per day have the potential to contaminate very large batches of edible oils in the event of deliberate contamination of the raw material. Locally produced food, processed in small processing facilities and sold in local markets, is much less vulnerable to this problem.

The complex food distribution system makes commodity food production vulnerable, not just to terrorist interference but to accidental contamination as well, by such well known and ubiquitous pathogens as *Listeria monocytogenes, Salmonella, Escherichia coli*, or plant toxins. Food products, whether grains or hamburger, which are processed in bulk in a few large plants and directly packaged in those plants for the consumer, have the potential for one contaminated batch to be delivered to thousands of consumers.

The consolidation of both production and processing into large farm units and processing plants increases the risk that large amounts of product will be contaminated by a single event. The production of food on an industrialized scale increases the vulnerability of the food chain to contamination by increasing the batch size in which commodities, such as beef hamburger, milk, or grains, are transported and processed. In 1997, Hudson Foods recalled 25 million pounds of ground beef after *E. coli serotype* O157:H7 contamination was found in quarter-pound hamburger patties.[11] This recall from one plant represented 0.3% of the 8 billion pounds of annual U.S. ground beef production.

Contamination of a milk tank on a large dairy farm with a toxin, such as an organophosphorus pesticide, could affect products ranging from bottled milk to manufactured products, such as butter, sour cream, and cheese. Even when small numbers of cows are involved, the impact may be widespread. In 2002, after five or six cows on a farm in Indiana were believed to have eaten from a field that had been sprayed with pesticide, milk and cottage cheese were recalled from stores in Illinois, Indiana, Ohio, and Michigan.*

Dissemination of Zoonotic Diseases

There seems to be little incentive for terrorists to infect animal populations with disease agents in the expectation that this will result in disease in

* http://www.wndu.com/news/productr/022002/productr_31897.php, accessed on August 14, 2006.

humans. In the vast majority of imaginable scenarios, health surveillance of animals and existing food safety inspection procedures make even a moderate-sized outbreak of human disease highly unlikely. There are, however, possible candidate infections which if established in animals could cause life-threatening disease in humans. Rift Valley fever, an insect-transmitted viral disease most often seen in North Africa and Arabia, can cause hemorrhagic fevers and hepatitis in humans. Although it is possible for humans to be infected by close contact with infected animals and their carcasses, in order to infect substantial numbers of humans, affected animals would have to pass the infection to a susceptible mosquito population, which would then be the vector for transmission to humans. This is theoretically possible, but it seems an unlikely terrorist aspiration.

Although the infection of animals with zoonotic pathogens in order to harm humans is relatively unlikely, the same is not true of the use of zoonotic pathogens to infect humans directly. Although it is outside the scope of the present discussion, some animal disease agents, such as anthrax spores, have been used directly in attacks on humans and animal bacteria, such as *Salmonella and E. coli* O157:H7 can be used to directly contaminate food supplies, e.g., salads, dairy, or meat products. (The reader is referred to texts on bioterrorism.)

Who Are the Terrorists?

Acts against agriculture and the food system, which may be construed as agroterrorism, could be carried out by different groups with widely differing capabilities and widely differing agendas. To a certain extent, the nature of the terrorist group may determine the type of target chosen and the nature of the action. For instance, groups that are sponsored by nation states, or nation states themselves, may have access to sophisticated and large-scale production of biological or toxic materials and, in some cases, sophisticated or militarized delivery systems. Given an appropriate delivery system, weaponized disease agents, such as anthrax organisms directed against humans and livestock, could expose large numbers of people and animals to anthrax infection during an initial attack. Ideologically or politically motivated non-state terror groups could get access to weaponized materials through theft or diversion of materials, but could more easily acquire infectious materials, such as FMD virus-infected tissue. Small amounts of infected tissue taken from animals in a country in which FMD is endemic could be smuggled into the U.S. and used to infect only small numbers of animals, but create a very large disease outbreak through subsequent spread of infection in the animal population. The attraction for a terrorist is that such materials are relatively easy to obtain from animals in the field, do not require any processing in a

laboratory, do not present a disease risk to the perpetrator, are very simple to deliver to the target population, and are highly infectious. Such terrorist groups may also be able to acquire or manufacture small quantities of toxic material, such as ricin, which, if used to contaminate food ingredients, could be widely spread through the food manufacturing and distribution system.

Individual agricultural and food businesses are also vulnerable to malicious criminal rather than terrorist attack, which although not initially aimed at the wider economy may have widespread impact. Antibiotic contamination of a farm milk tank in which milk is stored before being picked up from the farm could be aimed at causing economic harm to an individual dairy farmer, but if not detected may result in the contamination of large quantities of milk at the milk plant.

Domestic issue-based activist groups, the "terrorists so-called special interest," such as environmental, antiglobalization, animal rights, or anti-GM crops groups, may target the same agricultural targets, but as a way of attacking domestic policies or particular types of farm operations or commodities. Historically, they have engaged in more limited acts; sinking metal spikes in trees to cause damage to logging equipment and injuries to loggers when the spikes are struck by a chain saw; an arson attack on a livestock slaughtering plant in Redmond, California in 1997 that caused $1.3 million in damage. Activists opposed to the introduction of GM crops, including maize and oilseed rape (canola) into Europe have been responsible for the destruction of fields of GM crops at test sites.

Criminal mischief has always been a part of rural life, and the availability of laws to prosecute criminal acts as agroterror crimes makes the elevation of ordinary criminal acts directed at individual farms a prosecutorial temptation. Some of these crimes may inadvertently contaminate the food supply and cause mass public harm. The contamination with antibiotics of a milk storage tank on a dairy farm by a disgruntled former employee, aimed at causing business disruption and financial loss to the dairy producer may have the same effects as a deliberate act of terrorism aimed at exposing large numbers of the population to a harmful agent. With changes in the law in the U.S., the distinction between criminal acts and terrorist acts is in danger of becoming blurred. *The Star Press* of Muncie, Indiana (February 18, 2006) reported that investigators considered charging an individual, who put metal spikes in farm fields with the intent of damaging the tires of farm equipment, with agricultural terrorism. The field spiking was done as a protest against a planned agricultural business park on the site, and the person was eventually charged with criminal mischief. Interestingly, in a case involving the destruction of GM crops in France in 2004 and 2005, the court acquitted 49 activists who destroyed GM plants after ruling that their actions were justified.

Agroterrorism Agents

Agents that can be used in attacks against agriculture and the food system fall into a number of broad areas.[12]

1. Pathogens that affect animals only (e.g., rinderpest virus)
2. Pathogens that affect plants only (e.g., karnal bunt in wheat)
3. Zoonotic pathogens that affect animals and man (e.g., anthrax, rabies, and *Brucella*)
4. Pathogens spread by insect vectors to animals and man (e.g., Venezuelan equine encephalomyelitis virus)
5. Animal- and plant-related toxins (e.g., botulinum, ricin, aflatoxin, fumonisins, and tricocethenes)
6. Advanced biochemical agents, such as genetically manipulated organisms with enhanced toxicity or pathogenicity

Another way of looking at these agents is classify them as those that may be effectively used in a direct economic attack on agricultural production, those that may damage public confidence in the food supply, and zoonotic diseases. From a very large number of candidate pathogens, the following could be considered to have terrorism risk potential.

1. Economic attack
   (a) Animal diseases
      – Foot and mouth disease
      – Exotic Newcastle disease
      – Classical swine fever
      – African swine fever
   (b) Plant diseases
      – Soybean rust
      – Corn seed blight
      – Karnal bunt
2. Public confidence
   (a) Avian influenza
   (b) Anthrax
   (c) Brucellosis
3. Zoonotic diseases
   (a) Rift Valley fever

Protection and Surveillance

Protection of agricultural production in the U.S. has mainly been aimed at preventing the spread of infectious disease in livestock and crops between the different states and controlling the entry of disease agents at the borders.

Certificates of veterinary inspection (health papers) are used to regulate the movement of animals and to control the transmission of disease between states, with each state deciding on the requirements it wishes to impose on the movement of animals from other states. It is up to the person wishing to move livestock to another state to find out what the state requirements are in terms of documentation and testing. From time to time, these requirements change as states become free of diseases (such as brucellosis) or when there is a resurgence of disease, such as the current concern over the reappearance of tuberculosis in dairy cattle. Indeed, many states have recently established a requirement that any dairy animal over 6 months of age must be tested for tuberculosis before being allowed across the state line. This system, at least in theory, means that only healthy animals are moving between states, and it works well for animals that may have an established but not particularly infectious condition, such as brucellosis or tuberculosis. The weakness of any inspection system is that an animal may be exposed to a highly infectious disease, such as FMD *after* veterinary inspection and before traveling to another state or even be in the incubation period of the disease, but not yet showing any clinical signs. In the event of an epidemic disease outbreak, interstate movement of livestock would be restricted or banned once the disease is recognized. The dangerous period for disease spread is from the time of first introduction of a disease into the country to the time of diagnosis, and the imposition of movement restrictions — a crucial period of time, as far as disease control, is concerned. By the time FMD was recognized in the U.K. in 2001, it is thought that up to 57 premises spread over a large part of England were already infected.[13] Even so, a 3-day delay in halting animal movement in the U.K. after confirmation of the diagnosis of FMD has been blamed in part for the size of the outbreak.*

The protection of livestock from exotic diseases depends to a very large extent on the protection that is given by border inspection and quarantine. The ability to prevent smuggling of animal and plant products, whether for profit, with criminal intent, or simply by uninformed travelers, is crucial to the protection of domestic agriculture. Some diseases can cross borders without human assistance — soybean rust for instance, the spores of which are carried by air disturbances, particularly hurricanes and other severe weather systems, or avian influenza carried by migratory waterfowl, such as swans and ducks. Introductions of diseases of terrestrial animals, such as FMD or classical swine fever, are most likely to be through the illegal imports of animal products, such as hams, sausages, or dried meat, that then infect pigs through the practice of

* At the Royal Society of Edinburgh inquiry into the FMD epidemic, it was suggested that imposition of movement controls immediately after the confirmation of the diagnosis, as was done for international movement, instead of 3 days later, would have reduced by one third the number of animals that had to be killed. (Inquiry into FMD in Scotland, p. 18, July 2002, Royal Society of Edinburgh.)

feeding them household or restaurant waste (garbage feeding). In the U.S., the responsibilities for border inspection have been transferred to the Department of Homeland Security Customs and Border Protection, whereas quarantine stations for handling live animal imports are the responsibility of USDA Animal Plant Health Inspection Service (APHIS) National Center for Import and Export. There is a little risk of epidemic diseases finding their way into the U.S. among quarantined animals; quarantine times are relatively long and the incubation times for diseases that can threaten an epidemic are short. The danger at the border is the difficulty of intercepting animal products carried by innocuous travelers who are contaminated with infectious agents (the virus of swine vesicular disease can live in a salami sausage for up to 200 days at room temperature) and of intercepting terrorists carrying contaminated materials or infectious agents. The magnitude of the task is illustrated by the fact that 400 million people entered the U.S. in 2002, of which 330 million crossed at land crossings rather than at airports or seaports.*

The OIE is the international organization responsible for compiling disease reports provided by national governments. From the point of view of threats to the domestic animal population in the U.S., the most important are the List A diseases. These are also the diseases that, if present in a country, are most likely to result in the imposition of trade barriers. List A diseases are those transmissible diseases, which have the potential for very serious and rapid spread, irrespective of national borders, which are of serious socioeconomic or public health consequence, and which are of major importance in the international trade of animals and animal products.

The reports published by OIE are the main source of intelligence about the worldwide distribution of infectious diseases and provide an important method of assessing the risk of introduction of infectious disease through the movement of people, animals, or animal products.

Ultimately, the protection of agricultural production from the introduction of infectious disease agents depends on biosecurity measures adopted by the farmer. Farm-level biosecurity has received much more attention in recent years and has been a focus of many outreach and educational programs for producers. Poultry and pig farms in general employ higher levels of biosecurity than do beef, dairy, or sheep farms because of the nature of the agents that threaten the health of their animals. Pseudorabies virus infection in pigs and fowl cholera in poultry, for instance, can easily be introduced to farms that have lax security measures. Poultry and pig farms routinely restrict access to their premises, quarantine animals coming to the farm, and take precautions against service people, feed trucks, or livestock haulers carrying infection onto the farm. Farm biosecurity protocols may include such precautions as rodent control, restrictions on farm workers having contact with

* U.S. Department of Transportation and U.S. Department of Homeland Security statistics.

farm livestock off the farm, and even the provision of meals for the workforce so that illegally imported meat products, which may be contaminated with viruses, do not find their way onto the farm.

Once agricultural products have left the farm and become part of the food processing and distribution system, they need protection against accidental or deliberate contamination.

Hazard Analysis and Critical Control Point (HACCP) systems have been widely adopted by food processors and as the framework of the Food Safety Inspection Service (FSIS) procedures for monitoring the safety of the food supply. HACCP is aimed at determining the points in a process, in this case food materials handling and processing, at which contamination or process failures (for instance, failure to control product cooling) may affect the safety of the product. Since 1996, FSIS has applied this system to slaughter and processing plants in the U.S. as the basis of their regulatory inspection system. HACCP can be extended beyond processing plants to encompass the whole food system from farm-to-plate.

Vaccination and Population Resistance

Vaccination of susceptible animal populations would seem to offer opportunities for increasing resistance to infectious disease agents, thus mitigating the effects of a terrorist attack using infectious agents as a bioterror weapon. However, the logistical, technical, and economic obstacles to mass vaccination against a wide variety of diseases are huge. Vaccination has been successfully used in the eradication of diseases, such as FMD, following outbreaks of the disease caused by a single strain of the virus. Arguments against prophylactic vaccination for FMD are the number of animal species affected (all cloven-hoofed domestic species), the large number of distinct virus strains that can cause outbreaks of FMD, constant mutation, the possibility that a vaccinated population will mask the presence of active infection, that animals with antibodies to the vaccine strain will confuse diagnostic testing in the event of an outbreak, and the expense of maintaining vaccination cover over multiple species of animals. Other viruses, such as African swine fever, are difficult to vaccinate against because of the meager immune response elicited by the virus. Currently, stocks of vaccines for diseases, such as FMD, are held in vaccine banks and are available for deployment internationally to aid in the control of new incursions of the disease into countries previously free of it.

Diagnostic Resources

Computer modeling of infectious disease outbreaks and experience in the field shows that the time from first appearance of the disease on a farm to the time the diagnosis is made is a crucial factor in limiting the size of the

outbreak. The 2001 FMD outbreak in Britain had been in progress for approximately 3 weeks when infected sows were found in a packing plant during veterinary inspection before slaughter. It is now estimated that by that time 57 premises were already infected, leading to an outbreak that overwhelmed the government veterinary service right at the beginning.

The development of the National Animal Health Laboratories Network (NAHLN), which has brought existing state diagnostic laboratories into the Foreign Animal Disease (FAD) diagnostic effort, has marked a major philosophical shift in the management of serious disease outbreaks.

In 2001, the National Research Council (NRC) formed a committee to study the susceptibility of U.S. agriculture to bioterrorism. At the time, terrorist attacks on U.S. soil were thought to be unlikely. However, the World Trade Center attack on September 11, 2001 raised the specter of attacks against other targets, including essential industries.

There was an increasing awareness of the vulnerability of agriculture and the food system to terrorist interference. The NRC study found that the U.S. was not equipped to respond to biological threats to animal and public health and the agricultural economy. One of the major roadblocks to agrosecurity was the lack of a network of animal disease diagnostic laboratories capable of diagnosing diseases exotic to the U.S. As a result of the attacks on the World Trade Center, the Public Health Security and Bioterrorism Preparedness and Response Act became law in 2002. This act enabled the Secretary of Agriculture to develop programs that would enhance tracking of animal diseases and allow better communication between federal and state laboratories. In order to reach this goal, supplemental Homeland Security funding was used by the Veterinary Services division of USDA's APHIS to develop the NAHLN.

At the time of the British FMD outbreak in 2001, diagnostic specimens from an animal in the U.S. suspected of having a foreign animal disease could only be sent to the Foreign Animal Disease Diagnostic Laboratory (FADDL) on Plum Island, NY for testing and confirmation. Samples collected in the field by USDA or state-employed FAD diagnosticians were sent by air package service to an airport near Plum Island, which is off the eastern tip of Long Island. From there, it was taken by courier to the dock at Orient Point and by boat to Plum Island. The delay in receiving samples at the Plum Island facility, particularly those originating in the western states, could be considerable. In addition, the massive number of samples needing to be tested during the management of a major disease outbreak could easily overwhelm a single facility. Expanding the number of laboratories capable of carrying out diagnostic testing for epidemic diseases would solve some of these problems. It would increase the number of scientists able to work on the problem, improve crucial day-by-day situational awareness, and provide redundancy in the system to mitigate equipment or other breakdowns.

The NAHLN pilot program restructured the manner in which foreign and emerging animal diseases were monitored and confirmed. Originally, the NAHLN program offered funding for training and improved facilities to 12 laboratories across the U.S. However, the National Veterinary Services Laboratory (NVSL) in Ames, Iowa and FADDL on Plum Island remain the main reference laboratories for the detection of animal diseases.

Currently, several laboratories across the U.S. now assist the NVSL in the development of assays and surveillance of certain foreign animal diseases that are considered an agrosecurity risk. These diseases include African swine fever, classical swine fever, rinderpest, contagious bovine pleuropneumonia, lumpy skin disease, vesicular stomatitis, Rift Valley fever, and FMD.

A parallel organization focusing on plant diseases is the National Plant Diagnostic Network (NPDN). The Animal and Plant Disease and Pest Surveillance and Detection Network was established by the Secretary of Agriculture to develop a network linking plant and animal disease diagnostic facilities across the country. It was established to deal with the issues of timely diagnosis and, just as importantly, to create a mechanism for the sharing of diagnostic information among the laboratories and state and federal authorities. It consists of the NAHLN and the NPDN.

Response

Models of infectious disease outbreaks show the importance of early detection and early activation of the control methods employed to limit spread of the disease. Response times are critically important for control of highly infectious animal diseases, such as FMD and classical swine fever. This early response requires a cadre of professionals, whether they are veterinarians and animal scientists, agricultural extension agents, crop specialists, or farmers themselves, who are educated about the types of diseases that are mostly exotic to the U.S. and which they would not see in the normal course of their careers and have the confidence to report their suspicions of an unusual disease outbreak. Disease outbreaks initiated as a result of terrorist or criminal acts may not behave in the same way as unintentional outbreaks. They may, unlike most infectious disease outbreaks, begin at multiple sites simultaneously. They may begin at unusual locations, and the disease agents used and characteristics of the disease may be different from those expected. Early detection of such events requires that veterinarians and diagnosticians widen their index of suspicion beyond their knowledge of the epidemiology and appearance of naturally occurring disease.

A schematic of the steps and agencies involved in the response to a foreign animal disease outbreak in the U.S. is shown in Figure 3.1. A veterinarian suspecting the presence of a foreign animal disease in a client's animal or

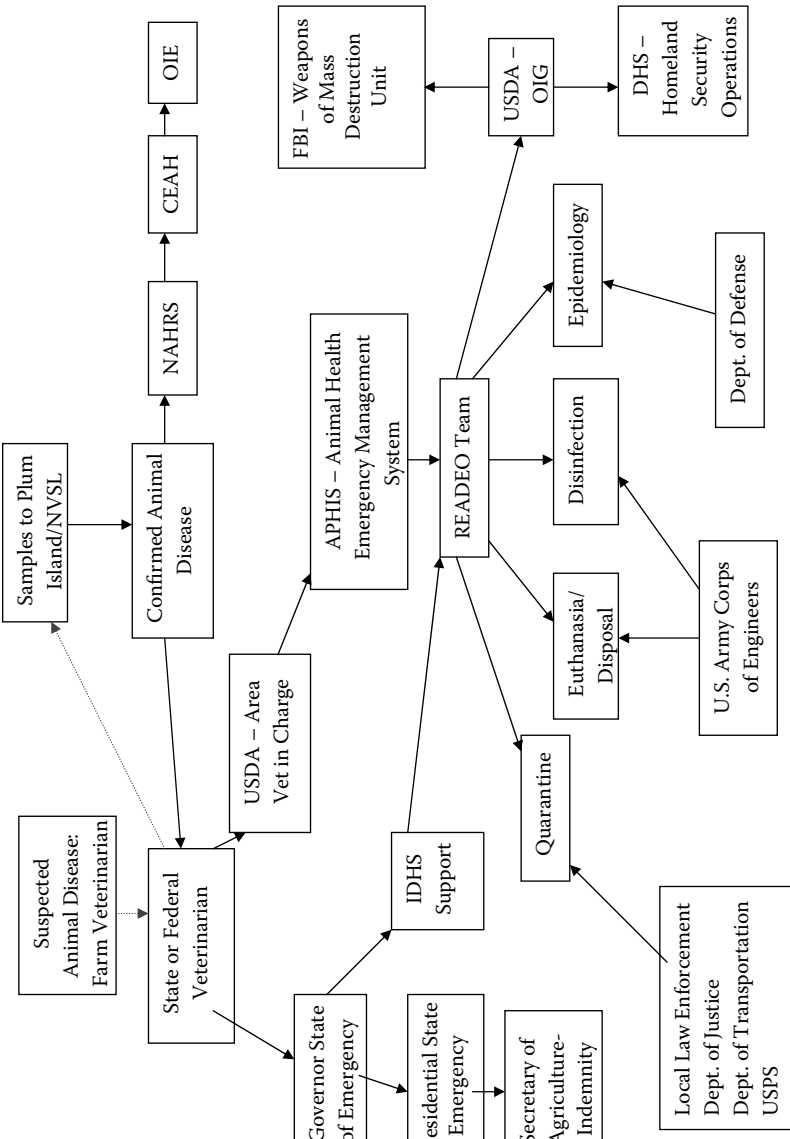


Figure 3.1 Schematic of steps and agencies involved in the response to a foreign animal disease outbreak in the U.S.

herd will make a telephone call to the office of either the state or federal veterinarian in the state. The state veterinarian or federal Area Veterinary Officer-in-Charge (USDA-AVIC) will assign a specially trained foreign animal disease diagnostician from the local office to conduct an examination and take the appropriate samples for diagnosis. At present, the samples are dispatched to NVSL or the Plum Island laboratory for diagnosis and confirmation of the presence of a foreign animal disease. Depending on the situation, the state veterinarian and the USDA-AVIC may request the assistance of the USDA Regional Emergency Animal Disease Eradication Organization (USDA-READEO) and place restrictions on the farm to prevent the spread of the disease while awaiting confirmation. This may require the involvement of local, county, and state law enforcement to isolate the area.

If a positive diagnosis is made, a USDA-READEO team is assigned to the outbreak. Simultaneously, the state veterinarian and the governor of the state may declare a State of Emergency that brings the state Department of Homeland Security and other agencies into the picture in supporting functions. Ultimately, a presidential declaration of a State of Emergency may be sought to provide access to funds for indemnification of producers for animals slaughtered to contain the outbreak. Disease outbreaks are reported to the National Animal Health Reporting Service (NAHRS) and through them and the Center for Epidemiology and Animal Health (CEAH) to the OIE in fulfillment of international reporting obligations.

If the origin of the disease outbreak is suspected to involve a terrorist or criminal act, then the FBI and the Department of Homeland Security will become involved as a result of contacts by the Office of the Inspector General of the USDA.

One should not underestimate the logistical challenges of bringing a highly infectious disease outbreak under control. Both state and federal personnel are involved in the responses to disease outbreaks, but, in the event of a major disease outbreak, other professionals are likely to be recruited into the effort. Personnel cuts have become a fact of life for the regulatory organizations that must be mobilized to deal with introductions of epidemic diseases. These cuts have been compounded by an increasing number of regulatory functions and increased responsibilities for homeland security issues. Many states have organized teams of private veterinary practitioners and university veterinary faculty to support the state and federal veterinary staffs, who have limited established manpower to deal with major infectious disease outbreaks. The logistical challenges for veterinary authorities include the ability to furnish sufficient trained veterinarians to diagnose new outbreaks of the disease, to handle the epidemiological data generated during a major disease outbreak, to kill affected and in-contact herds and flocks in a timely fashion, if that is the control policy, and to dispose of the carcasses promptly. If there is suspicion

of criminal or terrorist involvement in the disease outbreak, then the complications of crime scene management and chain of custody of specimens are added to the logistical challenges. Delays in the diagnosis of disease outbreaks on new premises, and from diagnosis to slaughter of the affected herds, result in increased risk of spread of the infection. In the case of highly infectious diseases, such as FMD, it is necessary to aim for a time from diagnosis of the disease to slaughter of the animals of 48 hours or less in order to effectively control the outbreak. This capacity needs to be achieved early on in the outbreak while few premises are infected if an exponential increase in infected premises is to be avoided.

The successful response to a major infectious disease outbreak requires a clear and well-rehearsed plan, flexible execution based on good epidemiological field data, a high degree of cooperation between agencies, clearly defined responsibilities in the Incident Command System, the ability to mount a control effort very quickly, and assign and, if necessary, recruit and train the required personnel in a matter days.

Conclusion

Agroterrorism is one facet of agrosecurity, which includes the protection of animal health and plant health in production agriculture, the safety of the food supply, and the economic security of an agriculturally based food system. Agriculture and the food industry deal daily with risk, including the occurrence of animal and plant diseases and the risk of contamination of the food supply by pathogens and toxins. Agriculture has experience with naturally occurring diseases, with unintentional introduction of animal and plant diseases, and of contaminants into the food supply. The food system has risk assessment tools, preventive measures, and incident control methodologies, such as HACCP, for food safety, and biosecurity measures and the Incident Command System for disease outbreaks. These have been mostly directed toward preventing and dealing with nonterrorist incidents. There is some experience with criminal contamination of the food supply, but virtually none with criminal or terrorist propagation of animal and plant diseases, except for small-scale incidents associated with issue-based radical groups. The elevated political status of all types of terrorism, including agroterrorism, has not been validated by open source risk assessment or by experience. Risk assessment for terrorist activities is, in any case, difficult to do and this makes it difficult to allocate resources based on the probability of terrorist events occurring. In the absence of viable risk assessment methodology, there has been a tendency to substitute *threat* for *risk* in the rhetoric surrounding terrorism, thus justifying a large commitment of resources to the prevention of acts of

terrorism. In the case of agriculture, this may not be as large a problem as it may be in other spheres, since the disease agents and contaminants that could be used by terrorists are, in most cases, those that already supply risk to agriculture and the food system: FMD virus, botulinus toxin, *Salmonella,* etc. Measures aimed at controlling these risks provide a framework for dealing with terrorist and criminal interference within production agriculture and the food chain. The additional resources allocated to agrosecurity in the name of terrorism prevention and terrorist incident management already pay dividends in an increased ability to deal with the better understood risks to agrosecurity.

References

1. United States General Accounting Office (GAO), Foot and Mouth Disease: To Protect U.S. Livestock, USDA Must Remain Vigilant and Resolve Outstanding Issues, GAO-02-0808, July 2002.
2. Carus, W.S., Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century, Center for Counterproliferation Research, National Defense University, Washington, D.C., 1999.
3. U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID), Glanders and melioidosis, Biological Warfare and Terrorism: Medical Issues and Response, 2000, pp. 21–25.
4. Westing, A.H., Herbicides in warfare: the case of Indochina, in *Ecotoxicology and Climate*, Bourdeau, P., et al., Eds., 1989, archived at Stanford University, Department of Global Ecology.
5. Reardon, J.W., Food Administrator, North Carolina Department of Agriculture and Consumer Services, Testimony to the House Committee on Homeland Security, May 25, 2005.
6. Chalk, P., *Hitting America's Soft Underbelly: The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*, RAND Corporation, National Defense Research Institute, 2004, pp. 9–10.
7. USDA/APHIS News Release, USDA Announces Availability of Draft Citrus Health Response Plan, USDA/APHIS News Release Mar. 7, 2006.
8. Wilkins, L. and Vultee, F., Disasters that communicate: a proposal for a definition and research agenda, *Nat., Haz. Obs.*, 29 (3), 5, 2005.
9. Quantifying the Economic Impact of Foot and Mouth Disease in the UK: Results from the Nottingham Model. Christel DeHaan Tourism and Travel Research Institute, Nottingham University Business School, University of Nottingham, U.K., 2001.
10. Fischoff, B. and Downs, J.S., Communicating foodborne disease risk, *Emerg. Infect. Dis.*, 3 (4), 489–495, 1997.

11. USDA Press Release, Glickman announces Hudson to act on USDA recommendation. USDA Press Release No. 0283.97, Washington D.C., Aug. 21, 1997.
12. Horn, F.P. and Breeze, R.G., Agriculture and Food Security in Food and Agricultural Security, *Ann. N.Y. Acad. Sci.,* 894, 9–17, 1999.
13. Evans, A., The 2001 Foot and Mouth Disease Epidemic In Great Britain, Proceedings of The Office of Science and Technology Blue Ribbon Panel on the Threat of Biological Terrorism Directed Against Livestock, December 8-9, 2003, pp. 147–152.

4 Illicit Trafficking in Nuclear and Radiological Materials

DAVID YORK

Contents

Introduction: Defining the Threat

The Cold War never ended, it just expanded to incorporate new silent enemies in a polarized world. As a result, other nation–states have initiated their search for the concept of mutually assured destruction to hold timeless enemies

at bay, which were previously restrained by the polarization between the U.S. and the Soviet Union. Everything changed in 1991 with the fall of the latter.

In 1991, it is estimated that the Soviet Union's nuclear arsenal consisted of 35,000 nuclear weapons.[1] After the Soviet Union collapsed, it is estimated that about 22,000 nuclear weapons were in newly independent states that were once a part of the Soviet Union.[2] Each of these states was in a decrepit state of disarray and financial ruin as each newly formed state's financial institutions were in dissolution. This forced each of the 15 republic central banks to increase the production of rubles and ruble credits to accommodate the price freeze on most items, which was put into effect to stifle the skyrocketing inflation. This, in turn, only created more inflation due to the lack of financial discipline among the individual financial institutions; inflation increased to over 1000%. Overnight, the Russian "Black Market" was seemingly legalized, nurturing smaller criminal groups into international criminal networks, and one product the former Soviet Union had a lot of was military weaponry and equipment.[3]

During this time, the Nunn–Lugar Nuclear Threat Reduction Act, fostered by Senator Sam Nunn (D-Ga.) and Richard Lugar (R-Ind.), was passed by Congress to provide assistance in dismantling or safely storing the majority of weapons that were in the suddenly independent republics of Ukraine, Kazakhstan, and Belarus.[4] However, most of the money provided to the Russian Federation was siphoned off into private bank accounts, leaving nuclear material stockpiles guarded with a master lock and a guard on duty, who would take a very long nap for a very small price.

The Russian nuclear black market has grown at breakneck speed since 1991, and has become an international crisis. Multiple incidents of trafficking in nuclear weapons, nuclear weapons grade material, nuclear triggers, nuclear weapons-related equipment, nuclear weapons schematics and blue-prints, and scientists selling their expertise have been recorded and are increasing in their frequency. The director of the International Atomic Energy Agency (IAEA), Director General Mohamed El Baradei dubbed the crisis a "nuclear Wal-Mart."[5]

To begin, it is important to understand exactly the threat that nuclear proliferation and trafficking of nuclear and radiological material poses to the U.S. Thus, we shall consider the following evidence.

In 1995, shortly after Chechens planted several canisters of cesium-137 in Izmailovsky Park in Moscow, Dzokhar Dudayev, Chechen mafia leader, made an interesting proposal to the U.S. Dudayev would sell his stockpile of nuclear weapons to the U.S. if the U.S. would recognize Chechnya as an independent state. The U.S. refused.

Dudayev sold the estimated 20 nuclear suitcase bombs to Al-Qaeda for $30 million and two tons of no. 4 heroin.[6] During the fruition of the deal, Al-Qaeda's

no. 2, Ayman al-Zawahiri, was arrested in Dagestan for illegal entry while traveling to Chechnya. He served 6 months in jail and was released.[7]

The existence of these suitcase nukes was further corroborated when General Alexander Lebed, a high-ranking GRU officer, suggested during an interview with CBS *60 Minutes*, on September 7, 1997, that the Russian armed forces had lost more than 100 of the suitcase bombs.[8] Even more alarming was the suggestion made by Stanislav Lunev, the highest-ranking Soviet military intelligence officer to defect, that during the Cold War, Russian Spetsnaz (Russian Special Forces) were forward deployed with atomic demolition munitions (ADMs) to the U.S. In the event of a U.S.–Soviet war, the Spetsnaz would detonate ADMs in strategic locations throughout the U.S.[9]

According to several sources, Soviet-made ADMs have found their way onto the Russian black market and into the hands of terrorists. During interrogations of captured Al-Qaeda leaders, a plan was uncovered dubbed the "American Hiroshima." This plan consists of multiple detonations of nuclear weapons in major U.S. cities. It is suggested that the range of nuclear weapons already smuggled into the U.S. is between 12 and 70.[10]

During 2001, shortly after September 11, George Tenet, the director of the Central Intelligence Agency (CIA), informed President Bush that at least two suitcase nukes had been smuggled into the U.S. The two devices, containing at least 2 kilotons of fissionable material, one bearing the serial number 9999, were believed to have been purchased by Al-Qaeda agents from Central Asian criminal groups. The devices are suspected to be of Russian make, as one of the devices had a Russian manufacturing date of 1988.[11]

Although this chapter is not focused on Al-Qaeda's plans in general, it is important to understand how nuclear proliferation and nuclear trafficking affect the U.S. as well as the international community. Nuclear trafficking is a part of nuclear proliferation. Thus, to comprehend the extent of nuclear trafficking, we must first understand the categories of nuclear proliferation.

Nuclear Proliferation

Nuclear proliferation is not limited to the diversion or dissemination of nuclear and/or radiological material, but encompasses the spread of nuclear weapons technology. This ultimately includes nuclear and radiological materials, dual-use items, weapon designs, and any type of technology that is considered necessary or accommodating to the production of nuclear weapons.[12]

As an example of nuclear proliferation involving the proliferation of material, one might consider the Democratic People's Republic of Korea (DPRK-North Korea). Yongbyon, 60 miles north of Pyonyang, hosts North Korea's Special Weapons Facilities, which include a 5-megawatt (MW) research reactor, the Radiochemical Laboratory of the Institute of Radiochemistry, the Nuclear Fuel Rod Fabrication Plant, a 50-MW reactor currently under construction, and a spent fuel storage pond. On January 8, 2004, an unofficial American delegation visited Yongbyon where they were shown an empty spent fuel storage pond where 8000 nuclear spent fuel rods once resided and remained under the watchful eye of the IAEA, sanctioned under the Agreed Framework and the Nuclear Nonproliferation Treaty (NPT): international treaty devised to prevent the proliferation of nuclear material and technologies.[13] North Korean scientists claimed that the spent fuel rods had been removed and reprocessed.[14] It is suspected that the 8000 spent fuel rods contained enough plutonium for six nuclear weapons.[15]

As mentioned previously, nuclear proliferation is not limited to the proliferation of nuclear or radiological material, and it does not necessarily have to be considered illicit in its nature. In 1995, Russia signed a deal with Iran to build two VVER-1000 light water reactors (LWR) at Bushehr. The Russian–Iranian deal also included a centrifuge facility to enrich uranium, which would provide fuel for the LWR. Shortly thereafter, the agreement for Russia to provide the centrifuge facility was cancelled under U.S. pressure.[16] Such a deployment of nuclear facilities by one nation–state to another is an excellent example of nuclear proliferation within international norms. Regardless of the international community's endorsement of these types of agreements between two nations, the deployment of any nuclear facility requires the technical expertise associated with handling such a facility, and warrants the country married to expansion of the nuclear fuel cycle due to financial investment. In 2002, Russia agreed to build several more reactors as a draft plan for technical cooperation between the two countries.[17]

Classes of Nuclear Proliferation

Due to the complexity of identifying the various forms of nuclear proliferation, we shall cover several classes that define the specific types of proliferation. The first class is divided into vertical and horizontal proliferation, which is directly associated with the proliferation of nuclear weapons capabilities. The second class, divided into induced and latent proliferation, deals more with the social interaction between nation–states and their capabilities as a function of current nuclear fuel cycle technologies.

Vertical vs. Horizontal Proliferation

Vertical proliferation is considered to be the modernization or advancement of existing weapons technologies in countries already possessing nuclear weapons. A perfect example of vertical proliferation is using tritium to "boost" fissionable devices.

In weapons development, a tritium–deuterium mix is utilized inside a plutonium pit, replacing the external neutron generator. This is primarily to increase the rate of burn of the fissile material, thus consuming more plutonium prior to pit disintegration. Therefore, the fission bomb can be doubled, respectively, using of a fusion boosted core by providing a burst of additional neutrons.[18]

Further development of nuclear weapons boosting has led to replacement of tritium–deuterium mix with lithium–deuteride, decreasing some of the maintenance issues posed by using tritium (short half-life requiring frequent replacement in an aging stockpile and the complications of dealing with a radioactive gas). Lithium splits into tritium and helium upon absorption of a neutron. Because lithium, deuterium, and other potentially dangerous elements may be used in large concentrations to facilitate the fission and fusion fuel cycles, it is important to keep in mind the danger dual-use items pose, which will not be covered in the scope of this chapter.[19,20]

Vertical proliferation encompasses the advancement of technologies to field a more sophisticated nuclear weapon, meaning it is not limited necessarily to the actual nuclear device. Rather, vertical proliferation may also include multiple re-entry vehicle technology and missile advancements, for example.[21]

Horizontal proliferation is considered to be the spread of nuclear materials and/or technologies by private companies or state nuclear programs to assist nation–states that do not have nuclear weapons or that possess a covert nuclear weapons program. There is no better example of horizontal proliferation than the infamous Khan network.[22]

In 1976, Abdul Qadeer Khan, a German-educated metallurgist, left the Urenco enrichment facility at Almelo, The Netherlands, taking with him uranium enrichment design blueprints. He returned to his home in Pakistan and began a covert nuclear weapons program that would be known as the Dr. A. Q. Khan Research Laboratories (KRL). This ultimately led to the successful detonation of Pakistan's first nuclear device on May 28, 1998. [23]

In October 2003, the BBC China, a German-flagged ship destined for Libya, was intercepted by a U.S. warship and forced to divert to Italy. Aboard the ship investigators found several thousand gas centrifuge components used for uranium enrichment.[24] It was determined that the centrifuge technology was part of a vast international black market for nuclear technology and material.

Not only did Khan proliferate nuclear centrifuge trade secrets to his country, but the Khan network expanded to include technology transfers to Iran, Libya, North Korea, Iraq, Saudi Arabia, Sudan, Nigeria, Malaysia, Indonesia, Algeria, Kuwait, Myanmar, Brazil, and possibly Syria, Egypt, South Africa, Turkey, and other South American countries. It is also suspected that workable designs for a nuclear warhead were sold to Libya and several other countries.[25] Even more disturbing, a KRL scientist, Dr. Sultan Bashiruddin Mahmood, after being interrogated for several weeks by CIA officers in Pakistan, admittedly met with Osama bin Laden, al-Zawahiri, and other Al-Qaeda officers in Kabul, Afghanistan. The contents of the meeting consisted of technical details regarding a nuclear blast in an American city. Interestingly enough, the meeting took place on September 11, 2001.[26]

The Khan network is a special case where nation–states with varying technical capabilities trade to enhance their nuclear weapons efforts. The discovery led to Libya's renunciation of a covert nuclear weapons program and the uncovering of Khan's trafficking network that undoubtedly spanned four continents.[23]

Horizontal proliferation might also include the transfer of advanced military technologies that would help field a more sophisticated nuclear arsenal. Thus, we can take into consideration the transfers of advanced Kh-55 missile technology from the Ukraine to China, Iran, and eventually North Korea as an incident of horizontal proliferation.

The transfer of Kh-55 missile technology is a particularly interesting case where advanced missile technology, abandoned in the Ukraine during the dissolution of the Soviet Union, made its way into the international arms market. In 2000, O. H. Orlov and E. V. Shelenko, two Russians associated with the Progress export company, furnished UkrSpetzExport, a Ukrainian exporter, with falsified contracts from Rosvooruzheniya arms for the transfer of 20 Kh-55SM missiles. It is suggested that six of the missiles went to China, six were transferred to Iran, and the remaining to undisclosed nation–states. The discovery of this transfer took place in January 2006, when Hrihory Omelchenko, deputy chairman of the committee on organized crime and corruption, informed Viktor Yushchenko, the new Ukrainian president.[27,28] It was discovered that the former Ukrainian Defense Ministry, under a pro-Russian government, knew of the missile transfer and assisted in providing falsified documentation to support the unimpeded shipment. The Kh-55 missile, similar to the U.S. AGM-86B and the BGM-109B Tomahawk, is an air-launched nuclear-armed cruise missile with a range of 1500 miles and has the potential of fielding a 200 kiloton warhead.[29,30]

Thus, vertical proliferation can be defined as the advancement or modernization of a nation–state's nuclear arsenal, whereas horizontal proliferation is the direct or indirect transfer of technologies from one

nation–state to another, which ultimately leads to the advancement of developing a nuclear weapon or fielding a more capable nuclear arsenal. It is also necessary to remember that both vertical and horizontal proliferation may not necessarily be illicit in nature, but that the transfer of dual-use items for a legitimate industry could also provide nation–states with latent, advanced technology to aid potential aspirations for joining the nuclear club.

Induced vs. Latent Proliferation

One of Khan's first customers was Iran. During 1987, Khan visited the Bushehr site and is suspected of supplying, at that time, blueprints for a uranium enrichment facility with a cascade of 50,000 P-1 centrifuges.[28] During the 1990s, A. Q. Khan expanded his network to include centrifuge shipments to Libya, Iraq, Iran, and North Korea; it is suspected that Khan provided nuclear weapon blueprints to several of these countries as well. Khan's network provided the means for advancing Pakistan's own nuclear ambitions, which were in large influenced by India's nuclear weapons program. The obvious pressure that India placed on Pakistan to develop nuclear weapons was depicted in May 1998. Several days after India conducted underground, experimental nuclear detonations, Pakistan conducted similar detonations.[29] This type of influence that one nation–state has on another to either initiate or hasten a nuclear weapons program is considered induced proliferation.

Another interesting example of induced proliferation involves two seemingly unlikely countries, Brazil and Argentina. It is assumed that the inception of Brazil's interest in nuclear technology far exceeded Argentina's. Brazil became interested in nuclear technology in the 1930s, with research into fission. Brazil's vast deposits of uranium ore aided in concessions for the transfer of nuclear technology, largely with the U.S. and West Germany from 1950 to 1970.[30] Brazil's nuclear ambitions focused primarily on energy production up to the 1970s. However, in 1975, Brazil transferred technology from its commercial nuclear energy program to a covert nuclear weapons program code-named "Solimoes." This project was eventually reclassified as the Navy Nuclear Parallel Program. Then, in 1990, the Brazilian president, Fernando Collor de Mello, exposed Brazil's intentions to build an atomic bomb and launched a congressional investigating committee to examine the covert weapons program managed by Brazil's National Nuclear Energy Commission (CNEN).[31] Alarmingly, it was discovered that two atomic devices, with yields of 12 and 30 kilotons, had been developed by the Instituto de Estudos Avancados (IEAv).[30]

While Argentinean interest in nuclear technology began in the 1950s, efforts to increase research into nuclear weapons amplified in 1976, after Brazil signed a deal to acquire an entire nuclear fuel cycle from West Germany.

In 1978, under the directorate of the National Atomic Energy Commission (CNEA), Argentina directed the construction of a secretive enrichment facility at Pilcaniyeu. However, in 1983, with the inauguration of a new president, Argentina's nuclear ambitions cooled and legislation was passed to prohibit the development of nuclear weapons.[32]

The revelation of both countries nuclear weapons programs led to an agreement between Brazil and Argentina, dubbed Argentina–Brazil Declaration on Common Nuclear Policy of Foz do Iguacu, which denounces the research and development of nuclear weapons. Argentina became a signatory of the NPT in 1995. Brazil followed in 1998.[33]

Latent proliferation is considered when a nation–state's technical expertise and industrial capability to facilitate nuclear energy will pose a serious latent proliferation potential or the inherent capability for applying a commercial nuclear energy program to weapons development and design. The proliferation of nuclear technology alone may induce other countries to understand better the capabilities of nuclear energy in relation to weapons development.[20]

The concern of latent proliferation capability accompanying the augmentation of fusion energy generation was described by the U.S. Department of Energy Office of Arms Control and Nonproliferation:

> … one cannot rule out that a technologically advanced country would be able to field a very conservatively designed thermonuclear weapon that would present a credible threat without nuclear testing…[34]

For instance, South Korea's uranium enrichment and plutonium extraction capabilities lend for the technical expertise required for nuclear weapons development. In August 2004, Korea Atomic Energy Research Institute (KAERI) disclosed that in February 2000, researchers had enriched uranium on three occasions without reporting these experiments to the Ministry of Science and Technology, violating South Korea's obligations under the NPT. Very small quantities of uranium were enriched to ~10% using an advanced separation technology, atomic vapor laser isotope separation.[35]

An exhaustive understanding of international and multilateral treaties is important when taking into consideration the legalities of nuclear proliferation. For example, countries that pose a serious threat due to previous behavior, but are interested in the nuclear fuel cycle for commercial electricity must accept the NPT and, possibly, additional protocols that supplement the NPT if they are to receive technical help from NPT members or members of the Nuclear Suppliers Group (NSG). This is to limit the import of certain materials and technologies that would assist that nation–state in diverting material or technology to a covert nuclear weapons program. If a nation–state ratifies the NPT, that nation–state must allow the IAEA to inspect operations at nuclear facilities within that nation–state.

The NPT is not without its faults. Nation–states may abrogate from the treaty after they have successfully deployed the nuclear fuel cycle within their country. Others may take advantage of vulnerabilities in monitoring by actively diverting material from the nuclear fuel cycle. As with several of the previous examples, nation–states might traffic in nuclear material and technology in trade for military technologies. Thus, we consider the illicit transport of nuclear material and or technologies.

Categories of Nuclear Proliferation

The categories of nuclear proliferation focus strictly on the proliferation of nuclear material from nuclear facilities for the purpose of supporting a covert nuclear weapons program. These categories consist of:

1. Diversion of material from the nuclear fuel cycle.
2. Transportation of diverted material to a covert weapons program.
3. Processing of material into fissionable weapons-grade material.
4. Generation of the actual weapon.

Diversion of Material

Diversion occurs when nuclear material is transferred out of the civilian nuclear fuel cycle within a nation–state for the purpose of sustaining a covert nuclear weapons program. A nation–state engaged in diversion must take into consideration the material attractiveness, which includes:

- *Fissionable isotopic content*: The amount of fissionable material that could be extracted from the diverted material.
- *Detectability*: The capabilities for an international nuclear watchdog, such as the IAEA, to detect diversion of the material from the facility.
- *Handling ability*: The difficulty with which to handle the specific nuclear material.
- *Processing potential*: The amount of processing the material requires before it could be used in a nuclear device.

Take into account material that would be deployed to a LWR; LWR types include pressurized water reactor (PWR), boiling water reactor (BWR), and water-moderated–water-cooled reactor (VVR). Nuclear fuel that is deployed to a typical LWR is considered inherently proliferation resistant. This is because uranium-235, the fissionable isotope of uranium, has a concentration of less than 20% in LWR fuel rods; anything below 20% is considered to be low enriched uranium. As well, spent fuel from a LWR has a plutonium concentration of ~1% and is quite radioactive. Thus, LWR fuel would require significant material processing resources for use in a covert nuclear program.[36]

At this level, it is also necessary to consider international agreements and treaties that require obligatory monitoring, material control, and accounting systems to be in place. Thus, a nation–state determined to divert material may participate in facility modification or detection facility modification to support undeclared production and/or diversion.

Transportation of Diverted Material

Attributes to consider during transportation of diverted material include the handling ability of the material and the remote detection capabilities during transportation. At this level, it is assumed that material diverted would remain within the nation–state that hosted the commercial facility. However, it is necessary to consider the possibility that nation–states may engage in horizontal proliferation, providing reciprocal assistance for the advancement of a covert nuclear weapons program or to support the means by which terrorists might acquire weapons-usable material.

In 2003, a prominent North Korean defector suggested that Pakistan transported to North Korea either the nuclear material required or a duplicate of the actual weapon that was tested by Pakistan in 1998.[37]

Processing of Diverted Material

It is assumed that, regardless of the material quality or attractiveness, there is some processing of the material that must take place. Attributes involved with processing of the material for use in a nuclear weapon include the facilities and equipment needed, knowledge and skills, transformation time of the material, and detectability of transformation activities and facilities. For example, on July 21, 2003, U.S. government officials announced the detection of krypton-85 at the border between North Korea and South Korea. Experts suggest that this could be indicative of spent fuel reprocessing.[38]

Generation of a Weapon

Weapon fabrication involves design and handling difficulties, detectability of fabrication activity, facilities and equipment needed, the technical expertise involved, and the fabrication time.

Conclusion

Though nuclear proliferation is a generalized label for a multifaceted issue, it remains to say that nuclear proliferation can best be described as the spread of material, production technology, or expertise to support a nuclear weapons program.

Declared Nuclear Weapon States[a]

Country	Warheads Active/Total[a]	Year of First Test
U.S.	5735/9960	1945 ("*Trinity*")
Russia (formerly the Soviet Union)	5830/16000	1949 ("*RDS-1*")
U.K.	<200	1952 ("*Hurricane*")
France	350	1960 ("*Gerboise Bleue*")
People's Republic of China	130	1964 ("*596*")
India	75–115	1974 ("*Smiling Buddha*")
Pakistan	65–90	1998 ("*Chagai-I*")
North Korea	0–10	2006

[a]Chart from Wikipedia.com.

Suspected Nuclear Weapon States

Israel

It is suspected that Israel may have 300 to 400 nuclear weapons. Israel is not a signatory of the NPT.[39]

States Formerly Possessing or Suspected of Developing Nuclear Weapons

Iran, Saudi Arabia, Brazil, Argentina, Australia, Egypt, Iraq, Libya, Poland, Romania, South Korea, Sweden, Switzerland, Taiwan, Myanmar, and Syria.

Nuclear Trafficking

Nuclear trafficking is deemed to be an outcome of nuclear proliferation and is defined as the illicit transfer or spread of nuclear or radiological material, and/or technologies that aid in the research and development of nuclear weapons. While nuclear proliferation transactions may be legal or illegal under international law, treaties, or agreements, nuclear trafficking is considered to be illegal. Briefly, history has revealed that nuclear trafficking occurs via the following:

- Rogue nations seeking to hide their involvement by using business legends or fronts or by utilizing gangs, criminal organizations, or terrorist networks to carry out their bidding.
- Terrorist organizations seeking to acquire nuclear and/or radiological materials due to the potential devastation and psychological effect of their use.

- Organized crime, which has discovered a lucrative market in trafficking of illicit material to international actors and/or nation–states.
- Amateur smugglers trying to feed their families in a post-Soviet era.

It is inevitable that the list of consumers will grow with the expansion of the nuclear fuel cycle.[40]

For the purpose of this chapter, let us consider nuclear trafficking to include the trafficking of nuclear and radiological materials, as well as nuclear technologies for developing and fielding a radiological dispersal device, an improvised nuclear device (IND), or a design-sophisticated nuclear warhead for placement specifically on a missile. Thus, let us examine the following incident of nuclear trafficking.

> Three residents of Tokmok, Kyrgyzstan, were detained for attempting to sell 4 kg of radioactive "liquid metal"mercury for over 1 million soms (approximately $25,000 as of February 2005), the news agency Kyrgyzinfo reported on 11 February 2005. The arrests were the result of a sting operation in which Kyrgyz National Security Service officers posed as buyers. The suspects have been charged with illicit trafficking in radioactive or poisonous substances, and if proved guilty, they will be sentenced to 2 to 5 years in prison.[41]

While mercury is not necessarily assumed to be associated with nuclear proliferation, the trafficking of mercury is of particular concern as it is used in the enrichment of lithium. In nuclear weapons production, lithium-6 is used to produce tritium, which, in turn, is used in nuclear weapons "boosting." Naturally occurring lithium contains about 8% lithium-6. This small percentage is extracted from the other 92% lithium-7 to produce tritium. This can be done using the column exchange (COLEX) or electric exchange (ELEX) methods, which both require large amounts of mercury.[42]

While the above incident involves a small amount when considering the massive amounts used in a standard industrial facility yielding a significant amount of material to justify the cost of such activity, it is important to consider these incidents, as traffickers may display a sample of a particular product before trafficking a large quantity.

The Nuclear Black Market

Since the fall of the Soviet Union, nuclear trafficking incidents have skyrocketed to levels never before imagined, eliciting the description as an international nuclear "Wal-Mart."[43]

Sandia National Laboratories has compiled a database of nuclear trafficking incidents from the fall of the Soviet Union to the present. At last

check, the current quota (based on open-source information) is ~750 incidents, involving primarily small seizures, such as the mercury seized that we covered previously.

However, seizures or thefts of large quantities of bomb-grade material have alarmed the international community. Below is a brief list of the more disquieting incidents.

Nuclear Trafficking Incidents (1993–2002)

Seized Materials	Date	Location	Suspects
2 kg HEU[a]	March 27, 2002	Chkalovsk, Tajikistan	Unknown
15 kg HEU[a]	August 29, 2002	Sanliurfa, Turkey	Two Turkish nationals
Uranium-235	July 24, 2001	Batumi, Georgia	Four Russians
Nuclear Projectile	March 3, 2001	Amasya, Turkey	Unknown
3.7 kg HEU[a]	August 29, 2000	Elektrostal, Russia	Unknown
6 kg Plutonium	July 29, 2000	Dagestan, Russia	Unknown
.770 kg HEU[a]	April 19, 2000	Batumi, Georgia	Four individuals were arrested in possession of HEU
1 kg HEU[a]	January 14, 2000	Bucharest, Romania	Two Moldavians, two Romanians
Uranium rods	January 1, 2000	Minsk, Belarus	Six international gang members
32 lbs. plutonium	June 28, 1999	Mayak Facility, Russia	Chechen Mafia
.100 kg enriched uranium	February 2, 1999	Bursa, Turkey	Four Turkish nationals
4.5 kg enriched uranium	September 7, 1998	Istanbul, Turkey	Four Turkish nationals, three Kazakh nationals (including a Kazakh army colonel), and one Azerbaijani national
13 cylinders of enriched uranium	July 1, 1998	Van, Turkey	Five Turkish nationals and one Iranian national
.850 kg uranium dioxide	May 26, 1997	Bursa, Turkey	Four individuals (nationality not reported)
20 kg enriched uranium	March 1996	Antalya, Turkey	Five Turkish nationals
1.2 kg enriched uranium	January 26, 1996	Yalova, Turkey	Two Turkish nationals
1.7 kg HEU[a]	June 1995	Moscow, Russia	An individual was arrested in possession of HEU, which he had previously stolen from a nuclear facility; the material was intended for an illegal sale

Nuclear Trafficking Incidents (1993–2002) (Continued)

Seized Materials	Date	Location	Suspects
1.7 kg "red mercury" and 1 kg "black mercury"	May 24, 1995	Constanta, Romania	Two Turkish nationals and three Romanian nationals
2.73 kg HEU[a]	December 1994	Prague, Czech Republic	HEU was seized by police in Prague; the material was intended for an illegal sale
.750 kg enriched uranium	October 19, 1994	Istanbul, Turkey	One Azerbaijani national
12 kg uranium	July 19, 1994	Istanbul, Turkey	Seven Turkish nationals
Uranium (quantity not reported)	April 22, 1994	Istanbul, Turkey	One Turkish national, one Azerbaijani national, and a Russian national
2.972 kg HEU[a]	March 1994	St. Petersburg, Russia	Unknown
4.5 kg enriched uranium	November 27, 1993	Bursa, Turkey	Three Georgian nationals
2.5 kg enriched uranium	October 5, 1993	Gayrettepe, Istanbul, Turkey	Four Turkish nationals and four Iranian nationals (suspected secret service agents)
6 kg enriched uranium	March 1993	Not reported	Not reported

Note: The above incidents were reported by the IAEA, CNS, NIS, or other nuclear authority.
[a]Abbreviation: HEU, highly enriched uranium.

An initial look at trafficking trends of this type seems scattered and erratic, localized primarily to a select group of countries (Figure 4.1). This is not necessarily the case. The success with which other contraband has been smuggled throughout the world suggests that nuclear trafficking may be carried out with relative ease along the same routes by the same criminals or criminal organizations.

Because of the inordinately high threat posed by terrorist or extremist groups acquiring the ingredients for unconventional weapons, it is necessary that illicit trafficking of these materials be better understood to prepare for the sustained global development of the nuclear fuel cycle. Conversely, modeling and analyses of this activity must not be limited in their scope to loosely organized criminal smuggling, but address the problem as a commercial, industrial project for the covert development of nuclear technologies, and unconventional weapon development.

Nuclear Trafficking Examples

Nation-states involved in trafficking regularly utilize criminal organizations with international ties to conduct the bidding, acquisition, and shipping of items to support a nuclear weapons program. This disavows the original

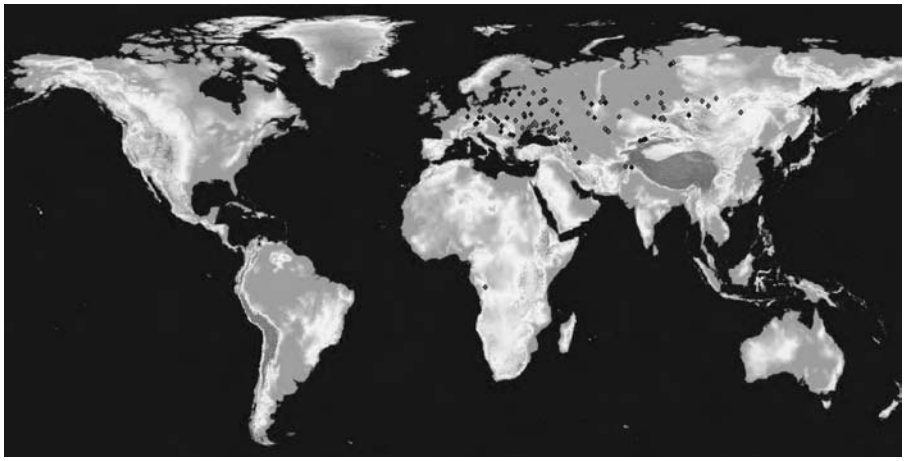


Figure 4.1 International trafficking incidents, 2002.

nation–state from the particular illicit activity and provides a means for plausible deniability, a very necessary step considering the devastating effects international sanctions could produce.

For example, in 1993, Joseph Rimkevicius, an ardent investigator in charge of the organized crime unit in Vilnius, Lithuania, stumbled onto 4.4 ton of beryllium ingots. The material was stashed in the Vilnius bank and another bank located in Kaunas, Lithuania. The tip came after a particularly bloody war between two rivaling criminal groups.

After coordinating an investigation with InterPol, evidence suggested that the beryllium originated from the Institute of Physics and Power Engineering located in Obninsk, Russian Federation. The material was being moved by a trading firm with powerful Russian Mafia connections. The material was to be sold to an Austrian firm, which had acquired a buyer in Zurich, Switzerland, who represented "Korean interests." It is assumed that the material was to be shipped to a Chinese trading company and then rerouted to North Korea.[44]

Beryllium is believed to be the most efficient reflector for nuclear weapons. Upon detonation of the primary high explosives, beryllium reflects neutrons back into the plutonium pit, which aids in the initiation of critical mass within the pit and, ultimately, increases the nuclear yield of the device. Beryllium can also act as a tamper device to increase the force of the explosion.[45]

Nuclear trafficking in support of terrorist organizations may also be facilitated by a nation–state to carry out its bidding.

Consider the likelihood that two senior nuclear scientists of the Pakistan Atomic Energy Commission could have provided technical expertise, weapon designs, and possibly materials to the Taliban and Al-Qaeda during 2001. After resigning due to extreme religious beliefs, Sultan Bashiruddin Mahmood

formed Ummah Tameer-e-Nau (Reconstruction of the Muslim Ummah).[46] This nongovernmental organization (NGO) was directly affiliated to the Pakistani-based Al-Rashid Trust, considered to be a terrorist organization by U.S. intelligence due to its involvement with Al-Qaeda, the Taliban, and Kashmiri separatists.[47] After September 11, CIA interrogators were permitted access to Dr. Mahmood regarding his interaction with the Taliban and Al-Qaeda. After several months of interrogation, Dr. Mahmood admitted to meeting bin Laden, al-Zawahiri, and several other Al-Qaeda officials while in Kabul. The subject of several conversations was the dynamics of a potential nuclear blast in an American city.[48,49]

Thus, we must consider that, within a nation–state, rogue or extremist organizations with close association to the central government may exact their religious and/or political will by aligning with terrorist or criminal organizations. However, it should always be in question how much the executive administration of a nation–state knows about such activities.

There can be no better example of international nuclear trafficking than the Khan network, mentioned in horizontal proliferation. Khan's network was riddled with rerouting of shipments, business legends, and falsified documents to make shipments look legitimate. Unlikely bedfellows emerged among countries with severe ideological and political differences, such as North Korea and Pakistan.

According to U.S. officials, Pakistan's relationship with North Korea began with the sale of North Korean Nodong missile designs in exchange for Pakistani uranium enrichment facility designs.[50] North Korean agents would purchase British-manufactured aluminum tubes from a German company with freight documents indicating an end-user destination for the Shenyang Aircraft Corporation in China.[51,52] Shipments of centrifuge components from the Scomi Precision Engineering company in Malaysia were rerouted in Dubai with falsified documents masking the contents of the shipments.[53,54] The purchase of motors and frequency converters were masked through Elektronik Kontrol Aletleri, an electronic components company located in Turkey.[55] Funds collected during exchange of illicit shipments were laundered by the Dubai Gulf Technical Industries.[56,57]

Analysis of Illicit Trafficking Trends

Clearly, the generation of an accurate analysis to model trafficking routes and nuclear trafficking trends is difficult when you consider that organized trafficking is riddled with the noise of trafficking of random radiological and nuclear sources. Thus, such an analysis requires:

- Cooperative, accurate coverage of incidents, and the material involved, including the origination of the material, the seizure site, and

the suspected or confirmed destination. The sources of information may include immediate reporting of "Material Unaccounted For" incidents, arrests, and recovery of any radiological or nuclear material, and intelligence on end-user involvement concerning the trafficking incidents.
- Quick, precise identification of material in relation to risk for a particular material threat, trend, or local/regional activity.
- Noise filtration of inaccurate information or intelligence from the analysis that may impede the incident interpretation and response to route and risk.

In collecting reports on illicit trafficking of nuclear and radiological material, it is expected that some information or authenticity may be lacking. Though, it is important to note that the collection and modeling of multiple incidents to provide an activity analysis will convey an overall supply and demand trend indicative of illicit nuclear activity and intentions. This may also fill in the gaps to previous reports.

Points to Consider

To comprehend the international crisis of nuclear proliferation and trafficking, we must first identify the origin, the root. Thus, we must consider the following:

1. International deployment of the nuclear fuel cycle is becoming more attractive to countries that have the financial means. It is also apparent that countries with advanced nuclear fuel cycle technologies are willing to sell their expertise.
2. The polarization that the Cold War helped to manage the maladroit race by developing countries to produce nuclear arsenals through mutual protection pacts or political pressures. The world is much more chaotic, absent of the traditional deterrence. For the first time, we face the potential that a substate organization or politically motivated group could enact the devastation of a nuclear blast in an American city and the retribution would probably remain unconventional at best.
3. The ability of international agencies and organizations to detect, report, and discourage nuclear trafficking requires desperate assistance. While it can be assumed that American intelligence agencies were aware of activities such as that of Dr. Khan's, the ability for intelligence to filter through an international organization is subject to political wills, private agendas, and, frankly, grudges. It is, especially important that scientific organizations, such as the IAEA, avoid political problems.

The track record of current international initiatives to prevent illicit nuclear and radiological trafficking is appalling. It is unfortunate that we will only understand our complacency when a nuclear detonation is the means of attack by terrorists. In closing, I will leave you with the following scenario.

Scenario

Members of a terrorist organization smuggle several tens of kilograms of highly enriched uranium (HEU) across the porous Mexican–American border. The material was stolen from an inadequately guarded nuclear facility in the former Soviet Union and then trafficked through Vladivostok to Mexico, on a poorly inspected merchant vessel. Prior to trafficking, the HEU ingot was machined into the respective uranium "bullet" and "target" for use in a gun-type improvised nuclear device (IND). Members of the organization had already trafficked the high explosives through the Mexican–American border successfully. These would be used to accelerate the bullet into the uranium target commencing the chain reaction required to initiate super criticality. The terrorists assemble the weapon in a hotel outside of Dallas– Fort Worth. After assembly, they drive to downtown Dallas and detonate the device.

Effects

The material and design provided for a 10 kiloton explosion. Everything within a radius of 200 miles would be vaporized. The overpressure and winds would severely damage anything out to 500 miles. Up to 1000 miles from the blast zone, winds of up to 150 mph would be recorded. Anyone surviving within 1100 meters of the blast zone would receive 500 rem from neutrons and gamma rays, enough for a 50% mortality rate. The thermal radiation from the nuclear fireball, which emits energy in infrared, visible, and ultraviolet wavelengths, would be enough to cause second degree burns out to as far as 1700 meters. It is estimated that the fallout from the nuclear blast would cover 30 square kilometers[2], with varying morbidity and mortality rates depending on atmospheric conditions.

If the detonation took place during a normal business day, it is estimated that ~30,000 people would die immediately. Several thousand more would die due to radiation or wounds. Hospitals throughout the region would be strained. Every airport around the country would be closed. Seaports would be closed. The borders with Canada and Mexico would be militarized. Martial law would be declared throughout most of the country.

We must take nuclear proliferation and nuclear trafficking *more seriously*. Otherwise, I fear we might see this happen.

References

1. Norris, R.S. and Kristensen, H.M., Russian nuclear forces, 2003, *Bull. Atom. Sci.,* 59 (4), 70–72, 2003.
2. Pelton, R.Y., *The World's Most Dangerous Places*, 4th ed., Harper Resource, New York, 2000, 783.
3. Kotkin, S., *Armageddon Averted: The Soviet Collapse 1970–2000*, Oxford University Press, Cambridge, United Kingdom, 2001.
4. Allison, G., *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, Henry Holt, New York, 2004.
5. Pan, E., Nonproliferation: The Pakistan Network, Council on Foreign Relations, Feb. 12, 2004, http://www.cfr.org/publication/7751/
6. Williams, P.L., *The Dunces of Doomsday*, WND Books, Nashville, TN, 2006, 116–119.
7. *Who is Ayman al-Zawahri*, MSNBC.com, http://www.msnbc.msn.com/id/4555901/
8. Sublette, C., *Alexander Lebed and Suitcase Nukes*, NuclearWeaponArchive.org, May 18, 2002, http://nuclearweaponarchive.org/News/Lebedbomb.html
9. Center for Nonproliferation Studies, *Suitcase Nukes: A Reassessment*, Monterey, California, Sept. 23, 2002.
10. *Al-Qaida nukes already in U.S.*, WorldNetDaily.com, Jul. 11, 2005, http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=45203
11. Miraj, N., Al Qaeda nukes may have reached US shores, *Frontier Post* (Islamabad) Nov. 10, 2001.
12. York, D.L., Nuclear Proliferation Resistance, International Conference on Emerging Nuclear Energy Systems, Belgian Nuclear Research Center, Brussels, Belgium, Aug. 21–26, 2005.
13. Yongbyon [Nyongbyon], Weapons of Mass Destruction, GlobalSecurity.org: http://www.globalsecurity.org/wmd/world/dprk/yongbyon.htm
14. Hecker, S.S., Visit to the Yongbyon Nuclear Scientific Research Center in North Korea, statement before the Senate Committee on Foreign Relations, 108th Congress, Second Session, January 21, 2004.
15. Niksch, L.A., North Korea Nuclear Weapons Program, Congressional Research Service (CRS) Issue Brief for Congress, IB91141, CRS, Washington, D.C., Aug. 23, 2003.
16. http://www.fas.org/nuke/guide/iran/facility/bushehr.htm
17. http://www.globalsecurity.org/wmd/world/iran/bushehr.htm
18. Operation Teapot: 1955-Nevada Proving Ground http://nuclearweaponarchive.org/Usa/Tests/Teapot.html
19. Plans Chapter 6 of the ITER Technical Basis Plant Description Document G A0 FDR R1.0, Jul. 13, 2001, http://www.iter.org/ITERPublic/ITER/ PDD5.pdf

20. York, D.L., Proliferation Resistance: Issues Concerning the Commercialization of Fusion Power and the Z-Pinch Fusion Power Plant, White Paper, Sandia National Laboratories, 2005.
21. Missile Proliferation, Globalized Insecurity, and Demand-Side Strategies, Project Ploughshares Briefing 01/4. http://www.ploughshares.ca/libraries/Briefings/brf014.html
22. Currie, D., Non-Proliferation under Security Council Resolution 1540, May 5, 2004, http://www.globelaw.com/Nukes/NonProliferation/NonProlif%20 Res% 201540.htm
23. Braun, C. and Chyba, C.F., Proliferation rings: new challenges to the nuclear nonproliferation regime, *Int. Secur.* 29 (2), 5–6, 2004.
24. Fight on WMDs Boasts Global Backing, *Washington Times*, Dec. 23, 2004.
25. Libyan Inspections Find Evidence of Collaboration with Egypt, WorldTribune.com, Mar. 29, 2004, http://216.26.163.62/2004/me_egypt_03_29.html
26. Benjamin, D. and Simon, S., The Age of Sacred Terror: Radical Islam's War against America, 2003, pp. 203–204.
27. Ukraine Reportedly Sold Nuclear-Capable Cruise Missiles to China, Iran, Missile Threat.com, http://www.missilethreat.com/news/200502020231.html
28. Missiles Sold to China and Iran, *Washington Times*, Apr. 6, 2005.
29. *Nuclear Weapons Test Map*, PBS.org: http://www.pbs.org/wgbh/amex/bomb/maps/index.html
30. Weapons of Mass Destruction: Brazil, GlobalSecurity.org: http://www.globalsecurity. org/wmd/world/brazil/nuke.htm
31. Roots of Nuclear Proliferation, *PakTribune*, Tuesday, May 30, 2006, http://www.paktribune.com/news/index.php?id=145249
32. Argentina: From Tracking Nuclear Proliferation 1998, Carnegie Endowment for International Peace: Non-Proliferation, http://www.ceip.org/programs/npp/nppargn.htm
33. The State of Nuclear Proliferation, ArmControl.org., http://www.armscontrol.org/factsheets/statefct.asp
34. Gsponer, A. and Hurni, J.-P., ITER: The International Thermonuclear Experimental Reactor and the Nuclear Weapons Proliferation Implications of Thermonuclear-Fusion Energy Systems, Independent Scientific Research Institute, ISRI-04-01.
35. Kang, J., Suzuki, T., and Hayes, P., South Korea's Nuclear Mis-Adventures, Nautilus Institute, Sept. 10, 2004.
36. Koch, L., Criteria to Assess the Proliferation Resistance of Nuclear Fuel Cycles, European Institute for Transuranium Elements (Germany), http://www.mi.infn.it/~landnet/Doc/Reactors/koch.pdf
37. Kapisthalam, K., Pakistan: Nuclear Trader, Islamist Swamp, FrontPage Magazine.com, Dec. 15, 2003, http://frontpagemag.com/Articles/ReadArticle.asp?ID=11298

38. Edwards, R., Krypton clue to North Korean nuclear progress, *New Scientist*, 2003, http://www.newscientist.com/article.ns?id=dn3960
39. Farr, W.D., The Third Temple's Holy of Holies: Israel's Nuclear Weapons, The Counter Proliferation Papers, Future Warfare Series No. 2, USAF Counter proliferation Center, Air War College, Sept. 1999, http://www.fas.org/nuke/guide/israel/nuke/farr.htm
40. York, D.L., Illicit Trafficking of Radiological and Nuclear Materials: Modeling and Analysis of Trafficking Trends and Risks, International Nuclear Materials Management Conference, IAEA, Vienna, Austria, Mar. 2005.
41. Nuclear Threat Initiative (NTI), Research Library, http://www.nti.org/db/nistraff/2005/20050160.htm
42. The Legacy Story, U.S. Dept. of Energy, http://legacystory.apps.em.doe.gov/text/link/link1.htm
43. Daalder, I.H. and Lindsay, J.M. Nuclear Wal-Mart? *The American Prospect*, Sept. 1, 2003.
44. Zimmermann, T. and Cooperman, A., The Russian Connection, *U.S. News & World Report*, Oct. 23, 1995, http://www.alternatives.com/crime/berryl.html
45. KH-55 GRANAT—AS-15 KENT, Russian Federation Missiles, http://www.softwar.net/rfed.html
46. 'Terrorist' NGO has nuclear weapons connection, *Asia Times Online*, atimes.com, Oct. 27, 2001, http://www.atimes.com/ind-pak/CJ27Df01.html
47. Escobar, P., The roving eye: anatomy of a 'terrorist' NGO, *Asia Times Online*, atimes.com, Oct. 26, 2001, http://atimes.com/c-asia/CJ26Ag01.html
48. Williams, P.L., *The Al Qaeda Connection: International Terrorism, Organized Crime, and the Coming Apocalypse*, Prometheus Books , 2005, 106–116.
49. Williams, P.L., *Osama's Revenge: The Next 9/11*, Prometheus Books, 2004, 134–137.
50. Broad, W.J., Sanger, D.E., and Bonner, R., A Tale of Nuclear Proliferation, *New York Times*, Feb. 12, 2004.
51. China's Weapons—Bought and Sold—Are a Threat, NewsMax.com, http://www.newsmax.com/archives/articles/2005/4/11/90752.shtml
52. Sanger, D.E. and Broad, W.J., From Rogue Nuclear Programs, Web of Trails Leads to Pakistan, *New York Times*, Jan. 4, 2004.
53. Albright D. and Hibbs, M., Pakistan's bomb: out of the closet, *Bull. Atom. Sci.,* 48 (4), 38–43, 1992.
54. Fidler, S. and Huband, M., Turks and South Africans Helped Libya's Secret Nuclear Arms Project, *Financial Times*, Jun. 10, 2004.
55. Fidler, S., Turkish Businessman Denies Nuclear Goods Claim, *Financial Times*, Jun. 11, 2004.
56. Bonner, R., Salesman on Nuclear Circuit Casts Blurry Corporate Shadow, *New York Times*, Feb. 18, 2004.

5 Nuclear Capabilities of North Korea: Issues in Intelligence Collection, Analysis, and National Security Policy

THOMAS A. JOHNSON

Contents

North Korea's development of both its missile technology and nuclear programs requires careful response not only from the U.S., but also the world community. The engagement of diplomatic discussions has a very profound effect on each of the impacted nations, namely North Korea, South Korea, U.S., China, Japan, and Russia. Additionally, the United Nations and other member states will all be impacted by the resolution of whether North Korea becomes a member of the nuclear community or relinquishes its efforts to obtain nuclear weapons.

Indeed, the question for a number of years has been whether North Korea actually possesses nuclear weapons, and if so, how many? This question was recently addressed by North Korea leader Kim Jong-Il in which he has stated that North Korea does possess nuclear weapons and that they have developed these weapons for defensive purposes.

To fully appreciate the current situation, we must review the major historical events that have led to this current crisis. At the conclusion of World War II, we found Europe in total disarray and the nations that would, in a few subsequent years, become major players in the 1950 Korean War were China, the Soviet Union, the U.S., the Chinese Nationalists under Chiang Kai Shek (Taiwan), and Korea, which was split between the North led by Kim II Sung and Syngman Rhee from the South.[1] So the Korean War, which occurred in 1950 and did not result in a victory for either side or a treaty and ended by an armistice in July of 1953, has in effect resulted in a continued stalemate for over a half of a century.

This chapter will present and build on the major issues occurring within a timeline that begins in 1950 with the invasion of South Korea by troops from North Korea. Other major actions that will be reviewed include the capture of the U.S.S. Pueblo in 1968, the Agreed Framework in 1994, the end of the Agreed Framework in 2003, and the current state of resolving this crisis. This background will assist the reader in appreciating the difficulty of forging a diplomatic solution, due to the several nations involved and their incompatible positions

An overview of the issues and timeline is presented in the following chart.

Event	Timeline
Korean War	1950–1953
U.S.S. Pueblo	1968–1969
North Korean Nuclear Programs	1960–1993
The 1994 Agreed Framework	1994–2003
North Korea's Missile Program	Current crisis
Multilateral—six-party nation positions	Preparing for diplomatic discussions
National Security Policy Ramifications	Current position posture
National Security Policy Decision Framework	Future decision

The U.S. will draft its national security policy on the basis of information collected, analyzed, and produced by our all-source intelligence community. The ability to collect information on North Korea has been exceptionally difficult and while the CIA has regarded North Korea as possessing from two to six nuclear weapons, we must be concerned with North Korea's capability to mate nuclear warheads with missiles capable of attacking the U.S. and one of our allies, namely Japan.

As the U.S. attempts to secure a diplomatic solution, we must also be prepared for exercising a military option, which could be expressed in terms

of a defensive posture under the Bush Doctrine of Preventative Action. An additional concern is whether North Korea has provided nonstate organizations, such as Al-Qaeda, with nuclear materials or whether we wish to chance that in the future they will provide terrorist organizations the nuclear materials for use against the U.S. or its allies.

As our nation formulates plans and policies to respond to the nuclear capabilities of North Korea, we rely on our intelligence process to provide insights and clarity as to the actual state of events within North Korea. The collection of data and information by our highly sophisticated collection disciplines must be analyzed with the full knowledge that our human intelligence in North Korea is virtually nonexistent, thus we can develop only partial insights into the North Korean nuclear program. This is further exacerbated by the fact that North Korea has built much of its nuclear capabilities underground, protected from our spy satellites. Therefore, this production of intelligence documents is at best, most fragmentary, and devoid of the totality of facts required that help guide our decision makers in formulating the carefully thought through policies so necessary to address the crisis created by North Korean nuclear and missile programs.

The Korean War (1950–1953)

We will leap over 13 centuries of Korea's history and begin our assessment of North Korea's potential nuclear threat capabilities by tracing events surrounding the beginning of the Korean War. Throughout its history, Korea has been invaded by its larger neighbors, and Japan formally annexed Korea in 1910. Japan remained in total control until the end of World War II. It was at the Yalta Conference, in 1945, that a four-power trusteeship was designed for Korea. However, with the surrender of Japan, the U.S. and the Soviet Union fixed the surrender of Japanese troops at the 38th parallel, with U.S. forces south of the 38th parallel and Soviet forces north of the line. By 1948, two different governments were inaugurated on the Korean Peninsula, fixing for the first time South Korea and North Korea. On August 15, 1948, the Republic of Korea (ROK) was established and Syngman Rhee became the republic's first president, in what is really South Korea. Shortly after this event, on September 9, 1948, the Democratic Peoples Republic of Korea (DPRK) was established in the North under Kim II Sung.[2] In less than 9 months, fighting between the South Korean forces and North Korean forces would begin in what historians regarded as a battle started by the South. By June 25, 1950, North Korean forces began an attack that crossed the 38th parallel and resulted in the U.S. committing troops as part of a United Nations "police action" team and this was the beginning of the Korean War, which continued

until truce talks began in July of 1951 and the fighting continued until July of 1953, when the conflict ended in a cease fire agreement.

Documents uncovered after the fall of the Soviet Union revealed that both the Soviet Union and China were aware and even supportive of North Korea's invasion plans in 1949. Another important facet of this "police action" occurred in October 1950, when China's Mao Tse Tung feared that General Douglas MacArthur would lead the allies through North Korea and into China.[3] As a result, China sent 300,000 combat troops into battle and totally changed the dynamics of this war.

By 1953, almost 900,000 soldiers had died and more than 2 million civilians had been killed or wounded. The Korean War split up the families of more than 7 million people, as a result of the nation being divided at the 38th parallel.[4]

It is important to note that over half a century later, China, Russia, Japan, and the U.S. are all still enmeshed in the conflict between North and South Korea. Economic and political interests on all sides make the resolution of this situation very difficult, as we shall point out in this chapter.

The U.S.S. Pueblo (January 23, 1968–February 5, 1969)

Twenty-five years after the Korean War, the U.S. once again encountered a major military event with North Korea when the U.S.S. Pueblo was captured by North Korean naval forces. The significance of this event was that the U.S.S. Pueblo was a U.S. Navy Intelligence Collection ship in international waters. Also significant was the fact that the U.S. was, at the time, engaged and preoccupied with a war in Vietnam and as a result, had limited options to rely on in our effort to free the 82 men captured by North Korea. Today, as we confront North Korea's potential for developing missiles and nuclear weapons, we have an opportunity to draw lessons from the Pueblo crisis. We are once again facing a challenge from North Korea at a time when we are preoccupied with our efforts to restore peace in Iraq and with substantial unrest throughout the Middle East. Then, as now, we have to rely on the intelligence community to provide information to aid our commanders and decision makers. In the Pueblo crisis, we discovered that our intelligence community provided uneven support. For example, the intelligence community was puzzled as to the motivation and intention of North Korea due to the difficulty in understanding the decision-making process of North Korea. Also, intelligence analysts attempted to provide useful reports as to a number of wide-ranging and fundamental questions that decision makers require in crisis situations. In the capture of the U.S.S. Pueblo, these questions were of substantial interest to both the intelligence community and decision makers within all levels of our command structure.

1. What were North Korea's capabilities against South Korea?
2. Was the North Korean army in a defensive or offensive posture?
3. What was North Korea's objective in seizing the U.S.S. Pueblo?
4. Where was the U.S.S. Pueblo?
5. What were North Korea's economic and political vulnerabilities?
6. What if the U.S. attacked?
7. What was the Soviet Union doing?[5]

Ironically, these questions, as applied to North Korea's interest in its nuclear weapons and missile development programs, are still very similar and most perplexing. Of further interest is the parallel between the U.S.S. Pueblo and the July 2006 North Korean launch of a Taepodong-2 missile in which both military and diplomatic options were considered.

In the case of the U.S.S. Pueblo, the National Security Council reviewed military options and also had a Korean Interagency Group consisting of representatives from the State and Defense Departments, the White House, the Central Intelligence Agency, the Agency for International Development, and the U.S. Information Agency. This group was charged with preparing 10 "think papers" for addressing purpose, feasibility, risk, and a North Korean response. These papers covered the following areas:

1. Selected air strikes on North Korea
2. Naval Blockade of Wonson Harbor
3. Mining Wonson Harbor
4. Seizing North Korean vessels
5. Sailing U.S.S. Banner into the area where the U.S.S. Pueblo was captured
6. Recovering cryptographic material jettisoned into the ocean
7. Conducting airborne reconnaissance
8. Informing the Soviets of actual or possible military moves
9. Raiding across the demilitarized zone
10. Economic pressure on North Korea[6]

Although the U.S. never abandoned the option of using military force, it did rely on diplomatic measures, which eventually were successful in releasing the 82 men by December 1968, almost a full year after their capture. The U.S.S. Pueblo was not returned and remains in Wonson Harbor in North Korea to this day. Since the U.S.S. Pueblo incident, we have experienced analogous problems in Tehran, Lebanon, and now, once again, in North Korea.

North Korea Nuclear Programs (1960–1993)

The United Nations International Atomic Energy Commission (IAEC) was founded in 1946, as the first resolution of the General Assembly, calling for the peaceful use of atomic energy and the elimination of weapons of mass

destruction. This evolved into the International Atomic Energy Agency (IAEA) created in 1957, as a result of President Eisenhower's "Atoms for Peace" address to the General Assembly of the United Nations in 1953. In 1956, 81 nations unanimously approved the IAEA statute which outlined the three areas of the Agency's role and mission as nuclear verification and security, safety, and technology transfer.

The IAEA is an independent, intergovernmental, science and technology based organization related to the United Nations system and reports annually to the U.N. General Assembly, and when appropriate, to the Security Council regarding noncompliance by states with their safeguard obligations, as well as on matters relating to internation peace and security. In 1968, the treaty on the Non-Proliferation of Nuclear Weaspons was approved and it froze the number of nuclear weapons states at five, the USA, Russia, UK, France, and China.

North Korea has pursued developing a weapons program that includes nuclear weapons, biological weapons, and chemical weapons. Their major interest clearly is focused on the development of a nuclear weapons program mated with a missile delivery system.

North Korea's nuclear program dates back to 1962, and by the mid-1960s, they established a large-scale atomic energy research complex in Yongbyon along with trained specialists who studied in the Soviet Union. Under a cooperative agreement between the Soviet Union and North Korea, a nuclear research center was constructed and by 1965 a Soviet IRT-2 megawatt (MW) research reactor was assembled for this center. During the early 1970s, North Korea focused its efforts on the nuclear fuel cycle, which included refining, conversion, and fabrication. By 1974, North Korean specialists independently modernized the Soviet IRT-2 MW research reactor, bringing its capacity up to 8 MW and switching to fuel enriched to 80%. During this same time period, North Korea began to build a 5 MW research reactor. By 1980, the focus was on the operation of facilities for uranium fabrication and conversion, and construction was started on a 200 MW nuclear reactor and nuclear reprocessing facilities in Taechon and Yongbyon. During the mid-1980s, high explosive detonation tests were completed.[7]

In 1977, North Korea concluded an agreement with the International Atomic Energy Agency (IAEA), permitting the IAEA to inspect the nuclear research reactor, which was built with the assistance of the Soviet Union. Eight years later, in 1985, under intense international pressure, North Korea acceded to the Treaty on the Nonproliferation of Nuclear Weapons. However, North Korea refused to sign a safeguards agreement with the International Atomic Energy Commission, an obligation it had as a party to the Nuclear Nonproliferation Treaty. By 1991, the joint declaration on denuclearization was initiated and this prohibited both North Korea and South Korea from testing, manufacturing, producing, receiving, possessing, storing, deploying,

or using nuclear weapons and prohibited the possession of nuclear reprocessing and uranium enrichment facilities.[8]

In 1992, North Korea finally signed a nuclear safeguards agreement with the International Atomic Energy Commission. This safeguards agreement allowed IAEA inspections to begin in June of 1992. However, in March 1992, the North–South Joint Nuclear Central Commission was established, but agreement was not reached on establishing a bilateral inspection protocol, so once again, tension began to build as to North Korean motives in its nuclear program. Concern over North Korea's nuclear program became a major issue between North and South Korea and now tension began to build between the U.S. and North Korea as well. The situation came to a head in January 1993 when North Korea refused the International Atomic Energy Inspectors access to two suspected nuclear waste sites and then announced in March 1993 its intent to withdraw from the Nonproliferation of Nuclear Weapons Treaty.[9]

The IAEA declared North Korea to be in noncompliance with the Nonproliferation Nuclear Weapons Treaty on April 1, 1993, and on April 2, 1993, the IAEA referred the North Korean violations of the treaty to the United Nations Security Council. On April 7, 1993, the IAEA issued a formal censure on North Korea for its noncompliance with the Nuclear Nonproliferation Treaty, the first censure in the history of the IAEA. On May 11, 1993, the United Nations Security Council passed a resolution asking North Korea to allow IAEA inspections under the NPT, and on May 12, 1993, North Korea rejected the request of the United Nations Security Council and refused access to any of its sites to IAEA inspectors.[10] All of this activity and tension regarding inspection refusal by North Korea not permitting IAEA inspectors access to appropriate sites ultimately led to the negotiations among North Korea, South Korea, Japan, and the U.S. and resulted in the Agreed Framework of 1994.

The 1994 Agreed Framework

In October 1994, an Agreed Framework was signed by the U.S. and North Korea in Geneva, thus freezing North Korea's nuclear program at its Yongbyon nuclear complex and also the operation of its plutonium reprocessing facility. North Korea also agreed to fully disclose its past nuclear activities and open its facilities to the IAEA inspectors. The U.S. agreed to provide heavy fuel oil to North Korea and to assume a leadership role in the multinational project to build two light water reactors so as to assist North Korea in meeting its energy needs. In fact, these light water reactors were to replace the graphite-moderated reactors, which would have permitted production of weapons-grade plutonium. Also required under this agreement was a mutual commitment to work together to achieve a nuclear-free Korean Peninsula and to strengthen the international nuclear nonproliferation program. Finally, both the U.S.

and North Korea agreed to move toward normalization of political and economic relations.[11]

The year and a half it required to negotiate the 1994 Agreed Framework was not uneventful time as the agreement encountered problems by December 1995 because North Korean officials refused to accept the South Korean design of the light water reactors. After 6 months of negotiation, the design was accepted. North Korea signed an agreement for the light water reactors, with the Korean Peninsula Energy Development Organization (KEDO) whose members were Japan, South Korea, and the U.S. South Korea, which promised to bear most of the cost of the project, which was estimated at $4.5 billion, asked the U.S. to assist in the cost. The U.S. declined on the basis that Congress had not appropriated the necessary budget. South Korean and U.S. officials encountered additional difficulties as Japan felt its significant monetary contribution of $1 billion toward the light water reactors (with only part of the money being spent on Japanese nuclear materials) was less than it expected. Another problem that emerged was how the three countries would finance the provision of heavy fuel oil shipments to North Korea. While the U.S. agreed to bear the cost of this fuel oil, it was having difficulty with congressional authorization due to other large financial commitments of the U.S.

In 2002, the U.S. Intelligence Community concluded that North Korea had undertaken a covert uranium-enrichment program that was initiated in the late 1990s, as an alternative source of fissile material to substitute for the plutonium reprocessing activities frozen under the 1994 Agreed Framework. This alternative path to developing nuclear weapons by use of a new source of fissile material was an action by North Korea that violated the 1994 Agreed Framework in which both sides pledged to keep the Korean Peninsula free of nuclear weapons. President George W. Bush authorized Assistant Secretary of State James Kelly to inform North Korean officials of our intelligence finding. The initial reaction by North Korea was to deny the allegation and when confronted with further evidence, the North Korean First Vice Minister of Foreign Affairs Kang Sok Ju admitted the existence of a clandestine nuclear weapons program, but asserted their sovereign right to develop nuclear weapons and "more powerful things as well." Furthermore, Kang also stated North Korea intended to terminate the Agreed Framework.[12]

Government officials in both North Korea and the U.S. were dissatisfied with the 1994 Agreed Framework, but for different reasons. North Korea complained repeatedly that the U.S. was not keeping on schedule with the completion of the light water reactors, and the U.S. stated the North Koreans were not in compliance with reporting their prior nuclear weapons activities. In fact, Jonathan Pollack goes on to suggest the following:

> Neither government saw compelling reasons to sustain the 1994 accord. The intelligence findings thus enabled both governments to

> deem their prior obligations null and void. With both countries putting forward maximal nonnegotiable policy positions, the subsequent collapse of the Agreed Framework was virtually foreordained…[13]

While the Clinton Administration, led by Ashton Carter, William Perry, and Madeline Albright, created the 1994 Agreed Framework, they only concluded this appropriate as an alternative to the military option that they were convinced would result in a full scale war on the Korean Peninsula. The aim of the 1994 Agreed Framework was to control the nuclear weapons development that North Korea was pursuing. The challenge for President Clinton in 2000 was to also create an Agreed Framework for missile defense. This did not occur in 2000, principally due to the end of President Clinton's term in office as it would have entailed protracted negotiations of considerable complexity and time. Also, the request for a presidential visit to North Korea was becoming an implicit expectation in the negotiations between the representatives of both nations, and President Clinton was not inclined to go to North Korea given the totality of circumstances existing at the time. Consequently, the problem of concluding a Treaty or an Agreed Framework for missiles remains today a major problem for the international community, especially if the nuclear bombs that the U.S. believes North Korea possesses are mated with the three-stage Taepodong-2 missile.

North Korea's Missile Programs

The current focus of North Korea is to continue testing its Taepodong-2 missile and this is precisely the concern of the international community, which on July 15, 2006 resulted in the United Nations Security Council reaffirming its resolutions 825 (1993) of May 11, 1993 and 1540 (2004) of April 28, 2004, bearing in mind the importance of maintaining peace and stability on the Korean Peninsula and in Northeast Asia at large.

- Reaffirming that proliferation of nuclear, chemical, and biological weapons, as well as their means of delivery, constitutes a threat to international peace and security.
- Expressing grave concern at the launch of ballistic missiles by the DPRK, given the potential of such systems to be used as a means to deliver nuclear, chemical, or biological payloads.
- Registering profound concern at the DPRK's breaking of its pledge to maintain its moratorium on missile launching, expressing further concern that the DPRK endangered civil aviation and shipping through its failure to provide adequate advance notice.
- Expressing its grave concern about DPRK's indication of possible additional launches of ballistic missiles in the near future.

- Expressing also its desire for a peaceful and diplomatic solution to the situation and welcoming efforts by Council members as well as other Member States to facilitate a peaceful and comprehensive solution through dialogue.
- Recalling that the DPRK launched an object propelled by a missile without prior notification to the countries in the region; this fell into the waters in the vicinity of Japan on August 31, 1998.
- Deploring the DPRK's announcement of withdrawal from the Treaty on Nonproliferation of Nuclear Weapons (the Treaty) and its stated pursuit of nuclear weapons in spite of its Treaty on Nonproliferation of Nuclear Weapons and IAEA safeguards obligations.
- Stressing the importance of the implementation of the Joint Statement issued on September 19, 2005 by China, DPRK, Japan, ROK, the Russian Federation, and the U.S.
- Affirming that such launches jeopardize peace, stability, and security in the region and beyond, particularly in light of the DPRK's claim that it has developed nuclear weapons.

Acting under its special responsibility for the maintenance of international peace and security, July 5, 2006 local time:

1. Condemns the multiple launches by the DPRK of ballistic missiles on July 5, 2006 local time.
2. Demands that the DPRK suspend all activities related to its ballistic missile program and in this context re-establish its pre-existing commitments to a moratorium on missile launching.
3. Requires all Member States, in accordance with their national legal authorities and legislation and consistent with international law, to exercise vigilance and prevent missile and missile-related items, materials, goods, and technology being transferred to DPRK's missile or WMD programs.
4. Requires all Member States, in accordance with their national legal authorities and legislation and consistent with international law, to exercise vigilance and prevent the procurement of missiles or missile related-items, materials, goods and technology from the DPRK, and the transfer of any financial resources in relation to DPRK's missile or WMD programs.
5. Underlines, in particular to the DPRK, the need to show restraint and refrain from any action that might aggravate tension and to continue to work on the resolution of nonproliferation concerns through political and diplomatic efforts.
6. Strongly urges the DPRK to return immediately to the six-party talks (China, DPRK, Japan, ROK, Russia, and the U.S.) without precondition, to work toward the expeditious implementation of September 10, 2005 Joint Statement, in particular to abandon all nuclear weapons and

existing nuclear programs, and to return at any early date to the Treaty on Nonproliferation of Nuclear Weapons and IAEA safeguards.
7. Supports the six-party talks, calls for their early resumption, and urges all the participants to intensify their efforts on the full implementation of the September 19, 2005 Joint Statement with a view to achieving the verifiable denuclearization of the Korean Peninsula in a peaceful manner and to maintaining peace and stability on the Korean Peninsula and in Northeast Asia.
8. Decides to remain seized of the matter.[14]

The history of North Korea's missile program is premised on the fact that missiles are one of their major exportable items in an economy that has few commodities of interest to other noted states and groups. Not only does North Korea produce missiles for sale, and for their own military use, but they also use their missile technology to trade for other technical skills and products for their nuclear development program. In fact, Seymour Hersh reports that one of North Korea's main sources of export income is arms sales and their most sought after products are their missiles. Also in 1997, according to the CIA, Pakistan paid North Korea with warhead design, weapons testing data, and other nuclear weapons secrets in return for missiles.[15]

The clear purpose for North Korea continuing development of their Taepodong-2 missile is this missile would provide the three-stage capability needed to attain an orbit that would put the U.S. within their target range. A nation that possesses nuclear, biological, and chemical weapons only needs a sufficiently powerful ballistic missile to acquire a capability for mating the weapons with the missile and then possessing a most intimidating weapon system. Clearly, Japan is concerned about North Korea's combined weapons and missile capability as is Taiwan, South Korea, and the U.S.

The patented sale of missiles or plutonium or enriched uranium to terrorist's organizations or other nations and states in the Middle East is also a troubling development. The attached chart depicts an unclassified sampling of several types of ballistic missiles in the North Korean inventory.

North Korean Ballistic Missiles

NK Name Alternate Name	Range (km)	Payload (kg)
Scud-B	300	987–989
Scud-C	500	770
Scud-D	700	500
Nodong	1000	700
Paektusan-1	2200	204
Taepodong-1	2200	204
Taepodong-2	4000–10000	907

The Taepodong missile was named by U.S. intelligence analysts after U.S. reconnaissance satellites first discovered North Korea's long range missile. Since we did not know the Korean name for their missile, we named it Taepodong as this was the area in Korea where they were observed. However, the North Korean name for their long range satellite is Paektusan in honor of their highest mountain. So, we may use the names Paektusan-1 or 2 interchangeably with Taepodong-1 or 2 because it represents the same missile.

The range of the Taepodong-2 missile has been estimated to be 4000 km and within range of striking Alaska. The payload weight factor is another important variable in its effectiveness. Although the July 5, 2006 missile test of the Taepodong-2 was considered a failure, the opportunity for North Korea to improve on its capabilities is very possible.

The resolution of the United Nations Security Council urging continued six-party negotiations is important, and it is most distressing that North Korean UN Ambassador Pak Gil Yon rejected the resolution and stated North Korea intends to continue missile launches and then offered the following statement:

> The delegation of the Democratic People's Republic of Korea resolutely condemns the attempt of some countries to misuse the Security Council for the despicable political aim to isolate and put pressure on the DPRK and totally rejects the resolution . . . The Korean People's Army "will go on with missile launch exercises as part of its efforts to bolster deterrent for self-defense in the future, too, . . .
>
> Pak warned that North Korea will "take stronger physical actions of other forms should any other country dare take issue with the exercises and put pressure on it."[16]

The international community will face another challenge when North Korea attempts to test its Taepodong-2 missile again. And the possible use of a military strike on this missile either in flight or just prior to its launch has enormous significance for both Japan and South Korea. Needless to say, the next phase will have to consist of diplomacy so that a military option can be minimized.

Multilateral Six-Party Nation Positions

One of the major issues that have disturbed North Korea is the U.S. refusal to engage in bilateral negotiations with North Korea. The George W. Bush Administration has taken the position that multilateral, six-party negotiations are the correct way to proceed and this has met with discouragement by some members of the six-party negotiation team. Both Russia and China have expressed concerns on this point to the Bush Administration. The response of the administration is premised on four points.

First, since the North Korean Nuclear Weapons program affects the security of all states in the region — as well as potentially other regions of the world — the regional powers must all have a voice in and take responsibility for resolving this issue. Second, since none of North Korea's neighbors wants the North to acquire nuclear weapons, a multilateral forum would allow these states to exert additional pressure on the North to abandon its program. Third, having participated in negotiations, America's partners would have an obligation to assist in the enforcement of any agreements. Finally, the multilateral approach could get around the constraint created by congressional unwillingness to provide funds for North Korea.[17]

While the U.S. and North Korea have each expressed its views toward either bilateral or multilateral negotiations, the remaining four nations each have views that are important to consider.

South Korea, for example, has favored a bilateral policy of direct negotiations between the U.S. and North Korea. It has also expressed its view for a "sunshine" policy that would open the economic process between North and South Korea, eventually considering a policy of eventual reunification. One of the reasons that South Korea is interested in opening the economic ties to the North is directly related to its concern as to how great the financial costs will be once reunification occurs.

Since North Korea's economic system has virtually collapsed, South Korea knows the costs of incorporating the vast economic needs of North Korea will be staggering. A parallel example was the economic cost involved in the reunification of Germany, which was approximately $2 trillion. This burden on the German economy has contributed to great economic distress over the past few years for the former West Germany, which reunified the collapsed East Germany.[18]

Japan is quite concerned for its safety as Nodong missiles are aimed directly at its country. Also, the first Taepodong-1 missile landed in the Sea of Japan, so the Japanese are clearly interested in negotiating a framework to contain North Korea's nuclear program. Their fear centers on how close and vulnerable they are to an attack by North Korea. Therefore, Japan and South Korea have urged caution on the U.S. and made clear that they do not favor the U.S. activating a preemptive military strike against North Korea's nuclear weapons facilities.

Russia has significant economic and strategic interests on the Korean Peninsula with ambitious plans to establish greater economic links with South Korea, using North Korean territory to transship its supply of natural gas to both Asia and Europe by means of the trans-Siberian railroad. While President Vladimir Putin is firmly opposed to North Korea becoming a nuclear weapon state, that question can only be viewed in terms of limiting North Korea's missile program since North Korea already possesses nuclear

weapons, by all accounts. Another concern that both Russia and China share is their fear of military activities or that a sudden collapse of the North Korean government might flood each of their countries with starving North Korean refugees, who will greatly impact each of their economic systems.[19]

China already has an estimated 200,000 to 300,000 North Koreans living within its borders, and any military activities would further stress its economic goals not only for supporting additional refugees, but also for the economic harm done to one of its largest trading partners, South Korea. China also wants the Korean Peninsula to remain a viable entity for its continued trading with Japan. China worries about the nuclearization of Northeast Asia with South Korea, Japan, and Taiwan all developing nuclear weapons capabilities. China simply does not want military activities in the Korean Peninsula for fear it would bring the U.S. into the area, as it now enjoys North Korea as a buffer zone to its borders.[20]

China has urged North Korea to reverse its nuclear weapons program and the U.S. to engage in bilateral discussions with North Korea to return to the 1994 Agreed Framework. In fact, China, which is the key player in these negotiations, having the most influence over North Korea, has stated its position on the issue by emphasizing three main points:

1. Peace and stability on the Korean Peninsula should be preserved.
2. The peninsula should remain nuclear free.
3. The dispute should be resolved through diplomatic and political channels.[21]

While each of these countries has expressed their views as to the direction a strategy of negotiation might follow. We also should make note of a Gallup Korea survey that reveals some rather startling perceptions South Koreans have of their five major negotiating partners.

It is evident that the South Korean–U.S. Alliance which has been successful for over 50 years, is now revealing signs of strain. If the alliance is not strengthened, the U.S. could lose one of its long-term allies in the Northeast Asia region.

One indicator of strained relations between the ROK and the U.S. is the rise in anti-American sentiment among South Koreans. A Gallup Korea survey conducted in December 2002 shows South Korean perceptions of the U.S. relative to other nations.[22]

The Republic of Korea (ROK)–U.S. Alliance

Feelings	U.S.	Japan	Russia	China	North Korea
Positive	37.2	30.3	36.7	55	47.4
Do not know	9.1	11.1	11.8	21.4	39.2
Negative	53.7	58.6	61	23.6	24.1

The survey indicates that South Koreans view North Korea and China more favorably than their longtime ally, the U.S. In fact, the negative ratings of South Koreans' views of the U.S. are more than twice as high as their view of North Korea. This may well be attributed to the number of incidents in which members of our military have become embroiled in criminal acts against citizens of South Korea. The interest for renewed reconciliation between the North and South is also viewed by many South Korean citizens as another reason for not needing the U.S. military within their country. Indeed, some views in South Korea have expressed the concern that the presence of the U.S. military serves the needs of the U.S. for basing military assets with access to the Northeast Asia corridor, as opposed to any genuine role that would be ultimately useful to the reintegration of both North and South Korea. Some views even hold the proposition that the presence of U.S. military within South Korea precludes the opportunity for any effort at reconciliation between the North and South and that the continued presence of U.S. military makes South Korea a target for eventual military action by North Korea.

National Security Policy Ramifications

It is apparent that there is little consensus among the six-party nations in how best to negotiate the crisis that North Korea has presented by virtue of its nuclear weapons program. South Korea, Russia, Japan, and China are of the opinion that the U.S. should negotiate directly with North Korea, as this would reduce the tension and minimize the outbreak of military activities. The U.S. view is that a bilateral negotiated deal would not necessarily eliminate North Korea's nuclear weapons and missile capability. As a matter of fact, the 1994 Agreed Framework did not address the question as to whether North Korea had already processed enough plutonium to make nuclear weapons prior to the implementation of the Agreed Framework.[23]

The current crisis that focuses on the North Korean Taepodong-2 missile launch really was created by U.S. intelligence discovering and confronting North Korea with evidence of its covert uranium enrichment program, which is a second path to the development of nuclear weapons and in violation of the 1994 Agreed Framework signed by North Korea. The problem confronted by the U.S., South Korea, China, Russia, and Japan centers on the collective inability to really know what North Korea's nuclear intentions are and this makes it most difficult to formulate a policy that could be articulated through a process of diplomatic negotiations. Phillip C. Saunders suggests several useful scenarios, which should be considered in assessing North Korea's nuclear intentions.

1. North Korean leaders have decided that nuclear weapons are essential to their security.
2. North Korean leaders are willing to negotiate their nuclear and missile programs away for a deal that guarantees their security and sovereignty.
3. North Korean leaders want both nuclear weapons (as an ultimate security guarantee) and better relations with the U.S., Japan, and South Korea.
4. North Korean leaders/factions disagree about whether nuclear weapons or a negotiated agreement with the U.S. is the best way to achieve security.
5. North Korean leaders seek nuclear weapons and ballistic missiles to enable offensive actions against South Korea.[24]

Given this range of alternatives, one can quickly see how difficult it is to formulate a policy and to then coherently apply it across the Six-Nation Party to this crisis. To further complicate this process, documented proof exists as to the North Korean violation of the 1994 Agreed Framework and this generates little confidence they will comply and honor new agreements. Verification and inspection agreements could take months to prepare and the implementation of inspection processes to assure compliance would have to be bound by sanctions for any violation. China, on July 15, 2006, has already gone on record as opposing sanctions in the recent United Nations Security Council Resolution. The difficulties confronting the creation of policies, which may provide the foundation for developing a multilateral negotiation process, are enormous.

In addition to the framing of policies for diplomatic negotiation, the development of policies to guide military options also must be considered. The question is whether this will entail a process seeking United Nations Security Council approval with the realization of veto power by any member of the Security Council impacting a decision to invoke military options. Also, do military preparations include an international peacekeeping force or are more limited joint force agreements to be considered? Another factor to consider is the range of military options that may be available from naval blockades, to, and including, military strikes.

Our intelligence community has informed us that North Korea has at a minimum, two nuclear bombs, an enormous stockpile of both chemical and biological weapons, and missiles capable of attacking both South Korea and Japan. Furthermore, North Korea has stated that they possess nuclear weapons and, if their missiles are intercepted, they will attack.

> The biggest military concern in striking North Korean nuclear facilities is the threat of North Korean counter-attacks. Seoul, the Capitol of South Korea, lies within range of North Korean

> long-range artillery. Five hundred 170 mm Koksan guns and 200 multiple-launch rocket systems could hit Seoul with artillery shells and chemical weapons, causing panic and massive civilian casualties. North Korea has between 500 and 600 Scud missiles that could strike targets throughout South Korea with conventional warheads or chemical weapons. North Korea could hit Japan with its 100 Nodong missiles. Seventy percent of North Korean army ground units are located within 100 miles of the Demilitarized Zone separating North and South Korea, positioned to undertake offensive ground operations. These units could fire up to 500,000 artillery rounds per hour against South Korean defenses for several hours. Finally, if North Korea does have one or two deliverable nuclear weapons, nuclear retaliation (or nuclear threats) would also be available to North Korean leaders.[25]

Phillip C. Saunders also observes that if a successful military strike against North Korea were to occur, the following three issues would be key to its success:

1. Locating all facilities and fissile material stocks that could be used in a nuclear weapons program.
2. Possessing the capability to destroy these targets.
3. Preventing North Korea from retaliating with artillery fire, missile strikes, chemical or biological weapons use, escalation to a full-scale conventional war, or nuclear weapons.[26]

The use of military force to remove North Korea's nuclear weapons and missile capabilities is an extremely difficult and tenuous option. Such a military strike would certainly invite retaliation, and we simply cannot be certain as to where in the underground cave structure of North Korea some of its nuclear weapons may be secreted. Further, even if we were to succeed with military strikes and were able to neutralize North Korea's retaliatory capability, we would still inherit enormous political problems for such actions and, in fact, might encounter a direct military conflict with China. On the other hand, can we or any nation become vulnerable to a nation who possesses nuclear weapons and who could well trade them or make them available to terrorist organizations?

The formation of a policy to address a major international crisis such as this, whether it results in a diplomatic or a military option requires thoughtful and careful preparation. The reliance on our intelligence community to provide our governmental leaders with the most fact-based, well-analyzed findings is critical to our decision-makers' selection of the best options and making the most well-informed decisions possible.

National Security Policy Decision Framework

The challenge for the resolution of the nuclear weapons and missile crisis is for proposing, selecting, and implementing a decision that emerges from one of the three decision frameworks:

1. Engagement
2. Containment
3. Preemptive

The U.S., China, South Korea, Russia, and Japan will have to decide as to which direction they will collectively pursue, so that a realistic option for engaging North Korea has an opportunity of succeeding.

The following summary of the Policy Decision Framework options was prepared by the WMD (weapons of mass destruction) Task Force, Alejandro Ruiz, Coordinator, May 13, 2006 and presented for discussion and analysis regarding an assessment of North Korea's nuclear program.

Engagement

Engagement encourages North Korea to abandon its nuclear ambitions through dialogue and negotiations. A policy of engagement emphasizes the use of diplomatic and economic elements of power over military action, much like the "Sunshine Policy" of former ROK President Kim Dae Jung and the "Peace and Prosperity" policy of the Roh administration.

The primary advantage of an engagement policy is that compared to containment or preemption (which could provide North Korea a rational basis for going to war in the form of a threat to its survival) engagement presents the least near-term risk of triggering provocation from the Kim Jong-Il regime because engagement avoids the conditions that make war a rational act in the eyes of North Korea.

Containment

A second course of action is to pursue a policy of containment.

- Containment seeks to force North Korea to abandon its nuclear ambitions through a series of punitive actions. In other words, North Korea would have to comply with internationally imposed conditions to avoid negative consequences of coercive diplomacy and economic sanctions.
- The goal of a containment policy would be to isolate North Korea to pressure the government to comply with nuclear control regimes.

- A containment policy would emphasize the military element of power (short of preemption), along with coercive diplomacy and further economic sanctions.

The main advantage of containment is it directly addresses the risk presented by North Korea's nuclear weapons today as well as the risk of proliferation in the future through a direct path to resolving the issue. However, this approach presents significant operational and political risks.

The greatest disadvantage of containment is that it may provoke North Korea into taking escalatory or preemptive action. The North Korean regime has mastered the art of brinksmanship and has threatened that a UN Security Council Resolution would be considered an act of war.

Preemptive Action

The third course of action is preemptive action (or preemptive counter proliferation) — military strikes against North Korea's nuclear weapons facilities. Preemptive counter proliferation would include a surprise military attack against North Korea's nuclear weapons and related facilities.

The main advantage of preemptive counterproliferation is that it potentially provides the most direct route to achieving the prompt and verifiable dismantling of North Korea's nuclear weapons programs. This, of course, assumes that any such preemptive action would be successful. Therein lies the main disadvantage — the extraordinary risks associated with this course of action.

Policy recommendations from the Council of Foreign Relations regarding the issues confronting the international community with reference to the North Korean nuclear and missile challenges suggested the following guidelines:

1. Restore relations between South Korea and the U.S. and improve their alliance.
2. Appoint a high level policy coordinator for Korea.
3. Reach an agreed strategy framework for dealing with North Korea.
4. Engage China in efforts with North Korea.
5. Engage in a U.S. bilateral negotiation with North Korea.[27]

Summary

Whether the North Korean nuclear and missile crisis is approached by a Six-Nation Party, or a multilateral, negotiation strategy with a sidebar bilateral negotiation between the U.S. and Korea, as China recommended, it appears that the following results should be the overarching goals of this process.

North Korea

Eliminate its nuclear weapons development program.
Remove from its territory all plutonium and all processed highly enriched uranium.
Removal of materials for a two-path process to nuclear weapons should include all plutonium and enriched uranium both prior to and after the 1994 Agreed Framework.
Rejoin the NPT and permit IAEA inspectors to begin verification programs.
Dismantle the gas-graphite reactors.

United States

Provide assurances that it will not launch any attack on North Korea while legitimate negotiations are underway.
Restore diplomatic relations.

United States, China, Japan, South Korea, and Russia

Provide replacement of conventional power plants, as the nuclear reactors are destroyed.
Begin shipment of 500,000 tons of heavy fuel oil for the year, on a measured basis consistent with North Korea's program efforts.
Open up economic opportunities and trade.
Provide food and medical aid to North Korea.

If these items are not attainable within a specific timeframe in which measured reciprocal objectives occur, there should be pre-established contingency plans that will serve as guidelines for implementing a series of phased actions intended to minimize danger to the world community. These contingency plans should be prepared within a framework of individual and joint nation development and participation, and should include sanctions and measures for applying sanctions, which can include military options.

Perhaps Michael E. O'Hanlon best captures the approach to addressing North Korea where he suggests we should present North Korea with a choice to improve its behavior, reform its country, and engage with the rest of the world in the participation of materials for its people. As we work with North Korea, we would be well advised to focus on substance, not only process, and on core values, not simply technical judgments.[28] In short, it will take a firm but fair and judicious perspective in dealing with the issues presented by the North Korean crisis. Wisdom, judgment, and a commitment to fully bringing resolution to this crisis in a timetable that offers protection and security to the entire world community is needed.

Conclusion

The eventual defusing of the North Korean crisis will require a very coherent and collaborative plan between the Six-Party Nation members involved in this crisis. The elimination of the North Korean nuclear weapons and missile program will not only require an inspection and monitoring program, but also an incentives package that is phased into the program with each nation assuming designated roles and responsibilities. As a result of the North Korean violation of the 1994 Agreed Framework, the plan for both monitoring and inspection will, by definition, have to exceed the normal IAEA protocols for inspection. Additionally, the U.S. intelligence community will have to become more focused and engaged in the North Korean nuclear and missile program, especially relative to its sale of these technologies to other nation–states or terrorist organizations. A joint-force intelligence program between the U.S., Japan, China, Russia, and South Korea should be implemented to assure for an increase in human intelligence to match our scientific collection capabilities. The method and manner of organizing this joint-force intelligence program among the five nations will require careful selection as to assigned roles and responsibilities, especially as it pertains to analysis and reporting responsibilities. Also important to this process will be an agreement among the joint-force intelligence program for the submission of reports that will be politically neutral and fact-based products that are equally designed to provide no one nation any advantage over the five nation coalition.

If the Six-Party Nation is sincere about defusing North Korea's nuclear weapons and missile program, it will require the creation and agreement of a schedule of sanctions for any violations of a new Agreed Framework covering both pathways to a nuclear weapons program and a missile program. The schedule of sanctions must delineate consensus by the five nations and be designed in such a manner to rein in any irresponsibilities by North Korea, while providing incentives for compliance to a new and expanded Agreed Framework covering both nuclear weapons and missiles. The express purpose of the joint-force intelligence program and a realistic schedule of sanctions administered by the five nation enclave will be to avoid the prospect of any individual nation having to use a military option to halt the North Korean nuclear weapons and missile program. However, it is imperative that the U.S. retain the option of selecting a military option should a schedule of sanctions prove unworkable, or should any further egregious violations occur, or should nuclear weapon or missile technology be provided to any other nation or terrorist organization. In the final analysis, the U.S. cannot permit the nuclear weapons and missile technology of North Korea to be less than fully contained. The safety and security of future generations require the U.S. provide a proactive role of sustained engagement

in which it becomes clear to all parties that our nation will not tolerate anything other than full and total containment of North Korea's nuclear weapons and missile program.

References

1. Chisholm, D., The Korean war remembered, *Naval War Coll. Rev.,* LVII (1), 117–121, 2004.
2. Pike, J., Korean War, Global Security. Org, www.globalsecurity.org/military/ops/korea.htm, May 14, 2006, pp. 1–3.
3. Loc.Cit.
4. O'Neill, T., Korea's dangerous divide: DMZ, *National Geographic*, July 2003, p. 6, 25.
5. Nobley, R., Pueblo: a retrospective, *Naval War Coll. Rev.,* LIV (2), 100–103, 2001.
6. Ibid. pp. 107–109.
7. Pike, J., Nuclear Weapons Programs, Global Security. Org, www.globalsecurity.org/wmd/world/dprk/nuke.htm, May 14, 2006, pp. 1–2.
8. Ibid.
9. Ibid.
10. Pike, J., North Korea Nuclear Crisis — February 1993–June 1994, www.globalsecurity.org/military/ops/dprk_nuke.htm; May 14, 2003, p. 1.
11. Pike, J., 1994 Agreed Framework, www.globalsecurity.org/wmd/world/dprk/nuke-agreedframework.htm, Dec. 13, 2002, p. 1.
12. Pollack, J.D., The United States, North Korea, and the end of the agreed framework, *Naval War Coll. Rev.,* LVI (3), 14, 2003.
13. Loc.Cit.
14. United Nations Security Council, Reaffirming Resolutions 825 (1993) and 1540 (2004) directed to the Democratic People's Republic of Korea, the United States, North Korea, and the end of the agreed framework. July 15, 2006.
15. Hersh, S.M., Annals of national security the cold test, *The New Yorker*, Jan. 27, 2003, p. 42.
16. *Associated Press*, UN passes resolution condemning North Korea, MSNBC, July 15, 2006.
17. Abramowitz, M.I., Laney, J.T., and Heginbotham, E. Meeting the North Korean Nuclear Challenge: Report of an Independent Task Force, Council on Foreign Relations, New York, 2003, p. 23.
18. Pritchard, C.L., Korean Reunification: Implications for the United States and Northeast Asia, URI Party Foundation International Symposium on Peace and Prosperity in Northeast Asia, Seoul, Korea January 13–14, 2005, p. 3.

19. Moltz, C., Russian policy on the North Korean nuclear crisis, 13th Annual International Security Conference of Sandia National Laboratories on International Security Challenges and Strategies in the New Era, Apr. 23–25, 2005, Albuquerque, NM, Monterey Institute of International Studies, pp. 1–3.
20. Yuan, J.D., China and the North Korean Nuclear Crisis, Center for Non-proliferation Studies, Monterey Institute of International Studies, Jan. 22, 2003, pp. 1–2.
21. Ibid., p. 1.
22. Gallup Korea Survey of South Korean Perceptions, Dec. 2002.
23. Saunders, P.C., Confronting Ambiguity: How to Handle North Korea's Nuclear Program, Arms Control Today, Arms Control Association, Washington, D.C., Mar. 2003, p. 1.
24. Ibid., pp. 3–5.
25. Saunders, P.C., Military Options for Dealing with North Korea's Nuclear Program, Center for Non-Proliferation Studies, Monterey Institute of International Studies, Jan. 27, 2003, pp. 2–3.
26. Ibid., p.1.
27. Abramowitz, M.I., Laney, J.T., and Heginbotham, E., Op.Cit., pp. 36–41.
28. O'Hanlon, M.E., Preemption and North Korea, Global Politics, *The Washington Times*, June 28, 2006, p. 2.

Section II

Cyber Terrorism and Cyber Security

A Framework for Deception[1]

6

FRED COHEN

Contents

Executive Summary

This chapter overviews issues associated with deception and its impact on a wide variety of critical national security areas. Its objective is to create a framework for understanding deception and for turning that framework into a practical capability for carrying out offensive and defensive deception and counter-deception operations.

Overview

It is clear that there is a great deal of detailed literature on deception and that the issues of deception have been long understood and applied by many people. This chapter outlines a framework for creating and analyzing deceptions involving individuals and groups, including combinations of animals and automata operating as organizations. This framework has been used to model select deceptions and, to a more limited extent, to assist in the development of new and perhaps improved deceptions.

After studying this subject matter in depth, students of deception should (1) understand and analyze deceptions with considerably more clarity than they could previously, (2) command a far greater collection of techniques than was previously available, and (3) gain a far clearer understanding of how and when to apply which sorts of techniques for effect.

Introduction and Overview

According to the American Heritage Dictionary of the English Language (1981), "*deception*" is defined as "*the act of deceit;*" "*deceit*" is defined as "*deception.*"[2]

Since long before 800 B.C. when Sun Tzu wrote "The Art of War,"[2] deception has been a key to success in warfare. Similarly, information protection as a field of study has been around for at least 4000 years[3] and has been used as a vital element in warfare. However, despite the criticality of deception and information protection in warfare and the historical use of these techniques, in the transition toward an integrated, digitized battlefield and digitally controlled critical infrastructures, the use of deception in information protection

has not been widely undertaken. Little study has apparently been undertaken to systematically explore the use of deception for protection of systems dependent on digital information. This chapter, and the effort of which it is a part, seeks to change that situation and to use this expanded understanding to understand how deception and counter-deception operate in a more general class of organizations.

In October of 1983,[4] in explaining INFOWAR, Robert E. Huber explains by first quoting from Sun Tzu:

> **Deception: The Key** — The act of deception is an art supported by technology. When successful, it can have devastating impact on its intended victim. In fact:
>
> All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near. Hold out baits to entice the enemy. Feign disorder, and crush him. If he is secure at all points, be prepared for him. If he is in superior strength, evade him. If your opponent is of choleric temper, seek to irritate him. Pretend to be weak, that he may grow arrogant. If he is taking his ease, give him no rest. If his forces are united, separate them. Attack him where he is unprepared, appear where you are not expected.[5]
>
> The ability to sense, monitor, and control own-force signatures is at the heart of planning and executing operational deception …
>
> The practitioner of deception utilizes the victim's intelligence sources, surveillance sensors, and targeting assets as a principal means for conveying or transmitting a deceptive signature of desired impression. It is widely accepted that all deception takes place in the mind of the perceiver. Therefore, it is *not* the act itself but the acceptance that counts!

Analysis appears to indicate that there are only two ways of defeating an enemy.

1. One way is to have overwhelming force of some sort (i.e., an actual asymmetry that is, in time, fatal to the enemy). For example, you might be faster, smarter, better prepared, better supplied, better informed, first to strike, better positioned, and so forth.
2. The other way is to manipulate the enemy into reduced effectiveness (i.e., induced misperceptions that cause the enemy to misuse their capabilities). For example, the belief that you are stronger, closer, slower, better armed, in a different location, and so forth.

Having both an actual asymmetric advantage and effective deception increases your advantage. Having neither is usually fatal. Having more of one may help balance against having less of the other. Most military organizations seek to gain both advantages, but this is rarely achieved for long because of the competitive nature of warfare.

Overview

The purpose of this chapter is to explore the nature of deception with some emphasis on information technology and systems. While it can be reasonably asserted that all information systems are in many ways quite similar, there are differences between systems used in warfare and systems used in other applications, if only because the consequences of failure are extreme and the resources available to attackers are so high. For this reason, military situations tend to be the most complex and risky for information protection and thus lead to a context requiring extremes in protective measures. When combined with the rich history of deception in warfare, this context provides fertile ground for exploring the underlying issues.

We begin by exploring the history of deception and deception techniques. Next, we explore the nature of deception and provide a set of dimensions of the deception problem that are common to deceptions of the targets of interest. We then explore a model for deception of humans, a model for deception of computers, and a set of models for deceptions of systems of people and computers. Finally, we consider how we might design and analyze deceptions, discuss the need for experiments in this arena, summarize, draw conclusions, and describe further work.

A Short History of Deception

Fundamentally, deception is about errors in cognitive systems that are exploited for advantage. As the history below shows, there are a wide range of approaches to the identification of cognitive errors and methods for their exploitation.

Deception in Nature

While Sun Tzu is the first known publication depicting deception in warfare as an art, long before Sun Tzu there were tribal rituals of war that were intended in much the same way. The beating of chests[6] is a classic example that we still see today, although in a slightly different form. Many animals display their apparent fitness to others as part of the mating ritual or for territorial assertions. Mitchell and Thompson[7] look at human and nonhuman deception and provide interesting perspectives from many astute authors on many aspects of this subject. We see much the same behavior in today's international politics.

Who could forget Khrushchev banging his shoe on the table at the UN and declaring, "We will bury you!" Of course, it is not only the losers that "beat their chests," but it is a more stark example if presented that way. Every nation declares its greatness, both to its own people and to the world at large. We may call it pride, but at some point it becomes bragging, and in conflict situations, it becomes a display. Like the ancient tribesmen, the goal is, in some sense, to avoid a fight. The hope is that, by making the competitor think that it is not worth taking us on, we will not have to waste our energy or our blood in fighting when we could be spending it in other ways. Similar noise-making tactics also work to keep animals from approaching an encampment. The ultimate expression of this is in the area of nuclear deterrence.[8]

Animals also have genetic characteristics that have been categorized as deceptions. For example, certain animals are able to change colors to match the background or, as in the case of certain types of octopi, the ability to mimic other creatures. These are commonly lumped together, but, in fact, they are very different. The moth that looks like a flower may be able to "hide" from birds, but this is not an intentional act of deception. Survival of the fittest simply resulted in the death of most of the moths that could be detected by birds. The ones that happened to carry a genetic trait that made them look like a particular flower happened to get eaten less frequently. This is not a deception; it is a trait that survives. The same is true of the Orca whale, which has colors that dazzle and serve to break up its shape.

On the other hand, anyone who has seen an octopus change coloring and shape to appear as if it were a rock when a natural enemy comes by and then change again to mimic a food source while lying in wait for a food source could not honestly claim that this was an unconscious effort. This form of concealment (in the case of looking like a rock or foodstuff) or simulation (in the case of looking like an inedible or hostile creature) is highly selective, driven by circumstance, and most certainly driven by a thinking mind of some sort. It is a deception that uses a genetically endowed physical capability in an intentional and creative manner. It is more similar to a person putting on a disguise than it is to a moth's appearance.

Historical Military Deception

The history of deception is a rich one. In addition to the many books on military history that speak to it, it is a basic element of strategy and tactics that has been taught since the time of Sun Tzu. But in many ways, it is like the history of biology before genetics. It consists mainly of a collection of examples loosely categorized into things that appear similar at the surface. Hiding behind a tree is thought to be similar to hiding in a crowd of people, so both are called concealment. On the surface, they appear to be the same, but if we look at the mechanisms underlying them, they are quite different.

> Historically, military deception has proven to be of considerable value in the attainment of national security objectives, and a fundamental consideration in the development and implementation of military strategy and tactics. Deception has been used to enhance, exaggerate, minimize, or distort capabilities and intentions; to mask deficiencies; and to otherwise cause desired appreciations where conventional military activities and security measures were unable to achieve the desired result. The development of a deception organization and the exploitation of deception opportunities are considered to be vital to national security. To develop deception capabilities, including procedures and techniques for deception staff components, it is essential that deception receive continuous command emphasis in military exercises, command post exercises, and in training operations.
>
> JCS Memorandum of Policy (MOP) 116[9]

MOP 116 also points out that the most effective deceptions exploit beliefs of the target of the deception and, in particular, decision points in the enemy commander's operations plan. By altering the enemy commander's perception of the situation at key decision points, deception may turn entire campaigns.

There are many excellent collections of information on deceptions in war. One of the most comprehensive overviews comes from Whaley,[10] which includes details of 67 military deception operations between 1914 and 1968. The appendix to Whaley is 628 pages long and the summary charts (in appendix B) are another 50 pages. Another 30 years have passed since this time, which means that it is likely that another 200 pages covering 20 or so deceptions should be added to update this study. Dunnigan and Nofi[11] review the history of deception in warfare with an eye toward categorizing its use. They identify the different modes of deception as concealment, camouflage, false and planted information, ruses, displays, demonstrations, feints, lies, and insight.

Dewar[12] reviews the history of deception in warfare and, in only 12 pages, gives one of the most cogent high-level descriptions of the basis, means, and methods of deception. In these 12 pages, he outlines (1) the weaknesses of the human mind (preconceptions, tendency to think we are right, coping with confusion by leaping to conclusions, information overload and resulting filtering, the tendency to notice exceptions and ignore commonplace things, and the tendency to be lulled by regularity); (2) the object of deception (getting the enemy to do or not do what you wish); (3) means of deception (affecting observables to a level of fidelity appropriate to the need, providing consistency, meeting enemy expectations, and not making it too easy); (4) principles of deception (careful centralized control and coordination, proper preparation and planning, plausibility, the use of multiple sources

and modes, timing, and operations security); and (5) techniques of deception (encouraging belief in the most likely when a less likely is to be used, luring the enemy with an ideal opportunity, the repetitive process and its lulling effect, the double bluff, which involves revealing the truth when it is expected to be a deception, the piece of bad luck, which the enemy believes they are taking advantage of, the substitution of a real item for a detected deception item, and disguising as the enemy). He also (6) categorizes deceptions in terms of senses and (7) relates "security" (in which you try to keep the enemy from finding anything out) to deception (in which you try to get the enemy to find out the thing you want them to find). Dewar also includes pictures and examples in these 12 pages.

In 1987, Knowledge Systems Corporation[13] created a useful set of diagrams for planning tactical deceptions. Among their results, they indicate that the assessment and planning process is manual, lacks automated applications programs, and lacks timely data required for combat support. This situation does not appear to have changed. They propose a planning process consisting of (1) reviewing force objectives, (2) evaluating your own and enemy capabilities and other situational factors, (3) developing a concept of operations and set of actions, (4) allocating resources, (5) coordinating and deconflicting the plan relative to other plans, (6) doing a risk and feasibility assessment, (7) reviewing adherence to force objectives, and (8) finalizing the plan. They detail steps to accomplish each of these tasks in useful process diagrams and provide forms for doing a more systematic analysis of deceptions than was previously available. Such a planning mechanism does not appear to exist today for deception in information operations.

These authors share one thing in common. They all carry out an exercise in building categories. Just as the long-standing effort of biology to build up genus and species based on bodily traits (phenotypes), eventually fell to a mechanistic understanding of genetics as the underlying cause, the scientific study of deception will eventually yield a deeper understanding that will make the mechanisms clear and allow us to understand and create deceptions as an engineering discipline. That is not to say that we will necessarily achieve that goal in this short examination of the subject, but rather that an in-depth study will ultimately yield such results.

There have been a few attempts in this direction. A RAND study included a "straw man" graphic[14] (H7076) that showed deception as being broken down into "Simulation" and "Dissimulation Camouflage."

> Whaley first distinguishes two categories of deception (which he defines as one's intentional distortion of another's perceived reality): (a) dissimulation (hiding the real) and (b) simulation (showing the false). Under dissimulation he includes: (a) masking (hiding

> the real by making it invisible), (b) repackaging (hiding the real by disguising), and (c) dazzling (hiding the real by confusion). Under simulation he includes: (a) mimicking (showing the false through imitation), (b) inventing (showing the false by displaying a different reality), and (c) decoying (showing the false by diverting attention). Since Whaley argues that "everything that exists can to some extent be both simulated and dissimulated, whatever the actual empirical frequencies, at least in principle hoaxing should be possible for any substantive area."[15]

The same slide reflects on Dewar's view[16] that security attempts to deny access and counterintelligence attempts, while deception seeks to exploit intelligence. Unfortunately, the RAND depiction is not as cogent as Dewar in breaking down the "subcategories" of simulation. The RAND slides do cover the notions of observables being "known and unknown," "controllable and uncontrollable," and "enemy observable and enemy nonobservable." This characterization of part of the space is useful from a mechanistic viewpoint and a decision tree created from these parameters can be of some use. Interestingly, RAND also points out the relationship of selling, acting, magic, psychology, game theory, military operations, probability and statistics, logic, information and communications theories, and intelligence to deception. It indicates issues of observables, cultural bias, and knowledge of enemy capabilities, analytical methods, and thought processes. It uses a reasonable model of human behavior, lists some well-known deception techniques, and looks at some of the mathematics of perception management and reflexive control.

Cognitive Deception Background

Many authors have examined facets of deception from both an experiential and cognitive perspective.

Chuck Whitlock has built a large part of his career on identifying and demonstrating these sorts of deceptions.[17] His book includes detailed descriptions and examples of scores of common street deceptions. Fay Faron points out that most such confidence efforts are carried as specific "plays" and details the anatomy of a "con."[18] She provides seven ingredients for a con (too good to be true, nothing to lose, out of their element, limited time offer, references, pack mentality, and no consequence to actions). The anatomy of the confidence game is said to involve (1) a motivation (e.g., greed), (2) the come-on (e.g., opportunity to get rich), (3) the shill (e.g., a supposedly independent third party), (4) the swap (e.g., take the victim's money while making them think they have it), (5) the stress (e.g., time pressure), and (6) the block (e.g., a reason the victim will not report the crime). She even includes a 10-step play that makes up the big con.

Bob Fellows[19] takes a detailed approach to how "magic" and similar techniques exploit human fallibility and cognitive limits to deceive people. According to Fellows,[20] the following characteristics improve the changes of being fooled:

- Under stress
- Naivety
- In life transitions
- Unfulfilled desire for spiritual meaning
- Tend toward dependency
- Attracted to trance-like states of mind
- Unassertive
- Unaware of how groups can manipulate people
- Gullible
- Have had a recent traumatic experience
- Want simple answers to complex questions
- Unaware of how the mind and body affect each other
- Idealistic
- Lack critical thinking skills
- Disillusioned with the world or the culture
- Lack knowledge of deception methods

Fellows also identifies a set of methods used to manipulate people.

Thomas Gilovich[21] provides in-depth analysis of human reasoning fallibility by presenting evidence from psychological studies that demonstrate a number of human reasoning mechanisms resulting in erroneous conclusions. This includes the general notions that people (erroneously) (1) believe that effects should resemble their causes, (2) misperceive random events, (3) misinterpret incomplete or unrepresentative data, (4) form biased evaluations of ambiguous and inconsistent data, (5) have motivational determinants of belief, (6) believe bias second-hand information, and (7) have exaggerated impressions of social support. Substantial further detailing shows specific common syndromes and circumstances associated with them.

Charles K. West[22] describes the steps in psychological and social distortion of information and provides detailed support for cognitive limits leading to deception. Distortion comes from the fact of an unlimited number of problems and events in reality, although human sensation can only sense certain types of events in limited ways: (1) a person can only perceive a limited number of those events at any moment, (2) a person's knowledge and emotions partially determine which of the events are noted and interpretations are made in terms of knowledge and emotion, (3) intentional bias occurs as a person consciously selects what will be communicated to others, and (4) the receiver of information provided by others will have the same set of interpretations and sensory limitations.

Al Seckel[23] provides nearly 100 excellent examples of various optical illusions, many of which work regardless of the knowledge of the observer and some of which are defeated after the observer sees them only once. Donald D. Hoffman[24] expands this into a detailed examination of visual intelligence and how the brain processes visual information. It is particularly noteworthy that the visual cortex consumes a great deal of the total human brain space and that it has a great deal of effect on cognition. Some of the "rules" that Hoffman describes with regard to how the visual cortex interprets information include:

1. Always interpret a straight line in an image as a straight line in three dimensions (3D).
2. If the tips of two lines coincide in an image, interpret them as coinciding in 3D.
3. Always interpret co-linear lines in an image as co-linear in 3D.
4. Interpret elements near each other in an image as near each other in 3D.
5. Always interpret a curve that is smooth in an image as smooth in 3D.
6. Where possible, interpret a curve in an image as the rim of a surface in 3D.
7. Where possible, interpret a T-junction in an image as a point where the full rim conceals itself; the cap conceals the stem.
8. Interpret each convex point on a bound as a convex point on a rim.
9. Interpret each concave point on a bound as a concave point on a saddle point.
10. Construct surfaces in 3D that are as smooth as possible.
11. Construct subjective figures that occlude only if there are convex cusps.
12. If two visual structures have a nonaccidental relation, group them and assign them to a common origin.
13. If three or more curves intersect at a common point in an image, interpret them as intersecting at a common point in space.
14. Divide shapes into parts along concave creases.
15. Divide shapes into parts at negative minima, along lines of curvature, of the principal curvatures.
16. Divide silhouettes into parts at concave cusps and negative minima of curvature.
17. The salience of a cusp boundary increases with increasing sharpness of the angle at the cusp.
18. The salience of a smooth boundary increases with the magnitude of (normalized) curvature at the boundary.
19. Choose figure and ground so that figure has the more salient part boundaries.
20. Choose figure and ground so that figure has the more salient parts.
21. Interpret gradual changes in hue, saturation, and brightness in an image as changes in illumination.

22. Interpret abrupt changes in hue, saturation, and brightness in an image as changes in surfaces.
23. Construct as few light sources as possible.
24. Put light sources overhead.
25. Filters do not invert lightness.
26. Filters decrease lightness differences.
27. Choose the fair pick that is most stable.
28. Interpret the highest luminance in the visual field as white, fluoroscent, or self-luminous.
29. Create the simplest possible motions.
30. When making motion, construct as few objects as possible, and conserve them as much as possible.
31. Construct motion to be as uniform over space as possible.
32. Construct the smoothest velocity field.
33. If possible, and if other rules permit, interpret image motions as projections of rigid motions in 3D.
34. If possible, and if other rules permit, interpret image motions as projections of 3D motions that are rigid and planar.
35. Light sources move slowly.

It appears that the rules of visual intelligence are closely related to the results of other cognitive studies. It may not be a coincidence that the thought processes that occupy the same part of the brain as visual processing have similar susceptibilities to errors and that these follow the pattern of the assumption that small changes in observation point should not change the interpretation of the image. It is surprising when such a change reveals a different interpretation, and the brain appears to be designed to minimize such surprises while acting at great speed in its interpretation mechanisms. For example, rule 2 (If the tips of two lines coincide in an image, interpret them as coinciding in 3D.) is very nearly always true in the physical world because coincidence of line ends that are not, in fact, coincident in 3D requires that you be viewing the situation at precisely the right angle with respect to the two lines. Another way of putting this is that there is a single line in space that connects the two points so as to make them appear to be coincident if they are not, in fact, coincident. If the observer is not on that single line, the points will not appear coincident. Since people usually have two eyes and they cannot align on the same line in space with respect to anything they can observe, there is no real 3D situation in which this coincidence can actually occur, it can only be simulated by 3D objects that are far enough away to appear to be on the same line with respect to both eyes, and there are no commonly occurring natural phenomena that pose anything of immediate visual import or consequence at that distance. Designing visual stimuli that violate these principles will confuse most

human observers and effective visual simulations should take these rules into account.

Deutsch[25] provides a series of demonstrations of interpretation and misinterpretation of audio information. This includes: (1) the creation of words and phrases out of random sounds, (2) the susceptibility of interpretation to predisposition, (3) misinterpretation of sound based on relative pitch of pairs of tones, (4) misinterpretation of direction of sound source based on switching speakers, (5) creation of different words out of random sounds based on rapid changes in source direction, and (6) the change of word creation over time based on repeated identical audio stimulus.

First Karrass[26] then Cialdini[27] have provided excellent summaries of negotiation strategies and the use of influence to gain advantage. Both also explain how to defend against influence tactics. Karrass was one of the early experimenters in how people interact in negotiations and identified:

credibility of the presenter,
message content and appeal,
situation setting and rewards, and
media choice for messages as critical components of persuasion.

He also identifies goals, needs, and perceptions as 3D of persuasion and lists scores of tactics categorized into types including:

Timing
Inspection
Authority
Association
Amount
Brotherhood
Detour

Karrass also provides a list of negotiating techniques including:

Agendas
Questions
Statements
Concessions
Commitments
Moves
Threats
Promises
Recess
Delays
Deadlock
Focal points

Standards
Secrecy measures
Nonverbal communications
Media choices
Listening
Caucus
Formal and informal memorandum
Informal discussions
Trial balloons and leaks
Hostility relievers
Temporary intermediaries
Location of negotiation
Technique of time

Cialdini[28] provides a simple structure for influence and asserts that much of the effect of influence techniques is built in and occurs below the conscious level for most people. His structure consists of reciprocation, contrast, authority, commitment and consistency, automaticity, social proof, liking, and scarcity. He cites a substantial series of psychological experiments that demonstrate quite clearly how people react to situations without a high level of reasoning and explains how this is both critical to being effective decision makers and results in exploitation through the use of compliance tactics. While Cialdini backs up this information with numerous studies, his work is largely based on and largely cites western culture. Some of these elements are apparently culturally driven and care must be taken to assure that they are used in context.

Robertson and Powers[29] have worked out a more detailed low-level theoretical model of cognition based on "perceptual control theory" (PCT), but extensions to higher levels of cognition have been highly speculative to date. They define a set of levels of cognition in terms of their order in the control system, but beyond the lowest few levels they have inadequate basis for asserting that these are orders of complexity in the classic control theoretical sense. The levels they include are intensity, sensation, configuration, transition/motion, events, relationships, categories, sequences/routines, programs/branching pathways/logic, and system concept.

David Lambert[30] provides an extensive collection of examples of deceptions and deceptive techniques mapped into a cognitive model intended for modeling deception in military situations. These are categorized into cognitive levels in Lambert's cognitive model. The levels include sense, perceive feature, perceive form, associate, define problem/observe, define problem-solving status (hypothesize), determine solution options, initiate actions/responses, direct, implement form, implement feature, and drive affecters. There are feedback and cross circuiting mechanisms to allow for reflexes, conditioned behavior, intuition, the driving of perception to higher and lower levels, and models of short-and long-term memory.

Charles Handy[31] discusses organizational structures and behaviors and the roles of power and influence within organizations. The National Research Council[32] discusses models of human and organizational behavior and how automation has been applied in this area. Handy models organizations in terms of their structure and the effects of power and influence. Influence mechanisms are described in terms of who can apply them in what circumstances. Power is derived from physicality, resources, position (which yields information, access, and right to organize), expertise, personal charisma, and emotion. These result in influence through overt (force, exchange, rules and procedures, and persuasion), covert (ecology and magnetism), and bridging (threat of force) influences. Depending on the organizational structure and the relative positions of the participants, different aspects of power come into play and different techniques can be applied. The National Research Council (NRC) report includes scores of examples of modeling techniques and details of simulation implementations based on those models and their applicability to current and future needs. Greene[33] describes the 48 laws of power and, along the way, demonstrates 48 methods that exert compliance forces in an organization. These can be traced to cognitive influences and mapped out using models such as Lambert's, Cialdini's, and the one we are considering for this effort.

Closely related to the subject of deception is the work done by the CIA on the MKULTRA project.[34] In June 1977, a set of MKULTRA documents was discovered, which had escaped destruction by the CIA. The Senate Select Committee on Intelligence held a hearing on August 3, 1977 to question CIA officials on the newly discovered documents. The net effect of efforts to reveal information about this project was a set of released documents on the use of sonic waves, electroshock, and other similar methods for altering peoples' perception. Included in this are such items as sound frequencies that make people fearful, sleepy, uncomfortable, and sexually aroused; results on hypnosis, truth drugs, psychic powers, and subliminal persuasion; LSD-related and other drug experiments on unwitting subjects; the CIA's "manual on trickery;" and so forth. One 1955 MKULTRA document gives an indication of the size and range of the effort; the memo refers to the study of an assortment of mind-altering substances which would:

> Promote illogical thinking and impulsiveness to the point where the recipient would be discredited in public.
> Increase the efficiency of mentation and perception.
> Prevent or counteract the intoxicating effect of alcohol.
> Promote the intoxicating effect of alcohol.
> Produce the signs and symptoms of recognized diseases in a reversible way so that they may be used for malingering, etc.
> Render the indication of hypnosis easier or otherwise enhance its usefulness.

Enhance the ability of individuals to withstand privation, torture, and coercion during interrogation and so-called "brainwashing."
Produce amnesia for events preceding and during their use.
Produce shock and confusion over extended periods of time and capable of surreptitious use.
Produce physical disablement, such as paralysis of the legs, acute anemia, etc.
Produce "pure" euphoria with no subsequent letdown.
Alter personality structure in such a way that the tendency of the recipient to become dependent upon another person is enhanced.
Cause mental confusion of such a type that the individual under its influence would find it difficult to maintain a fabrication under questioning.
Lower the ambition and general working efficiency of men when administered drugs in undetectable amounts.
Promote weakness or distortion of the eyesight or hearing faculties, preferably without permanent effects.

A good summary of some of the pre-1990 results on psychological aspects of self-deception is provided in Heuer's CIA book on the psychology of intelligence analysis.[35] Heuer goes one step farther in trying to start assessing ways to counter deception, and concludes that intelligence analysts can make improvements in their presentation and analysis process. Several other papers on deception detection have been written and substantially summarized in Vrij's book on the subject.[36]

Computer Deception Background

In the early 1990s, the use of deception in defense of information systems came to the forefront with a paper about a deception "Jail" created in 1991 by AT&T researchers in real time to track an attacker and observe the attacker actions.[37] An approach to using deceptions for defense by customizing every system to defeat automated attacks was published in 1992.[38] In 1996, descriptions of Internet Lightning Rods were given[39] and an example of the use of perception management to counter perception management in the information infrastructure was given.[40] More thorough coverage of this history was covered in a 1999 paper on the subject.[41] Since that time, deception has increasingly been explored as a key technology area for innovation in information protection. Examples of deception-based information system defenses include concealed services, encryption, feeding false information, hard-to-guess passwords, isolated subfile-system areas, low building profile, noise injection, path diversity, perception management, rerouting attacks, retaining confidentiality of security status information, spread spectrum, and traps. In addition, it appears that criminals seek certainty in their attacks on

computer systems and increased uncertainty caused by deceptions may have a deterrent effect.[42]

The public release of Deception ToolKit (DTK) led to a series of follow-on studies, technologies, and increasing adoption of technical deceptions for defense of information systems. This includes the creation of a small but growing industry with several commercial deception products, the HoneyNet project, the RIDLR project at Naval Post Graduate School, NSA-sponsored studies at RAND, the D-Wall technology,[43] and a number of studies and developments now underway.[44]

- *Commercial deception products:* The dominant commercial deception products today are DTK and Recourse Technologies. While the market is very new, it is developing at a substantial rate and new results from deception projects are leading to an increased appreciation of the utility of deceptions for defense and a resulting increased market presence.
- *The HoneyNet project:* The HoneyNet project is dedicated to learning and to the tools, tactics, and motives of the black hat community and sharing the lessons learned. The primary tool used to gather this information is the Honeynet: a network of production systems designed to be compromised. This project has been joined by a substantial number of individual researchers and has had substantial success at providing information on widespread attacks, including the detection of large-scale denial of service worms prior to the use of the "zombies" for attack. At least, one Master's thesis is currently underway based on these results.
- *The RIDLR:* The RIDLR is a project launched from the Naval Post Graduate School designed to test out the value of deception for detecting and defending against attacks on military information systems. RIDLR has been tested on several occasions at the Naval Post Graduate School and members of that team have participated in this project to some extent. There is an ongoing information exchange with that team as part of this project's effort.
- *RAND Studies:* In 1999, RAND completed an initial survey of deceptions in an attempt to understand the issues underlying deceptions for information protection.[45] This effort included a historical study of issues, limited tool development, and limited testing with reasonably skilled attackers. The objective was to scratch the surface of possibilities and assess the value of further explorations. It predominantly explored intelligence-related efforts against systems and methods for concealment of content and creation of large volumes of false content. It sought to understand the space of friendly defensive deceptions and gain a handle on what was likely to be effective in the future.

This report indicates challenges for the defensive environment including: (1) adversary initiative, (2) response to demonstrated adversary capabilities or established friendly shortcomings, (3) many potential attackers and points of attack, (4) many motives and objectives, (5) anonymity of threats, (6) large amount of data that might be relevant to defense, (7) large noise content, (8) many possible targets, (9) availability requirements, and (10) legal constraints.

Deception may (1) condition the target to friendly behavior, (2) divert target attention from friendly assets, (3) draw target attention to a time or place, (4) hide presence or activity from a target, (5) advertise strength or weakness as their opposites, (6) confuse or overload adversary intelligence capabilities, or (7) disguise forces.

The animal kingdom is studied briefly and characterized as ranging from concealment to simulation, at levels of static, dynamic, adaptive, and premeditated.

Political science and psychological deceptions are fused into maxims:

(1) Pre-existing notions given excessive weight
(2) Desensitization degrades vigilance
(3) Generalizations or exceptions based on limited data
(4) Failure to fully examine the situation limits comprehension
(5) Limited time and processing power limit comprehension
(6) Failure to adequately corroborate
(7) Over-valuing data based on rarity
(8) Experience with source may color data inappropriately
(9) Focusing on a single explanation when others are available
(10) Failure to consider alternative courses of action
(11) Failure to adequately evaluate options
(12) Failure to reconsider previously discarded possibilities
(13) Ambivalence by the victim to the deception
(14) Confounding effect of inconsistent data

This is very similar to the coverage of Gilovich[46] reviewed in detail elsewhere in this chapter.

Confidence artists use a three-step screening process: (1) low-investment deception to gauge target reaction, (2) low-risk deception to determine target pliability, and (3) reveal a deception and gauge reaction to determine willingness to break the rules.

Military deception is characterized through Joint Pub 3-58 (Joint Doctrine for Military Deception) and Field Manual 90-02,[47] which are already covered in this overview.

The report then goes on to review things that can be manipulated, actors, targets, contexts, and some of the then-current efforts to manipulate observables, which they characterize as honey pots, fishbowls, and canaries. They characterize a space of raw materials, deception means, and level

of sophistication. They look at possible mission objectives of shielding assets from attackers, luring attention away from strategic assets, the induction of noise or uncertainty, and profiling identity, capabilities, and intent by creation of opportunity and observation of action. They hypothesize a deception toolkit consisting of user inputs to a rule-based system that automatically deploys deception capabilities into fielded units as needed, and detail some potential rules for the operation of such a system in terms of deception means, material requirements, and sophistication. Consistency is identified as a problem, the potential for self-deception is high in such systems, and the problem of achieving adequate fidelity is reflected as it has been elsewhere.

The follow-up RAND study[48] extends the previous results with a set of experiments in the effectiveness of deception against sample forces. They characterize deception as an element of "active network defense." Not surprisingly, they conclude that more elaborate deceptions are more effective, but they also find a high degree of effectiveness for select superficial deceptions against select superficial intelligence probes. They conclude, among other things, that deception can be effective in protection, counterintelligence, against cyber-reconnaissance, and to help to gather data about enemy reconnaissance. This is consistent with previous results that were more speculative. Counter-deception issues are also discussed, including structural, strategic, cognitive, deceptive, and overwhelming approaches.

- *Theoretical work:* One historical and three current theoretical efforts have been undertaken in this area, and all are currently quite limited. Cohen looked at a mathematical structure of simple defensive network deceptions in 1999[49] and concluded that as a counterintelligence tool, network-based deceptions could be of significant value, particularly if the quality of the deceptions could be made good enough. Cohen suggested the use of rerouting methods combined with live systems of the sorts being modeled as yielding the highest fidelity in a deception. He also expressed the limits of fidelity associated with system content, traffic patterns, and user behavior, all of which could be simulated with increasing accuracy for increasing cost. In this paper, networks of up to 64,000 IP addresses were emulated for high-quality deceptions using a technology called D-Wall.[50]

Dorothy Denning of Georgetown University is undertaking a small study of issues in deception. Matt Bishop of the University of California at Davis is undertaking a study funded by the department of energy on the mathematics of deception. Glen Sharlun of the Naval Post Graduate School is finishing a master's thesis on the effect of deception as a deterrent and as a detection method in large-scale distributed denial of service attacks.

- Custom deceptions: Custom deceptions have existed for a long time, but only recently have they gotten adequate attention to move toward high fidelity and large scales.

The reader is asked to review citation[51] Cohen's "A note on the role of Deception in Information Protection" for more thorough coverage of computer-based defensive deceptions and to get a more complete understanding of the application of deceptions in this arena over the last 50 years.

Another major area of information protection through deception is in the area of steganography. The term steganography comes from the Greek "steganos" (covered or secret) and "graphy" (writing or drawing) and thus means, literally, covered writing. As commonly used today, steganography is closer to the art of information hiding and is an ancient form of deception used by everyone from ruling politicians to slaves. It has existed in one form or another for at least 2000 years and probably a lot longer.

With the increasing use of information technology and increasing fears that information will be exposed to those for whom it is not intended, steganography has undergone a sort of emergence. Computer programs that automate the processes associated with digital steganography have become widespread in recent years. Steganographic content is now commonly hidden in graphic files, sound files, text files, covert channels, network packets, slack space, spread spectrum signals, and video conferencing systems. Thus, steganography has become a major method for concealment in information technology and has broad applications for defense.

The Nature of Deception

Even the definition of deception is illusive. As we saw from the circular dictionary definition presented earlier, there is no end to the discussion of what is and is not deception. This notwithstanding, there is an end to this chapter, so we will not be making as precise a definition as we might like to. Rather, we will simply assert that deception is a set of acts that seek to increase the chances that a set of targets will behave in a desired fashion when they would be less likely to behave in that fashion if they knew of those acts.

We will generally limit our study of deceptions to targets consisting of people, animals, computers, and systems comprised of these things and their environments. While it could be argued that all deceptions of interest to warfare focus on gaining compliance of people, we have not adopted this position. Similarly, from a pragmatic viewpoint, we see no current need to try to deceive some other sort of being.

While our study will seek general understanding, our ultimate focus is on deception for information protection and is further focused on information technology and systems that depend on it. At the same time, in order

for these deceptions to be effective, we have to, at least potentially, be successful at deception against computers used in attack, people who operate and program those computers, and ultimately, organizations that task those people and computers. Therefore, we must understand deception that targets people and organizations, not just computers.

Limited Resources Lead to Controlled Focus of Attention

There appear to be some features of deception that apply to all of the targets of interest. While the detailed mechanisms underlying these features may differ, commonalities are worthy of note. Perhaps, the core issue that underlies the potential for success of deception as a whole is that all targets not only have limited overall resources, but they have limited abilities to process the available sensory data they are able to receive. This leads to the notion that, in addition to controlling the set of information available to the targets, deceptions may seek to control the focus of attention of the target.

In this sense, deceptions are designed to emphasize one thing over another. In particular, they are designed to emphasize the things you want the targets to observe over the things you do not want them to observe. While many who have studied deception in the military context have emphasized the desire for total control over enemy observables, this tends to be highly resource consumptive and very difficult to do. Indeed, there is not a single case in our review of military history where such a feat has been accomplished and we doubt whether such a feat will ever be accomplished.

> Example: Perhaps the best example of having control over observables was in the Battle of Britain in World War II when the British turned all of the Nazi intelligence operatives in Britain into double agents and combined their reports with false fires to try to get the German Luftwaffe to miss their factories. But even this incredible level of success in deception did not prevent the Germans from creating technologies, such as radio beam guidance systems, that resulted in accurate targeting for periods of time.

It is generally more desirable from an assurance standpoint to gain control over more target observables, assuming you have the resources to affect this control in a properly coordinated manner, but the reason for this may be a bit surprising. The only reason to control more observables is to increase the likelihood of attention being focused on observables you control. If you could completely control focus of attention, you would only need to control

a very small number of observables to have complete effect. In addition, the cost of controlling observables tends to increase nonlinearly with increased fidelity. As we try to reach perfection, the costs presumably become infinite. Therefore, there should be some cost benefit analysis undertaken in deception planning and some metrics are required in order to support such analysis.

All Deception Is a Composition of Concealments and Simulations

Reflections of world events appear to the target as observables. In order to affect a target, we can only create causes in the world that affect those observables. Thus, all deceptions stem from the ability to influence target observables. At some level, all we can do is create world events whose reflection appear to the target as observables or prevent the reflections of world events from being observed by the target. As terminology, we will call induced reflections "*simulations*" and inhibition of reflections "*concealments*." In general then, all deceptions are formed from combinations of concealments and simulations.

Put another way, deception consists of determining what we wish the target to observe and not observe and creating simulations to induce desired observations while using concealments to inhibit undesired observations. Using the notion of focus of attention, we can create simulations and concealments by inducing focus on desired observables while drawing focus away from undesired observables. Simulation and concealment are used to affect this focus and the focus then produces more effective simulation and concealment.

Memory and Cognitive Structure Force Uncertainty, Predictability, and Novelty

All targets have limited memory state and are, in some ways, inflexible in their cognitive structure. While space limits memory capabilities of targets, in order to be able to make rapid and effective decisions, targets necessarily trade away some degree of flexibility. As a result, targets have some predictability. The problem at hand is figuring out how to reliably make target behavior (focus of attention, decision processes, and ultimately actions) comply with our desires. To a large extent, the purpose of this study is to find ways to increase the certainty of target compliance by creating improved deceptions.

There are some severe limits to our ability to observe target memory state and cognitive structure. Target memory state and detailed cognitive structure is almost never fully available to us. Even if it were available, we would be unable, at least at the present, to adequately process it to make detailed predictions of behavior because of the complexity of such computations and our own limits of memory and cognitive structure. This means that we are forced to make imperfect models and that we will have uncertain results for the foreseeable future.

While modeling of enough of the cognitive structures and memory state of targets to create effective deceptions may often be feasible, the more common methods used to create deceptions are the use of characteristics that have been determined through psychological studies of human behavior, animal behavior, analytical and experimental work done with computers, and psychological studies done on groups. The studies of groups containing humans and computers are very limited and those that do exist ignore the emerging complex global network environment. Significant additional effort will be required in order to understand common modes of deception that function in the combined human–computer social environment.

A side effect of memory is the ability of targets to learn from previous deceptions. Effective deceptions must be novel or varied over time in cases where target memory affects the viability of the deception.

Time, Timing, and Sequence Are Critical

Several issues related to time come up in deceptions. In the simplest cases, a deception might come to mind just before it is to be performed, but for any complex deception, preplanning is required and that preplanning takes time. In cases where special equipment or other capabilities must be researched and developed, the entire deception process can take months to years.

In order for deception to be effective in many real-time situations, it must be very rapidly deployed. In some cases, this may mean that it can be activated almost instantaneously. In other cases, this may mean a time frame of seconds to days or even weeks or months. In strategic deceptions, such as those in the Cold War, this may take place over periods of years.

In every case there is some delay between the invocation of a deception and its effect on the target. At a minimum, we may have to contend with speed of light effects, but in most cases, cognition takes from milliseconds to seconds. In cases with higher momentum, such as organizations or large systems, it may take minutes to hours before deceptions begin to take effect. Some deceptive information is even planted in the hopes that it will be discovered and acted on in months or in years.

Eventually, deceptions may be discovered. In most cases, a critical item to success in the deception is that the time before discovery be long enough for some other desirable thing to take place. For one-shot deceptions intended to gain momentary compliance, discovery after a few seconds may be adequate, but other deceptions require longer periods over which they must be sustained. Sustaining a deception is generally related to preventing its discovery, in that, once discovered, sustainment often has very different requirements.

Finally, nontrivial deceptions involve complex sequences of acts, often involving branches based on feedback attained from the target. In almost all cases, out of the infinite set of possible situations that may arise, some set of

critical criteria are developed for the deception and used to control sequencing. This is necessary because of the limits of the ability of deception planning to create sequencers for handling more complex decision processes because of limits on available observables for feedback, and because of limited resources available for deception.

> Example: In a commonly used magician's trick, the subject is given a secret that the magician cannot possibly know based on the circumstances. At some time in the process, the subject is told to reveal the secret to the whole audience. After the subject makes the secret known, the magician reveals that same secret from a hiding place. The trick comes from the sequence of events. As soon as the answer is revealed, the magician chooses where the revealed secret is hidden. What really happens is that the magician chooses the place based on what the secret is and reveals one of the many preplanted secrets. If the sequence required the magicians to reveal their hidden result first, this deception would not work.[52]

Observables Limit Deception

In order for targets to be deceived, their observations must be affected. Therefore, we are limited in our ability to deceive based on what they are able to observe. Targets may also have allies with different observables and, in order to be effective, our deceptions must take those observables into account. We are limited both by what can be observed and what cannot be observed. We cannot use what cannot be observed to induce simulation, whereas what can be observed creates limits on our ability to conceal.

> Example: Dogs are commonly used in patrol units because of the fact that they have different sensory and cognitive capabilities than people. Thus, when people try to conceal themselves from other people, the things they choose to do tend to fool other people, but not animals like dogs, which, for example, might smell them out even without seeing or hearing them.

Our own observables also limit our ability to do deceptions because sequencing of deceptions depends on feedback from the target and because our observables in terms of accurate intelligence information drive our ability to understand the observables of the target and the effect of those observables on the target.

Operational Security Is a Requirement

Secrecy of some sort is fundamental to all deception, if only because the target would be less likely to behave in the desired fashion if they knew of

the deception (by our definition earlier). This implies operational security of some sort.

One of the big questions to be addressed in some deceptions is who should be informed of the specific deceptions under way. Telling too many people increases the likelihood of the deception being leaked to the target. Telling too few people may cause the deception to fool your own side into blunders.

> Example: In Operation Overlord during World War II, some of the allied deceptions were kept so secret that they fooled allied commanders into making mistakes. These sorts of errors can lead to fratricide.[53]

Security is expensive and creates great difficulties, particularly in technology implementations. For example, if we create a device that is only effective if its existence is kept secret, we will not be able to apply it very widely, so the number of people that will be able to apply it will be very limited. If we create a device that has a set of operational modes that must be kept secret, the job is a bit easier. As we move toward a device that only needs to have its current placement and current operating mode kept secret, we reach a situation where widespread distribution and effective use is feasible.

A vital issue in deception is the understanding of what must be kept secret and what may be revealed. If too much is revealed, the deception will not be as effective as it otherwise may have been. If too little is revealed, the deception will be less effective in the larger sense because fewer people will be able to apply it. History shows that device designs and implementations eventually leak out. That is why soundness for a cryptographic system is usually based on the assumption that only the keys are kept secret. The same principle would be well considered for use in many deception technologies.

A further consideration is the deterrent effect of widely published use of deception. The fact that high-quality deceptions are in widespread use potentially deters attackers or alters their behavior because they believe that they are unable to differentiate deceptions from nondeceptions or because they believe that this differentiation substantially increases their workload. This was one of the notions behind DTK.[54] The suggestion was even made that if enough people use the DTK deception port, the use of the deception port alone might deter attacks.

Cybernetics and System Resource Limitations

In the systems theory of Norbert Weiner (called Cybernetics),[55] many systems are described in terms of feedback. Feedback and control theory address the notions of systems with expectations and error signals. Our targets tend to take the difference between expected inputs and actual inputs and adjust outputs in an attempt to restore stability. This feedback mechanism both enables and limits deception.

Expectations play a key role in the susceptibility of the target to deception. If the deception presents observables that are very far outside the normal range of expectations, it is likely to be hard for the target to ignore it. If the deception matches a known pattern, the target is likely to follow the expectations of that pattern unless there is a reason not to. If the goal is to draw attention to the deception, creating more difference is more likely to achieve this, but it will also make the target more likely to examine it more deeply and with more skepticism. If the object is to avoid something being noticed, creating less apparent deviation from expectation is more likely to achieve this.

Targets tend to have different sensitivities to different sorts and magnitudes of variations from expectations. These result from a range of factors including, but not limited to, sensor limitations, focus of attention, cognitive structure, experience, training, reasoning ability, and predisposition. Many of these can be measured or influenced in order to trigger or avoid different levels of assessment by the target.

Most systems do not perform deep logical thinking about all situations as they arise. Rather, they match known patterns as quickly as possible and only apply the precious deep processing resources to cases where pattern matching fails to reconcile the difference between expectation and interpretation. As a result, it is often easy to deceive a system by avoiding its logical reasoning in favor of pattern matching. Increased rush, stress, uncertainty, indifference, distraction, and fatigue all lead to less thoughtful and more automatic responses in humans.[56] Similarly, we can increase human reasoning by reduced rush, stress, certainty, caring, attention, and alertness.

> Example: Someone who looks like a valet parking person and is standing outside of a pizza place will often get car keys from wealthy customers. If the customers really used reason, they would probably question the notion of a valet parking person at a pizza place, but their mind is on food and conversation and perhaps they just miss it. This particular experiment was one of many done with great success by Whitlock.[57]

Similar mechanisms exist in computers where, for example, we can suppress high-level cognitive functions by causing driver-level response to incoming information or force high-level attention and, thus, overwhelm reasoning by inducing conditions that lead to increased processing regimens.

The Recursive Nature of Deception

The interaction we have with targets in a deception is recursive in nature. To get a sense of this, consider that while we present observables to a target, the target is presenting observables to us. We can only judge the effect of our

deception based on the observables we are presented with and our prior expectations influence how we interpret these observables. The target may also be trying to deceive us, in which case, they are presenting us with the observables they think we expect to see, but at the same time, we may be deceiving them by presenting the observables we expect them to expect us to present. This goes back and forth potentially without end. It is covered by the well-known story.

> The Russian and U.S. ambassadors met at a dinner party and began discussing in their normal manner. When the subject came to the recent listening device, the Russian explains that they knew about it for some time. The American explains that they knew the Russians knew for quite a while. The Russian explains they knew the Americans knew they knew. The American explains that they knew the Russians knew that the Americans knew they knew. The Russian states that they knew they knew they knew they knew they knew they knew. The American exclaims, "I didn't know that!"

To handle recursion, it is generally accepted that you must first characterize what happens at a single level, including the links to recursion, but without delving into the next level those links lead to. Once your model of one level is completed, you then apply recursion without altering the single level model. We anticipate that by following this methodology, we will gain efficiency and avoid mistakes in understanding deceptions. At some level, for any real system, the recursion must end for there is ground truth. The question of where it ends deals with issues of confidence in measured observables and we will largely ignore this issue throughout the remainder of this chapter.

Large Systems Are Affected by Small Changes

In many cases, a large system can be greatly affected by small changes. In the case of deception, it is normally easier to make small changes without the deception being discovered than to directly make the large changes that are desired. The indirect approach then tells us that we should try to make changes that cause the right effects and go about it in an unexpected and indirect manner.

As an example of this, in a complex system with many people, not all participants have to be affected in order to cause the system to behave differently than it might otherwise. One method for influencing an organizational decision is to categorize the members into four categories: zealots in favor, zealots opposed, neutral parties, and willing participants. The object of this influence tactic in this case is to get the right set of people into the right categories.

> Example: Creating a small number of opposing zealots will stop an idea in an organization that fears controversy. Once the set of desired changes is understood, moves can be generated with the

> objective of causing these changes. For example, to get opposing zealots to reduce their opposition, you might engage them in a different effort that consumes so much of their time that they can no longer fight as hard against the specific item you wish to get moved ahead.

This notion of finding the right small changes and backtracking to methods to influence them seems to be a general principle of organizational deception, but there has only been limited work on characterizing these effects at the organizational level.

Even Simple Deceptions Are Often Quite Complex

In real attacks, things are not so simple as to involve only a single deception element against a nearly stateless system. Even relatively simple deceptions may work because of complex processes in the targets.

> As a simple example, we analyzed a specific instance of audio surveillance, which is itself a subclass of attack mechanism called audio/video viewing. In this case, we are assuming that the attacker is exploiting a little known feature of cellular telephones that allows them to turn on and listen to conversations without alerting the targets. This is a deception because the attacker is attempting to conceal the listening activity so that the target will talk when they otherwise might not, and it is a form of concealment because it is intended to avoid detection by the target. From the standpoint of the telephone, this is a deception in the form of simulation because it involves creating inputs that cause the telephone to act in a way it would not otherwise act (presuming that it could somehow understand the difference between owner intent and attacker intent — which it likely cannot). Unfortunately, this has a side effect.
>
> When the telephone is listening to a conversation and broadcasting it to the attacker, it consumes battery power at a higher rate than when it is not broadcasting and it emits radio waves that it would otherwise not emit. The first objective of the attacker would be to have these go unnoticed by the target. This could be enhanced by selective use of the feature so as to limit the likelihood of detection, again a form of concealment.
>
> But suppose the target notices these side effects. In other words, the inputs do get through to the target. For example, suppose the target notices that their new batteries don't last the advertised

8 hours, but rather last only a few hours, particularly on days when there are a lot of meetings. This might lead them to various thought processes. One very good possibility is that they decide the problem is a bad battery. In this case, the target's association function is being misdirected by their predisposition to believe that batteries go bad and a lack of understanding of the potential for abuse involved in cell phones and similar technologies. The attacker might enhance this by some form of additional information if the target started becoming suspicious, and the act of listening might provide additional information to help accomplish this goal. This would then be an act of simulation directed against the decision process of the target.

Even if the target becomes suspicious, they may not have the skills or knowledge required to be certain that they are being attacked in this way. If they come to the conclusion that they simply don't know how to figure it out, the deception is affecting their actions by not raising it to a level of priority that would force further investigation. This is a form of concealment causing them not to act.

Finally, even if they should figure out what is taking place, there is deception in the form of concealment in that the attacker may be hard to locate because they are hiding behind the technology of cellular communication.

But the story doesn't really end there. We can also look at the use of deception by the target as a method of defense. A wily cellular telephone user might intentionally assume they are being listened to some of the time and use deceptions to test out this proposition. The same response might be generated in cases where an initial detection has taken place. Before association to a bad battery is made, the target might decide to take some measurements of radio emissions. This would typically be done by a combination of concealment of the fact that the emissions were being measured and the inducement of listening by the creation of a deceptive circumstance (i.e., simulation) that is likely to cause listening to be used. The concealment in this case is used so that the target (who used to be the attacker) will not stop listening in, while the simulation is used to cause the target to act.

The complete analysis of this exchange is left as an exercise to the reader . . . good luck. To quote the immortal bard:

"Oh what a tangled web we weave when first we practice to deceive"

The Twelfth Night

Simple Deceptions Are Combined to Form Complex Deceptions

Large deceptions are commonly built up from smaller ones. For example, the commonly used "big con" plan[58] goes something like this: find a victim, gain the victim's confidence, show the victim the money, tell the tale, deliver a sample return on investment, calculate the benefits, send the victim for more money, take them for all they have, kiss off the victim, keep the victim quiet. Of these, only the first does not require deceptions. What is particularly interesting about this very common deception sequence is that it is so complex and yet works so reliably. Those who have perfected its use have ways out at every stage to limit damage if needed and they have a wide number of variations for keeping the target (called victim here) engaged in the activity.

Knowledge of the Target

The intelligence requirements for deception are particularly complex to understand because, presumably, the target has the potential for using deception to fool the attacker's intelligence efforts. In addition, seemingly minor items may have a large impact on our ability to understand and predict the behavior of a target. As was pointed out earlier, intelligence is a key to success in deception. But doing a successful deception requires more than just intelligence on the target. To get to high levels of surety against capable targets, it is also important to anticipate and constrain their behavioral patterns.

In the case of computer hardware and software, in theory, we can predict precise behavior by having detailed design knowledge. Complexity may be driven up by the use of large and complicated mechanisms (e.g., try to figure out why and when Microsoft Windows will next crash) and it may be very hard to get details of specific mechanisms (e.g., what specific virus will show up next). While generic deceptions (e.g., false targets for viruses) may be effective at detecting a large class of attacks, there is always an attack that will, either by design or by accident, go unnoticed (e.g., not infect the false targets). The goal of deceptions in the presence of imperfect knowledge (i.e., all real-world deceptions) is to increase the odds. The question of what techniques increase or decrease odds in any particular situation drives us toward deceptions that tend to drive up the computational complexity of differentiation between deception and nondeception for large classes of situations. This is intended to exploit the limits of available computational power by the target. The same notions can be applied to human deception. We never have perfect knowledge of a human target, but in various aspects, we can count on certain limitations. For example, overloading a human target with information will tend to make concealment more effective.

Example: One of the most effective uses of target knowledge in a large-scale deception was the deception attack against Hitler that supported the D-Day invasions of World War II. Hitler was specifically targeted in such a manner that he would personally prevent the German military from responding to the Normandy invasion. He was induced not to act when he otherwise would have by a combination of deceptions that convinced him that the invasion would be at Pas de Calais. They were so effective that they continued to work for as much as a week after troops were inland from Normandy. Hitler thought that Normandy was a feint to cover the real invasion and insisted on not moving troops to stop it.

The knowledge involved in this grand deception came largely from the abilities to read German encrypted Enigma communications and psychologically profile Hitler. The ability to read ciphers was, of course, facilitated by other deceptions such as over attribution of defensive success to radar. Code breaking had to be kept secret in order to prevent the changing of code mechanisms, and in order for this to be effective, radar was used as the excuse for being able to anticipate and defend against German attacks.[59]

Knowledge for Concealment

The specific knowledge required for effective concealment is details of detection and action thresholds for different parts of systems. For example, knowing the voltage used for changing a 0 to a 1 in a digital system leads to knowing how much additional signal can be added to a wire while still not being detected. Knowing the electromagnetic profile of target sensors leads to better understanding of the requirements for effective concealment from those sensors. Knowing how the target's doctrine dictates responses to the appearance of information on a command and control system leads to understanding how much of a profile can be presented before the next level of command will be notified. Concealment at any given level is attained by remaining below these thresholds.

Knowledge for Simulation

The specific knowledge required for effective simulation is a combination of thresholds of detection, capacity for response, and predictability of response. Clearly, simulation will not work if it is not detected and, therefore, detection thresholds must be surpassed. Response capacity and response predictability are typically for more complex issues.

Response capacity has to do with quantity of available resources and ability to use them effectively. For computers, we know pretty well the limits of computational and storage capacity as well as what sorts of computations can be done in how much time. While clever programmers do produce astonishing results, for those with adequate understanding of the nature of computation, these results lead clearly toward the nature of the breakthrough. We constantly face deceptions, perhaps self-deceptions, in the proposals we see for artificial intelligence in computer systems and can counter it based on the understanding of resource consumption issues. Similarly, humans have limited capacity for handling situations and we can predict these limits at some level generically and in specific through experiments on individuals. Practice may allow us to build certain capacities to an artificially high level. The use of automation to augment capacities is one of the hallmarks of human society today, but even with augmentation, there are always limits.

Response predictability may be greatly facilitated by the notions of cybernetic stability. As long as we do not exceed the capacity of the system to handle change, systems designed for stability will have predictable tendencies toward returning to equilibrium. One of the great advantages of term limits on politicians, particularly at the highest levels, is that each new leader has to be recalibrated by those wishing to target them. It tends to be easier to use simulation against targets that have been in place for a long time because their stability criteria can be better measured and tested through experiment.

Legality

There are legal limitations on the use of deception for those who are engaged in legal activities, while those who are engaged in illegal activities, risk jail or, in some cases, death for their deceptions.

In the civilian environment, deceptions are acceptable as a general rule unless they involve a fraud, reckless endangerment, or libel of some sort. For example, you can legally lie to your wife (although I would advise against it), but if you use deception to get someone to give you money, in most cases it is called fraud and carries a possible prison sentence. You can legally create deceptions to defeat attacks against computer systems, but there are limits to what you can do without creating potential civil liability. For example, if you hide a virus in software and it is stolen and damages the person who stole it or an innocent bystander; you may be subject to civil suit. If someone is injured as a side effect, reckless endangerment may be involved.

Police and other governmental bodies have different restrictions. For example, police may be subject to administrative constraints on the use of deceptions and, in some cases, there may be a case for entrapment if deceptions are used to create crimes that otherwise would not have existed.

For agencies like the CIA and National Security Agency (NSA), deceptions may be legally limited to affect those outside the U.S., while for other agencies, restrictions may require activities only within the U.S. Similar legal restrictions exist in most nations for different actions by different agencies of their respective governments. International law is less clear on how governments may or may not deceive each other, but in general, governmental deception is allowed and is widely used.

Military environments also have legal restrictions, largely as a result of international treaties. In addition, there are codes of conduct for most militaries and these include requirements for certain limitations on deceptive behavior. For example, it is against the Geneva convention to use a red cross or other similar markings in deceptions, to use the uniform of the enemy in combat (although use in other select circumstances may be acceptable), to falsely indicate a surrender as a feint, and to falsely claim there is an armistice in order to draw the enemy out. In general, there is the notion of good faith and certain situations where you are morally obligated to speak the truth. Deceptions are forbidden if they contravene any generally accepted rule or involve treachery or perfidy. It is especially forbidden to make improper use of a flag of truce, the national flag, the military insignia and uniform of the enemy, or the distinctive badges of the Geneva Convention.[60] Those violating these conventions risk punishment ranging up to summary execution in the field.

Legalities are somewhat complex in all cases and legal council and review should be considered before any questionable action.

Modeling Problems

From the field of game theory, many notions about strategic and tactical exchanges have been created. Unfortunately, game theory is not as helpful in these matters as it might be both because it requires that a model be made in order to perform analysis and because, for models as complex as the ones we are already using in deception analysis, the complexity of the resulting decision trees often become so large as to defy computational solution. Fortunately, there is at least one other way to try to meet this challenge. This solution lies in the area of "model-based situation anticipation and constraint."[61] In this case, we use large numbers of simulations to sparsely cover a very large space.

In each of these cases, the process of analysis begins with models. Better models generally result in better results, but sensitivity analysis has shown that we do not need extremely accurate models to get usable statistical results and meaningful tactical insight.[62] This sort of modeling of deception and the scientific investigation that supports accurate modeling in this area has not yet begun in earnest, but it seems certain that it must.

One of the keys to understanding deception in a context is that the deceptions are oriented toward the overall systems that are our targets. In order for

us to carry out meaningful analysis, we must have meaningful models. If we do not have these models, then we will likely create a set of deceptions that succeed against the wrong targets and fail against the desired targets and, in particular, we will most likely be deceiving ourselves.

The main problem we must first address is what to model. In our case, the interest lies in building more effective deceptions to protect systems against attacks.

These targets of such defensive deceptions vary widely and they may ultimately have to be modeled in detail independently of each other, but there are some common themes. In particular, we believe we will need to build cognitive models of computer systems, humans, and their interactions as components of target systems. Limited models of attack strengths and types associated with these types of targets exist[63] in a form amenable to simulation and analysis. These have not been integrated into a deception framework and development has not been taken to the level of specific target sets based on reasonable intelligence estimates.

There have been some attempts to model deceptions before invoking them in the past. One series of examples is the series of deceptions starting with the DTK,[64] leading to the D-Wall,[65] and then to the other projects. In these cases, increasingly detailed models of targets of defensive deceptions were made and increasingly complex and effective deceptions were achieved.

Unintended Consequences

Deceptions may have many consequences, and these may not all be intended when the deceptions are used. Planning to avoid unintended consequences and limit the effects of the deceptions to just the target raises complex issues.

> Example: When deception was first implemented to limit the effectiveness of computer network scanning technology, one side effect was to deceive the tools used by the defenders to detect their own vulnerabilities. In order for the deceptions to work against attackers, they also had to work against the defenders who were using the same technology.

In the case of these deception technologies, this is an intended consequence that causes defenders to become confused about their vulnerabilities. This then has to be mitigated by adjusting the results of the scanning mechanism based on knowledge of what is a known defensive deception. In general, these issues can be quite complex.

In this case, the particular problem is that the deception affected observables of cognitive systems other than the intended target. In addition, the responses of the target may indirectly affect others. For example, if we force targets to spend their money on one thing, the finiteness of the resource means that they will not spend that money on something else.

That something else, in a military situation, might include feeding their prisoners, who also happen to be our troops.

All deceptions have the potential for unintended consequences. From the deceiver's perspective this is then an operations security issue. If you do not tell your forces about a deception, you risk it being treated as real, while telling your own forces risks revealing the deception, either through malice or the natural difference between their response to the normal situation and the known deception.

Another problem is the potential for misassociation and misattribution. For example, if you are trying to train a target to respond to a certain action on your part with a certain action or inaction on their part, the method being used for the training may be misassociated by the target so that the indicators they use are not the ones you thought they would use. In addition, as the target learns from experiencing deceptions, they may develop other behaviors that are against your desires.

Counter Deception

Many studies appear in the psychological literature on counter deception,[66] but little work has been done on the cognitive issues surrounding computer-based deception of people and targeting computers for deception. No metrics relating to effectiveness of deception were shown in any study of computer-related deception we were able to find. The one exception is in the provisioning of computers for increased integrity, which is generally discussed in terms of honesty and truthfulness, freedom from unauthorized modification, and correspondence to reality. Of these, only freedom from unauthorized modification has been extensively studied for computer systems. There are studies that have shown that people tend to believe what computers indicate to them, but few of these are helpful in this context.

Pamela Kalbfleisch categorized counter deception in face-to-face interviews according to the following schema:[67]

- No nonsense
- Indifference
- Hammering
- Unkept secret
- Fait accompli
- Wages alone
- All alone
- Discomfort and relief
- Evidence bluff
- Imminent discovery
- Mum's the word
- Encouragement
- Elaboration
- Blaming
- Buildup of lies
- No explanations allowed
- Repetition
- Compare and contrast
- Provocation
- Question inconsistencies as they appear
- Exaggeration
- Embedded discovery
- A chink in the defense
- Self-disclosure
- Point of deception cues
- You are important to me

- No nonsense
- Diffusion of responsibility
- Just having fun
- Praise
- Excuses
- It is not so bad
- Others have done worse
- Blaming
- Empathy
- What will people think?
- Appeal to pride
- Direct approach
- Silence

It is also noteworthy that most of these counter-deception techniques themselves depend on deception and stem, perhaps indirectly, from the negotiation tactics of Karrass.[68]

Extensive studies of the effectiveness of counter-deception techniques have indicated that success rates with face-to-face techniques rarely exceed 60% accuracy and are only slightly better at identifying lies than truths. Even poorer performance result from attempts to counter deception by examining body language and facial expressions. As increasing levels of control are exerted over the subject, increasing care is taken in devising questions toward a specific goal, and increasing motivation for the subject to lie are used, the rate of deception detection can be increased with verbal techniques, such as increased response time, decreased response time, too consistent or pat answers, lack of description, too ordered a presentation, and other similar indicators. The aide of a polygraph device can increase accuracy to about 80% detection of lies and more than 90% detection of truths for very well structured and specific sorts of questioning processes.[69]

The limits of the target in terms of detecting deception lead to limits on the need for high fidelity in deceptions. The lack of scientific studies of this issue inhibits current capabilities to make sound decisions without experimentation.

Summary

The following table summarizes the dimensions and issues involved:

Limited resources lead to controlled focus of attention	By pressuring or taking advantage of pre-existing circumstances, focus of attention can be stressed. In addition, focus can be inhibited, enhanced, and through the combination of these, redirected.
All deception is a composition of concealments and simulations	Concealments inhibit observation whereas simulations enhance observation. When used in combination they provide the means for redirection.
Memory and cognitive structure force uncertainty, predictability, and novelty	The limits of cognition force the use of rules of thumb as shortcuts to avoid the paralysis of analysis. This provides the means for inducing desired behavior through the discovery and exploitation of these rules of thumb in a manner that restricts or avoids higher-level cognition.

Time, timing, and sequence are critical	All deceptions have limits in planning time, time to perform, time until effect, time until discovery, sustainability, and sequences of acts.
Observables limit deception	Target, target allies, and deceiver observables limit deception and deception control.
Operational security is a requirement	Determining what needs to be kept secret involves a tradeoff that requires metrics in order to properly address.
Cybernetics and system resource limitations	Natural tendencies to retain stability lead to potentially exploitable movement or retention of stability states.
The recursive nature of deception	Recursion between parties leads to uncertainty that cannot be perfectly resolved, but that can be approached with an appropriate basis for association to ground truth.
Large systems are affected by small changes	For organizations and other complex systems, finding the key components to move and finding ways to move them forms a tactic for the selective use of deception to great effect.
Even simple deceptions are often quite complex	The complexity of what underlies a deception makes detailed analysis a substantial task.
Simple deceptions are combined to form complex deceptions	Big deceptions are formed from small subdeceptions and yet they can be surprisingly effective.
Knowledge of the target	Knowledge of the target is one of the key elements in effective deception.
Legality	There are legal restrictions on some sorts of deceptions and these must be considered in any implementation.
Modeling problems	There are many problems associated with forging and using good models of deception.
Unintended consequences	You may fool your own forces, create misassociations, and create misattributions. Collateral deception has often been observed.
Counter-deception	Target capabilities for counter-deception may result in deceptions being detected.

A Model for Human Deception

By looking extensively at the literature on human cognition and deception, a model was formed of human cognition with specific focus on its application to deception. This includes Lambert's data collection and mapping into his model of human deception.

Lambert's Cognitive Model

We begin with Lambert's model of human cognition.[70] This model is linked to the history of psychological models of brain function and cognition and, as such, does not represent so much the physiology of the brain as the things

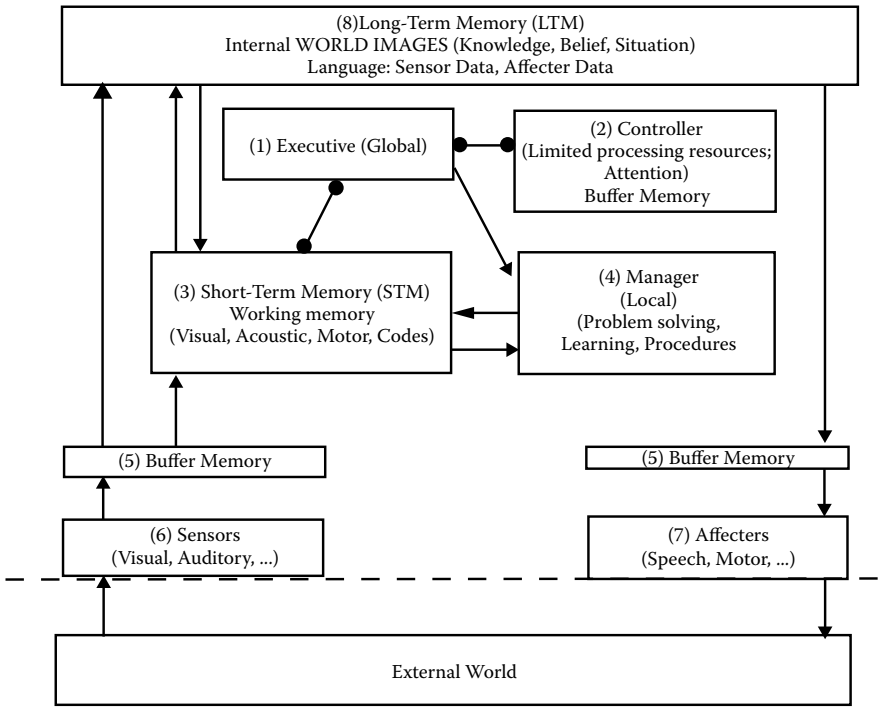


Figure 6.1 System components of the cognitive model.

it is generally believed to do and the manner in which it is generally believed to operate. There is no sense that this model will be found to match physiology in the long run; however, it is useful because it relates to a great deal of other experimental work that has been done on deception and the limits of human perception. It may also be related to Perceptual Control Theories (PCT) notions of orders of control and, through that mechanistic view, to physiology.[71]

Lambert's model identifies integers as labels for major brain functions (Figure 6.1). Within this model, Lambert has created a structure of subprocesses identified with behavior in general and deception in particular. This structure is broken down into subsections as follows. In addition to the structural association, Lambert created a detailed mapping of how cognitive function was thought to work. The structure can be interpreted as a stimulus response network, but there is an isomorphism to a model-referenced adaptive control system. The components consist of (1) the global executive; (2) a controller with limited processing resources and buffer memory; (3) short-term memory and working memory, which includes visual acoustic, motor, and coded memories; (4) the local manager that does problem solving, learning, and procedures; (5) buffer memories for both input and

output; (6) sensors, which include transducers for the senses; (7) affecters, which includes transducers for all outputs; and (8) long-term memory, which includes internal images of the world (knowledge, belief, and situation) and language (sensor data and affecter data).

The model provides for specific interconnections between components that appear to occur in humans. Specifically, long-term memory is affected only by short-term memory, but affects short-term memory and buffer memories for sensors and affecters. The executive sends information to the local manager and acts in a controlling function over short-term memory and the controller. The short-term memory interacts with the long-term memory, receives information from sensor buffers, and interacts with the local manager. The local manager receives information from the global executive and interacts with the short-term memory. The sensor observes reflections of the world and sends the resulting signals through incoming buffer memory to short and long-term memory. Long-term memory feeds information to output buffers that then pass the information on to affecters.

This depiction is reflected in a different structure that models the system processes of cognition (Figure 6.2).

In this depiction of Lambert's model of cognition, we see the movement of information from senses through a cognitive process that includes reflexes, conditioned behavior, intuition, and reasoning, and a movement back down to action. Many more details are provided, but this is the general structure of cognition with which Lambert worked. From a standpoint of understanding deception, the notion is that the reflections of the world that reach the senses of the cognition system are interpreted based on its present state. The deception objective is to control those reflections so as to produce the desired changes in the perception of the target so as to achieve compliance. This can be done by inhibiting or inducing cognitive activities within this structure.

The induction of signals at the sense level is relatively obvious, and the resulting reflexive responses are quite predictable in most cases. The problems start becoming considerable as higher levels of the victim's cognitive structure get involved. While the mechanism of deception may involve the perception of feature, any feedback from this can only be seen as a result of conditioned behaviors at the perceive form level or higher level cognitive affects reflected in the ultimate drives of the system. For this reason, while the model may be helpful in understanding internal states, affects at the perceive feature level are aliased as affects at higher levels. Following the earlier depiction of deceptions as consisting of inhibitions and inducements of sensor data, we can think of internal effects of deception on cognition in terms of combinations of inhibitions and inducements of internal signals. The objective of a deception might then, for example, be the inhibition of sensed content from being perceived as a feature, perhaps accomplished by a combination

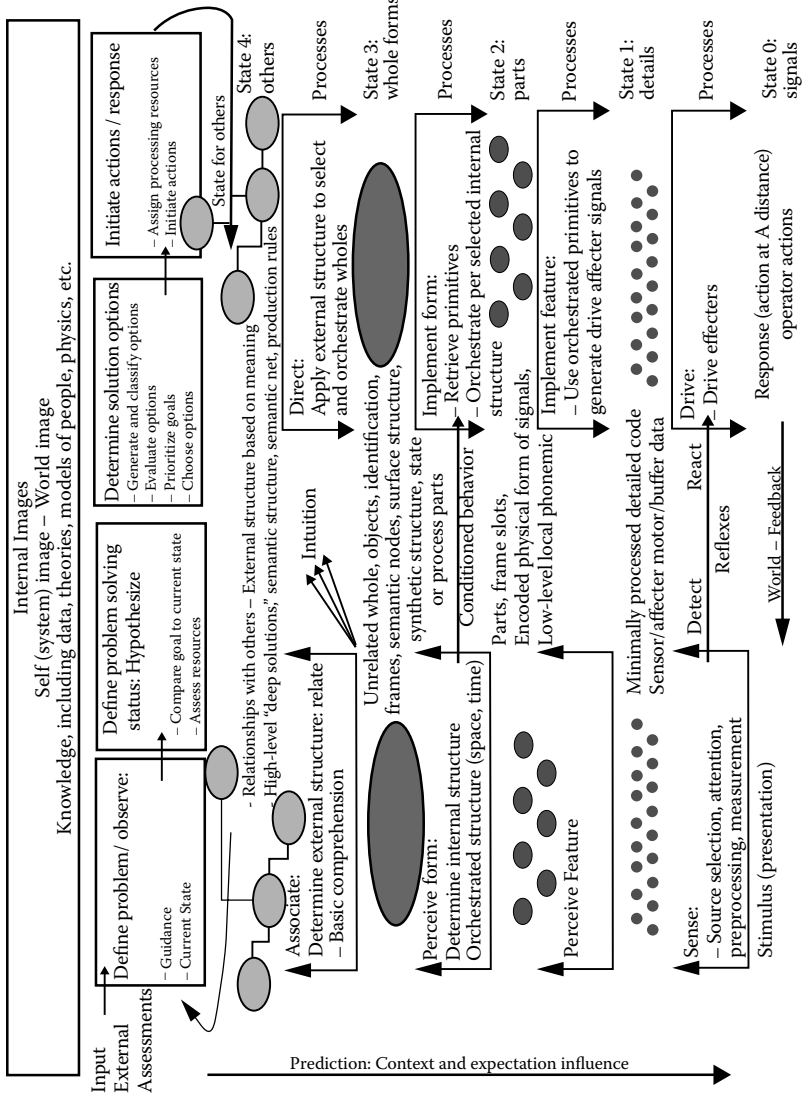


Figure 6.2 System processes of the cognitive model.

of reducing the available signal and distracting focus of attention by inducing the perception of a different form and causing a simultaneous reflexive action to reduce the available signal. This is precisely what is done in the case of the disappearing elephant magic trick. The disappearing elephant trick is an excellent example of the exploitation of the cognitive system and can be readily explained through Lambert's model.

> Example: This trick is set up by the creation of a rippling black silk curtain behind the elephant, which is gray. The audience is in a fairly close pack staring right at the elephant some distance away. Just before the elephant disappears, a scantily clad woman walks across the front of the crowd and the magician is describing something that is not very interesting with regard to the trick. Then, as eyes turn toward the side the girl is walking toward, a loud crash sound is created to that side of the crowd. The crowd's reflexive response to a crashing sound is to turn toward the sound, which they do. This takes about one third to one half second. As soon as they are looking that way, the magician causes another black silk rippling curtain to rise up in front of the elephant. This takes less than one quarter second. Because of the low contrast between the elephant and the curtain and the rippling effect of the black back and front curtains, there is no edge line induced in the audience and, thus, attention is not pulled toward the curtains. By the time the crowd looks back, the elephant is gone and is then moved away while out of sight. The back curtain is lowered, and the front curtain is then raised to prove that only the wall remains behind the curtain.

For low-level, one-step deceptions such as this one, Lambert's model is an excellent tool both for explanation and for planning. There are a set of known sensors, reflexes, and even well known or trainable conditioned responses that can be exploited almost at will. In some cases, it will be necessary to force the cognitive system into a state where these prevail over higher-level controlling processes, such as a member of the crowd who is focusing very carefully on what is going on. This can be done by boring them into relaxation, which the magician tries to do with his boring commentary and the more interesting scantily clad woman, but otherwise it is pretty straightforward. Unfortunately, this model provides inadequate structure for dealing with higher-level or longer-term cognitive deceptions. For these, you need to move to another sort of model that, while still consistent with this model, provides added clarity regarding possible moves.

A Cognitive Model for Higher-Level Deceptions

The depiction below attempts to provide additional structure for higher-level cognitive deceptions. This model starts to look at how humans interact to create deceptions and how those deceptions can, at a broad level, cause interpretation and behavior in the target that is compliant with the deceiver. It also shows the recursive nature of deception because of the regress induced by both time and symmetry.

Model of Human Cognition for Deceptions

Figure 6.3 shows interaction between two human or group cognitive systems. The interaction all takes place through the world using human senses (smell, taste, hearing, touching, seeing, pheromones, and allergic reactions). Deception is modeled by the induction or suppression of target observables by the deceiver.

Cognitive processes responding directly to inputs include sensory data, which, after sensor bias and the filter of a set of observables, become observable. Sensory data, after bias, can trigger reflexive responses, which also induce observable internal changes. Other actions can also be generated and expectations actively control everything in this list. Focus of attention can also be affected at this level because of detection mechanisms and their triggering of higher-level processes. This paragraph summarizes what we will tentatively call the "low-level" cognitive system.

Cognitive processes in, what we tentatively call, the middle level of cognition include conditioned and other automatic but nonreflexive responses, measurement mechanisms, and automatic or trained evaluation and decision methods, learned and nearly automated capabilities including skills, tools, and methods that are based on pattern matching, training, instinctual responses, the actions they trigger, and the feedback mechanisms involved in controlling those actions. This level also involves learned patterns of focus of attention.

The remaining cognitive processes are called high level. This includes reason-based assessments and capabilities, expectations, which include biases, fidelity of interest, level of effort, consistency with observables, and high-level focus of attention, and intent, which includes objectives, qualitative evaluation, schedule, and budgetary requirements. The link between expectations and the rest of the cognitive structure is particularly important because expectations alter focus of attention sequences, cognitive biases, assessment, intent, and the evaluation of expectations, while changing of expectation can keep them stable, moves them at a limited rate, or cause dissonance.

Deceptions of Low-Level Cognition

In this model, we have collapsed the lower levels (up to conditioned response) of Lambert's model into the bottom two boxes (observables and ACTIONS)

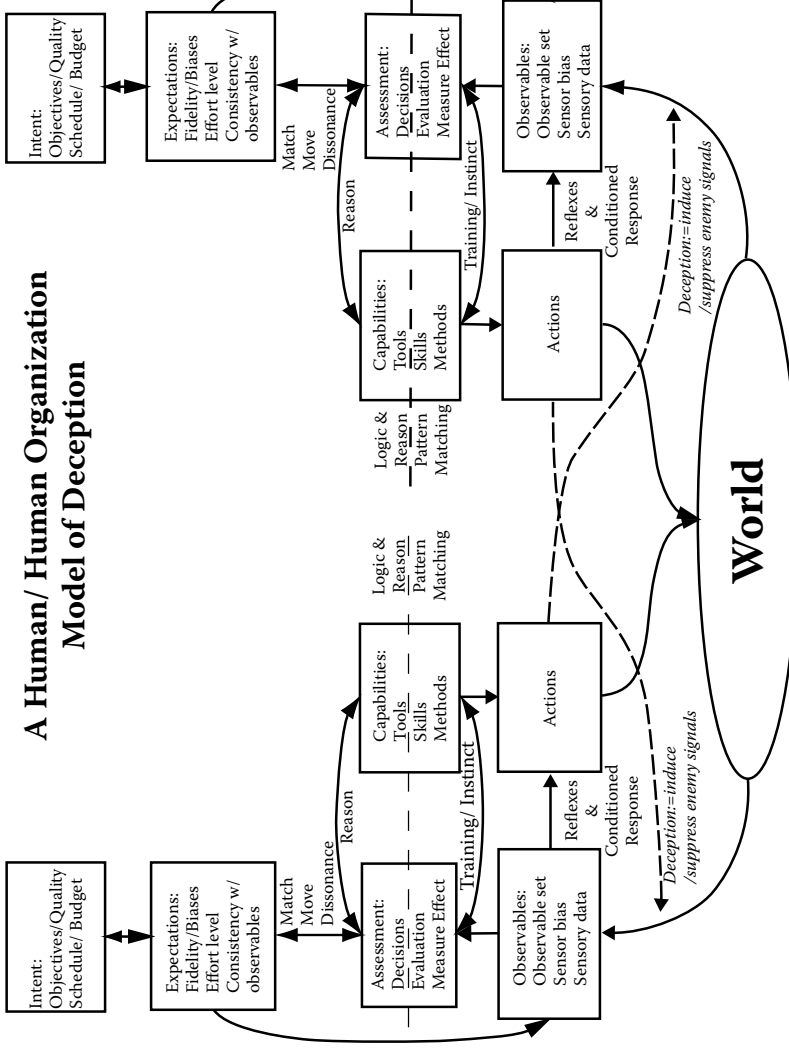


Figure 6.3 A human/human organization model of deception.

and created a somewhat more specific higher-level structure. Details of these deceptions are provided in Section 6 and Section 7 of Lambert's data collection. Low-level visual deceptions are demonstrated by Seckel[72] and described by Hoffman.[73] Audio deceptions are demonstrated on an audio CD-ROM by Deutsch.[74]

Deceptions of Mid-Level Cognition

The notion is that there are pattern matching and reason-based assessments and capabilities that interact to induce more thoughtful decisions than conditioned response. While pattern matching cognition mechanisms are more thoughtful than conditioned response, they are essentially the programmed behaviors identified by Cialdini[75] and some of the negotiation tactics of Karrass.[76] These include, but are not limited to, reciprocation, authority, contrast, commitment and consistency, automaticity, social proof, liking, and scarcity, and as Karrass formulates it, credibility, message content and appeal, situation setting and rewards, and media choice are all methods.

The potential for decisions to be moved to more logical reasoning exists, but this is limited by the effects identified by Gilovich.[77] Specifically, the notions that people (erroneously) believe that effects should resemble their causes, they misperceive random events, they misinterpret incomplete or unrepresentative data, they form biased evaluations of ambiguous and inconsistent data, they have motivational determinants of belief, they form bias of second-hand information, and they have exaggerated impressions of social support. More content is provided in the Sections 1, 2, and some portions of 4 and 8 of Lambert's data collection.

Deceptions of High-Level Cognition

Karrass[78] also provides techniques for affecting influence in high-level thoughtful situations. He explains that change comes from learning and acceptance. Learning comes from hearing and understanding, whereas acceptance comes from comfort with the message, relevance, and good feelings toward the underlying idea. These are both affected by audience motives and values, the information and language used for presentation, audience attitudes and emotions, and the audience's perception and role in the negotiation. Karrass provides a three-dimensional depiction of goals, needs, and perceptions and asserts that people are predictable. He also provides a set of tactics including timing, inspection, authority, association, amount, brotherhood, and detour that can be applied in a deception context. Handy[79] also provides a set of influence tactics that tend to be most useful at higher levels of reasoning, including physicality, resources, position (which yields information, access, and right to organize), expertise, personal charisma, and emotion. More content is also provided in Section 4 and Section 8 of Lambert's data collection.

Moving from High-Level to Mid-Level Cognition

Karrass also augments Cialdini's notions[80] of rush, stress, uncertainty, indifference, distraction, and fatigue leading to less thoughtful and more automatic responses and brings out Maslow's needs hierarchy (basic survival, safety, love, self-worth, and self-actualization). By forcing earlier sets of these issues, reasoning can be driven away and replaced by increased automaticity. Tactics of timing can also be used to drive people toward increased automaticity. Thus, we can either drive the target toward less thought or use Karrass's methods of negotiation to cause desired change.

Moving from Mid-Level to High-Level Cognition

Cognition moves to higher levels only when there are intent-based forcing factors that lead to deeper analysis (e.g., when objectives are oriented toward more in-depth thought, quality requirements drive more detailed consideration, schedule availability provides free time to do deeper consideration, or extra budget is available for this purpose) or when expectations are not met (i.e., the fidelity of the deception is inadequate, biases trigger more detailed examination, inconsistencies or errors are above some threshold, or the difference between expectations and observations is so great or changing at so great a rate as to cause dissonance). In these cases, higher levels of reasoning are applied, complete with all of their potential logical fallacies and their special skills, tools, and methods. Higher-level reasoning is desired when we wish to change intent or make radical changes in expectations, while we try to drive decisions to lower cognitive levels when we can induce less thoughtful responses in our favor.

An Example

To get a sense of how the model might be applied to deceptions, we have included a sample analysis of a simple human deception. The deception is an attack with a guard at a gate as the target. It happens many times each day and is commonly called tailgating.

> The target of this deception is the guard and our method will be to try to exploit a natural overload that takes place during the return from lunch hour on a Thursday. We choose the end of the lunch hour on Thursday because the guard will be as busy as they ever get and because they will be looking forward to the weekend and will probably have a somewhat reduced alertness level. Thus, we are intentionally trying to keep processing at a pattern-matching level by increased rush, stress, indifference, distraction, and fatigue.
>
> We stand casually out of the guard's sight before the crowd comes along, join the crowd as it approaches the entry, hold a

notepad where a badge appears on other peoples' attire, and stay away from the guard's side of the group. Our clothing and appearance is such that it avoids dissonance with the guard's expectations and does not affect the guard's intent in any obvious way.

We tag along in the third row back near someone that looks generally like us and, when the guard is checking one of the other people, we ease our way over to the other side of the guard, appearing to be in the already checked group. Here we are using automaticity and social proof against the guard and liking by similarity against the group we are tailgating with. We are also using similarity to avoid triggering sensory detection and indifference, distraction and fatigue to avoid triggering higher-level cognition.

As the group proceeds, so do we. After getting beyond the guard's sight, we move to the back of the group and drop out as they round a corner. Here we are using automaticity, liking, and social proof against the group to go along with them, followed by moving slowly out of their notice, which exploits slow movement of expectations followed by concealment from observation.

Team members have used variations on this entry technique in red teaming exercises against facilities from time to time and have been almost universally successful in its use. It is widely published and well known to be effective. It is clearly a deception because if the guard knew you were trying to get past without a badge or authorization they would not permit the entry. While the people who use it do not typically go through this analytical process at a conscious level, they do some part of it at some level and we postulate that this is why they succeed at it so frequently.

As an aside, there should always be a backup plan for such deceptions. The typical tailgater, if detected, will act lost and ask the guard how to get to some building or office, perhaps finding out that this is the wrong address in the process. This again exploits elements of the deception framework designed to move the guard away from high-level cognition and toward automaticity that would favor letting the attacker go and not reporting the incident.

In the control system isomorphism, we can consider this same structure as attempting to maintain internal consistency and allow change only at a limited rate. The high-level control system is essentially oblivious to anything unless change happens at too high a rate or deviations of high-level signals from expectations are too high. Similarly, the middle levels operate using Cialdini's rules of thumb unless a disturbance at a lower level prompts obvious dissonance and low-level control decisions (e.g., remain balanced) do not get above the reflexive and conditioned response levels unless there is a control system failure.

A Model for Computer Deception

In looking at computer deceptions, it is fundamental to understand that the computer is an automaton. Anthropomorphizing it into an intelligent being is a mistake in this context, a self-deception. Fundamentally, deceptions must cause systems to do things differently based on their lack of ability to differentiate deception from a nondeception. Computers cannot really yet be called "aware" in the sense of people. Therefore, when we use a deception against a computer, we are really using a deception against the skills of the human that design, program, and use the computer.

In many ways, computers could be better at detecting deceptions than people because of their tremendous logical analysis capability and the fact that the logical processes used by computers are normally quite different than the processes used by people. This provides some level of redundancy and, in general, redundancy is a way to defeat corruption. Fortunately, for those of us looking to do defensive deception against automated systems, most of the designers of modern attack technology have a tendency to minimize their programming effort and, thus, tend not to include a lot of redundancy in their analysis.

People use shortcuts in their programs just as they use shortcuts in their thinking. Their goal is to get to an answer quickly and in many cases without adequate information to make definitive selections. Computer power and memory are limited just like human brainpower and memory are limited. In order to make efficient use of resources, people write programs that jump to premature conclusions and fail to completely verify content. In addition, people who observe computer output have a tendency to believe it. Therefore, if we can deceive the automation used by people to make decisions, we may often be able to deceive the users and avoid in-depth analysis.

Our model for computer deception starts with Cohen's "Structure of Intrusion and Intrusion Detection."[81] In this model, a computer system and its vulnerabilities are described in terms of intrusions at the hardware, device driver, protocol, operating system (OS), library and support function, application, recursive language, and meaning vs. content levels. The levels are all able to interact, but they usually interact hierarchically with each level interacting with the ones just above and below it. This model is depicted in Figure 6.4.

Model of Computer Cognition with Deceptions

This model is based on the notion that at every level of the computer's cognitive hierarchy signals can either be induced or inhibited. The normal process is shown in black, whereas inhibitions are shown as grayed out signals, and induced signals are shown in red. All of these affect memory states and processor activities at other, typically adjacent, levels of the cognitive system.

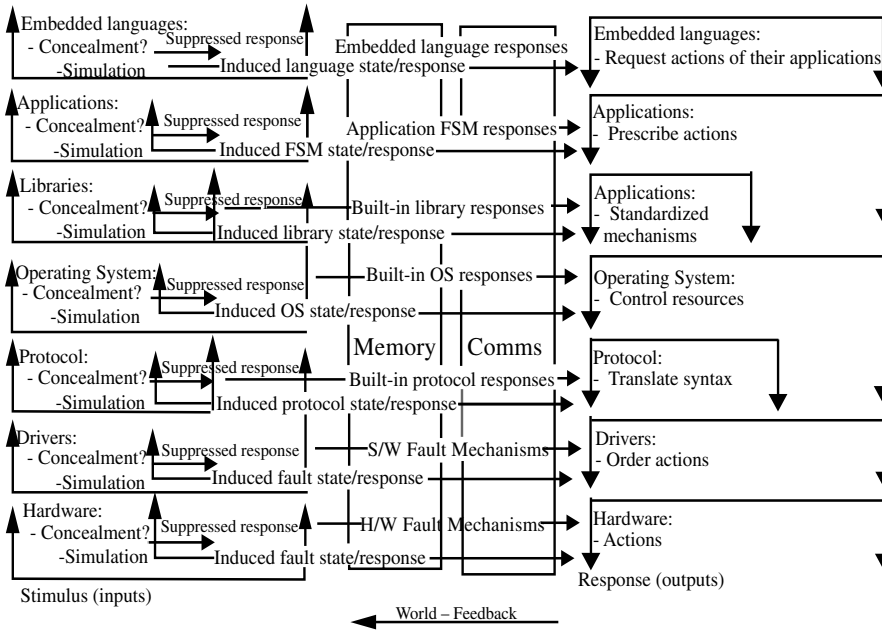


Figure 6.4 Model of computer deceptions.

Deception detection and response capabilities are key issues in the ability to defend against deceptions, so there is a concentration on the limits of detection in the following discussions.

Hardware-Level Deceptions

If the hardware of a system or network is altered, it may behave arbitrarily differently than expected. While there is a great deal of history of tamper-detection mechanisms for physical systems, no such mechanism is or likely ever will be perfect. The use of intrusion detection systems (IDSs) for detecting improper modifications to hardware today consist primarily of built-in self-test mechanisms, such as the power on self test (POST) routine in a typical personal computer (PC). These mechanisms are designed to detect specific sorts of random stochastic fault types and are not designed to detect malicious alterations. Thus, deception of these mechanisms is fairly easy to do without, otherwise altering their value in detecting fault types they already detect.

Clearly, if the hardware is altered by a serious intruder, this sort of test will not be revealing. Motion sensors, physical seals of different sorts, and even devices that examine the physical characteristics of other devices are all examples of intrusion detection techniques that may work at this level. In software, we may detect alterations in external behavior due to hardware

modification, but this is only effective in large-scale alterations, such as the implanting of additional infrastructure. This is also likely to be ignored in most modern systems because intervening infrastructure is rarely known or characterized as part of intrusion detection and operating environments are intentionally designed to abstract details of the hardware.

Intrusions can also be the result of the interaction of hardware of different sorts rather than the specific use of a particular type of hardware. This type of intrusion mechanism appears to be well beyond the capability of current technology to detect or analyze. Deceptions exploiting these interactions will, therefore, likely go undetected for extended periods of time. Hardware-level deceptions designed to induce desired observables are relatively easy to create and hard to detect. Induction of signals requires only knowledge of protocol and proper design of devices.

The problem with using hardware-level deception for defense against serious threat types is that it requires physical access to the target system or logical access with capabilities to alter hardware level functions (e.g., microcode access). This tends to be difficult to attain against intelligence targets, if attempted against insiders it introduces deceptions that could be used against the defenders, and in the case of overrun, it does not seem feasible. That is not to say that we cannot use deceptions that operate at the hardware level against systems, but rather that affecting their hardware level is likely to be infeasible.

Driver-Level Deceptions

Drivers are typically ignored by intrusion detection and other security systems. They are rarely inspected, in modern OS they can often be installed from or by applications, and they usually have unlimited hardware access. This makes them prime candidates for exploitations of all sorts, including deceptions.

A typical driver-level deception would cause the driver to process items of interest without passing information to other parts of the operating environment or to exfiltrate information without allowing the system to notice that this activity was happening. It would be easy for the driver to cause widespread corruption of arbitrary other elements of the system as well as inhibiting the system from seeing undesired content.

From a standpoint of defensive deceptions, drivers are very good target candidates. A typical scenario is to require that a particular driver be installed in order to gain access to defended sites. This is commonly done with applications like RealAudio. Once the target loads the required driver, hardware-level access is granted and arbitrary exploits can be launched. This technique is offensive in nature and may violate rules of engagement in a military setting or induce civil or criminal liability in a civilian setting. Its use for defensive purposes may be overly aggressive.

Protocol-Level Deceptions

Many protocol intrusions have been demonstrated, ranging from exploitations of flaws in the IP protocol suite to flaws in cryptographic protocols. Except for a small list of known flaws that are part of active exploitations, most current IDSs do not detect such vulnerabilities. In order to fully cover such attacks, it would likely be necessary for such a system to examine and model the entire network state and effects of all packets and be able to differentiate between acceptable and unacceptable packets.

Although this might be feasible in some circumstances, the more common approach is to differentiate between protocols that are allowed and those that are not. Increasing granularity can be used to differentiate based on location, time, protocol type, packet size and makeup, and other protocol-level information. This can be done today at the level of single packets or, in some circumstances, limited sequences of packets, but it is not feasible for the combinations of packets that come from different sources and might interact within the end systems. Large-scale effects can sometimes be detected, such as aggregate bandwidth utilization, but without a good model of what is supposed to happen, there will always be malicious protocol sequences that go undetected. There are also interactions between hardware and protocols. For example, there may be an exploitation of a particular hardware device, which is susceptible to a particular protocol state transition, resulting in a subtle alteration to normal timing behaviors. This might then be used to exfiltrate information based on any number of factors, including very subtle covert channels.

Defensive protocol level deceptions have proven relatively easy to develop and hard to defeat. DTK[82] and D-Wall[83] both use protocol-level deceptions to great effect and these are relatively simplistic mechanisms compared to what could be devised with substantial time and effort. This appears to be a ripe area for further work. Most intelligence gathering today starts at the protocol level, overrun situations almost universally result in communication with other systems at the protocol level, and insiders generally access other systems in the environment through the protocol level.

Operating System-Level Deceptions

At the OS level, there are a very large number of intrusions possible, and not all of them come from packets that come over networks. Users can circumvent OS protection in a wide variety of ways. For a successful IDS to work, it has to detect this before the attacker gains the access necessary to disable the intrusion detection mechanisms (the sensors, fusion, analysis, or response elements or the links between them can be defeated to avoid successful detection). In the late 1980s, a lot of work was done in the limitations of the ability of systems to protect themselves and integrity-based self-defense mechanisms were implemented that could do a reasonable job of detecting

alterations to OS.[84] These systems are not capable of defeating attacks that invade the OS without altering files and reenter the OS from another level after the system is functioning. Process-based intrusion detection has also been implemented with limited success. Thus, we see that OS level deceptions are commonplace and difficult to defend against.

Any host-based IDS and the analytical part of any network-based IDS involve some sort of operating environment that may be defeatable. But even if defeat is not directly attainable, denial of services against the components of the IDS can defeat many IDS mechanisms, replay attacks may defeat keep-alive protocols used to counter these denial of service attacks, selective denial of service against only desired detections are often possible, and the list goes on and on. If the OS are not secure, the IDS have to win a battle of time in order to be effective at detecting things it is designed to detect.

Thus, we see that the induction or suppression of signals into the IDS can be used to enhance or cover OS-level deceptions that might otherwise be detected.

OS can have complex interactions with other OS in the environment as well as between the different programs operating within the OS environment. For example, variations in the timing of two processes might cause race conditions that are extremely rare, but which can be induced through timing of otherwise valid external factors. Heavy usage periods may increase the likelihood of such subtle interactions, and thus the same methods that would not work under test conditions may be inducible in live systems during periods of high load. An IDS would have to detect this condition and, of course, because of the high load the IDS would be contributing to the load as well as susceptible to the effects of the attack. A specific example is the loading of a system to the point where there are no available file handles in the system tables. At this point, the IDS may not be able to open the necessary communications channels to detect, record, analyze, or respond to an intrusion.

OS may also have complex interactions with protocols and hardware conditions, and these interactions are extremely complex to analyze. To date, nobody has produced an analysis of such interactions as far as we are aware. Thus, deceptions based on mixed levels including the OS are likely to be undetected as deceptions.

Of course, an IDS cannot detect all of the possible OS attacks. There are systems that can detect known attacks, detect anomalous behavior by select programs, and so forth, but again, a follow-up investigation is required in order for these methods to be effective, and a potentially infinite number of attacks exist that do not trip anomaly detection methods. If the environment can be characterized closely enough, it may be feasible to detect the vast majority of these attacks, but even if you could do this perfectly, there is then the library and support function level intrusion that must be addressed.

OS are the most common point of attack against systems today largely because they afford a tremendous amount of cover and capability.

They provide cover because of their enormous complexity and capability. They have unlimited access within the system and the ability to control the hardware so as to yield arbitrary external effects and observables. They try to control access to themselves and, thus, higher-level programs do not have the opportunity to measure them for the presence of deceptions. They also seek to protect themselves from the outside world so that external assessment is blocked. While they are not perfect at either of these types of protection, they are effective against the rest of the cognitive system they support. As a location for deception, they are prime candidates.

To use defensive deception at the target's OS level requires offensive actions on the part of the deceiver and yields only indirect control over the target's cognitive capability. This has to then be exploited in order to affect deceptions at other levels and this exploitation may be very complex depending on the specific objective of the deception.

Library- and Support Function-Level Intrusions

Libraries and support functions are often embedded within a system and are largely hidden from the programmer so that their role is not as apparent as either OS calls or application-level programs. A good example of this is in languages like C wherein the language has embedded sets of functions that are provided to automate many of the functions that would otherwise have to be written by programmers. For example, the C strings library includes a wide range of widely used functions. Unfortunately, the implementations of these functions are not standardized and often contain errors that become embedded in every program in the environment that uses them. Library-level intrusion detection has not been demonstrated at this time other than by the change detection methodology supported by the integrity-based systems of the late 1980s and behavioral detection at the OS level. Most of the IDS mechanisms themselves depend on libraries.

An excellent recent example is the use of leading zeros in numerical values in some UNIX systems. On one system call, the string -08 produces an error, whereas in another, it is translated into the integer -8. This was traced to a library function that is very widely used. It was tested on a wide range of systems with different results on different versions of libraries in different operating environments. These libraries are so deeply embedded in operating environments and so transparent to most programmers that minor changes may have disastrous effects on system integrity and produce enormous opportunities for exploitation. Libraries are almost universally delivered in loadable form only so that source codes are only available through considerable effort. Trojan horses, simple errors, or system-to-system differences in libraries can make even the most well written and secure applications an opportunity for exploitation. This includes system applications, commonly

considered part of the OS, service applications, such as web servers, accounting systems, and databases, and user level applications including custom programs and host-based IDSs.

The high level of interaction of libraries is a symptom of the general intrusion detection problem. Libraries sometimes interact directly with hardware, such as the libraries that are commonly used in special device functions like writing CD-rewritable disks. In many modern OS, libraries can be loaded as parts of device drivers that become embedded in the OS itself at the hardware control level. A hardware device with a subtle interaction with a library function can be exploited in an intrusion, and the notion that any modern IDS would be able to detect this is highly suspect. While some IDS systems might detect some of the effects of this sort of attack, the underlying loss of trust in the operating environments resulting from such an embedded corruption is plainly outside of the structure of intrusion detection used today.

Using library functions for defensive deceptions offers great opportunity, but, like OS, there are limits to the effectiveness of libraries because they are at a level below that used by higher level cognitive functions, and thus there is great complexity in producing just the right effects without providing obvious evidence that something is not right.

Application-Level Deceptions

Applications provide many new opportunities for deceptions. The apparent user interface languages offer syntax and semantics that may be exploited, whereas the actual user interface languages may differ from the apparent languages because of programming errors, back doors, and unanticipated interactions. Internal semantics may be in error, may fail to take all possible situations into account, or there may be interactions with other programs in the environment or with state information held by the operating environment. They always trust the data they receive so that false content is easily generated and efficient. These include most intelligence tools, exploits, and other tools and techniques used by severe threats. Known attack detection tools and anomaly detection have been applied at the application level with limited success. Network detection mechanisms also tend to operate at the application level for select known application vulnerabilities.

As in every other level, there may be interactions across levels. The interaction of an application program with a library may allow a remote user to generate a complex set of interactions causing unexpected values to appear in interprogram calls, within programs, or within the OS itself. It is most common for programmers to assume that system calls and library calls will not produce errors, and most programming environments are poor at handling all possible errors. If the programmer misses a single exception — even

one that is not documented because it results from an undiscovered error in an interaction that was not anticipated — the application program may halt unexpectedly, produce incorrect results, pass incorrect information to another application, or enter an inconsistent internal state. This may be under the control of a remote attacker who has analyzed or planned such an interaction. Modern IDSs are not prepared to detect this sort of interaction.

Application-level defensive deceptions are very likely to be a major area of interest because applications tend to be driven more by time to market than by surety and because applications tend to directly influence the decision processes made by attackers. For example, a defensive deception would typically cause a network scanner to make wrong decisions and report wrong results to the intelligence operative using it. Similarly, an application-level deception might be used to cause a system that is overrun to act on the wrong data. For systems administrators, the problem is somewhat more complex and it is less likely that application-level deceptions will work against them.

Recursive Languages in the Operating Environment

In many cases, application programs encode Turing Machine-capable embedded languages, such as a language interpreter. Examples include Java, Basic, Lisp, APL, and Word Macros. If these languages can interpret user-level programs, there is an unlimited possible set of embedded languages that can be devised by the user or anybody the user trusts. Clearly, an IDS cannot anticipate all possible errors and interactions in this recursive set of languages. This is an undecidable problem that no IDS will ever likely be able to address. Current IDS systems only address this to the extent that anomaly detection may detect changes in the behavior of the underlying application, but this is unlikely to be effective.

These recursive languages have the potential to create subtle interactions with all other levels of the environment. For example, such a language could consume excessive resources, use a graphical interface to make it appear as if it were no longer operating while actually interpreting all user input and mediating all user output, test out a wide range of known language and library interactions until it found an exploitable error, and so on. The possibilities are literally endless. All attempts to use language constructs to defeat such attacks have failed to date, and even if they were to succeed to a limited extent, any success in this area would not be due to intrusion detection capabilities.

It seems that no IDS will ever have a serious hope of detecting errors induced at these recursive language levels as long as we continue to have user-defined languages that we trust to make decisions affecting substantial value. Unless the IDS is able to "understand" the semantics of every level of the implementation and make determinations that differentiate desirable intent

from malicious intent, the IDS cannot hope to mediate decisions that have implications on resulting values. This is clearly impossible.

Recursive languages are used in many applications, including many intelligence and systems administration applications. In cases where this can be defined or understood or cases where the recursive language itself acts as the application, deceptions against these recursive languages should work in much the same manner as deceptions against the applications themselves.

The Meaning of the Content Vs. Realities

Content is generally associated with meaning in any meaningful application. The correspondence between content and realities of the world cannot reasonably be tracked by an IDS, is rarely tracked by applications, and cannot practically be tracked by other levels of the system structure because it is highly dependent on the semantics of the application that interprets it. Deceptions often involve generating human misperceptions or causing people to do the wrong thing based on what they see at the user interface. In the end, if this wrong thing corresponds to making a different decision than is supposed to be made, but still a decision that is a feasible and reasonable one in a slightly different context, only somebody capable of making the judgment independently has any hope of detecting the error.

Only certain sorts of input redundancy are known to be capable of detecting this sort of intrusion and this becomes cost prohibitive in any large-scale operation. This sort of detection is used in some high surety critical applications, but not in most intelligence applications, most overrun situations, or by most systems administrators. The programmers of these systems call this "defensive programming" or some such thing and tend to fight against its use.

Attackers commonly use what they call "social engineering" (a.k.a., perception management) to cause the human operator to do the wrong thing. Of course, such behavioral changes can ripple through the system as well, ranging from entering wrong data to changing application-level parameters to providing system passwords to loading new software updates from a website to changing a hardware setting. All of the other levels are potentially affected by this sort of interaction.

Ultimately, deception in information systems intended to affect other systems or people will cause results at this level and, thus, all deceptions of this sort are well served to consider this level in their assessments.

Commentary

Unlike people, computers do not typically have ego, but they do have built-in expectations and in some cases automatically seek to attain "goals." If those expectations and goals can be met or encouraged while carrying out the deception, the computers will fall prey just as people do.

In order to be very successful at defeating computers through deception, there are three basic approaches. One approach is to create as high a fidelity deception as you can and hope that the computer will be fooled. Another is to understand what data the computer is collecting and how it analyzes the data provided to it. The third is to alter the function of the computer to comply with your needs. The high fidelity approach can be quite expensive but should not be abandoned out of hand. At the same time, the approach of understanding enemy tools can never be done definitively without a tremendous intelligence capability. The modification of cognition approach requires an offensive capability that is not always available and is quite often illegal, but all three avenues appear to be worth pursuing.

High Fidelity

High fidelity deception of computers with regard to their assessment, analysis, and use against other computers tends to be fairly easy to accomplish today using tools like D-Wall[85] and the Invisible Router (IR) effort associated with this project. D-Wall created high fidelity deception by rerouting attacks toward substitute systems. The IR does a very similar process in some of its modes of operation. The notion is that by providing a real system to attack, the attacker is suitably entertained. While this is effective in the generic sense, for specific systems, additional effort must be made to create the internal system conditions indicative of the desired deception environment. This can be quite costly. These deceptions tend to operate at a protocol level and are augmented by other technologies to affect other levels of deception.

Defeating Specific Tools

Many specific tools are defeated by specific deception techniques. For example, nmap and similar scans of a network seeking out services to exploit are easily defeated by tools like the DTK.[86] More specific attack tools; such as Back Orafice (BO), can be directly countered by specific emulators such as "NoBO"— a PC-based tool that emulates a system that has already been subverted with BO. Some deception systems work against substantial classes of attack tools.

Modifying Function

Modifying the function of computers is relatively easy to do and is commonly used in attacks. The question of legality aside, the technical aspects of modifying function for defense falls into the area of counterattack and, thus, is not a purely defensive operation. The basic plan is to gain access, expand privileges, induce desired changes for ultimate compliance, leave those changes

in place, periodically verify proper operation, and exploit as desired. In some cases, privileges gained in one system are used to attack other systems as well. Modified function is particularly useful for getting feedback on target cognition.

The intelligence requirements of defeating specific tools may be severe, but the extremely low cost of such defenses makes them appealing. Against off-the-Internet attack tools, these defenses are commonly effective and, at a minimum, increase the cost of attack far more than they affect the cost of defense. Unfortunately, for more severe threats, such as insiders, overrun situations, and intelligence organizations, these defenses are often inadequate. They are almost certain to be detected and avoided by an attacker with skills and access of this sort. Nevertheless, from a standpoint of defeating the automation used by these types of attackers, relatively low-level deceptions have proven effective. In the case of modifying target systems, the problems become more severe in the case of more severe threats. Insiders are using your systems, so modifying them to allow for deception allows for self-deception and enemy deception of you. For overrun conditions, you rarely have access to the target system, so unless you can do very rapid and automated modification, this tactic will likely fail. For intelligence operations, this requires that you defeat an intelligence organization one of whose tasks is to deceive you. The implications are unpleasant and inadequate study has been made in this area to make definitive decisions.

There is a general method of deception against computer systems being used to launch fully automated attacks against other computer systems. The general method is to analyze the attacking system (the target) in terms of its use of responses from the defender and create sequences of responses that emulate the desired responses to the target. Because all such mechanisms published or widely used today are quite finite and relatively simplistic, with substantial knowledge of the attack mechanism, it is relatively easy to create a low-quality deception that will be effective. It is noteworthy, for example, that the DTK, which was made publicly available in source form in 1998, is still almost completely effective against automated intelligence tools attempting to detect vulnerabilities. It seems that the widely used attack tools are not yet being designed to detect and counter deception.

That is not to say that red teams and intelligence agencies are not beginning to start to look at this issue. For example, in private conversations with defenders against select elite red teams, the question often comes up of how to defeat the attackers when they undergo a substantial intelligence effort directed at defeating their attempts at deceptive defense. The answer is to increase the fidelity of the deception. This has associated costs, but as the attack tools designed to counter deception improve, so will the requirement for higher fidelity in deceptions.

Deception Mechanisms for Information Systems

This content is extracted from a previous paper on attack mechanisms[87] and is intended to summarize the attack mechanisms that are viable deception techniques against information systems — in the sense that they induce or inhibit cognition at some level. All of the attack techniques in the original paper may be used as parts of overall deception processes, but only these are specifically useful as deception methods and specifically oriented toward information technology as opposed to the people that use and control these systems. We have explicitly excluded mechanisms used for observation only and included examples of how these techniques affect cognition and, thus, assist in deception and added information about deception levels in the target system.

Mechanism	Levels
Cable cuts	HW
Fire	HW
Flood	HW
Earth movement	HW
Environmental control loss	HW
System maintenance	All
Trojan horses	All
Fictitious people	All
Resource availability manipulation	HW, OS
Spoofing and masquerading	All
Infrastructure interference	HW
Insertion in transit	All
Modification in transit	All
Sympathetic vibration	All
Cascade failures	All
Invalid values on calls	OS and up
Undocumented or unknown function exploitation	All
Excess privilege exploitation	App, Driver
Environment corruption	All
Device access exploitation	HW, Driver
Modeling mismatches	App and up
Simultaneous access exploitations	All
Implied trust exploitation	All
Interrupt sequence mishandling	Driver, OS
Emergency procedure exploitation	All
Desychronization and time-based attacks	All
Imperfect daemon exploits	Lib, App
Multiple error inducement	All
Viruses	All
Data diddling	OS and up
Electronic interference	HW
Repair-replace-remove information	All
Wire closet attacks	HW

Mechanism	Levels
Process bypassing	All
Content-based attacks	Lib and up
Restoration process corruption or misuse	Lib and up
Hang-up hooking	HW, Lib, Driver, OS
Call forwarding fakery	HW
Input overflow	All
Illegal value insertion	All
Privileged program misuse	App, OS, Driver
Error-induced misoperation	All
Audit suppression	All
Induced stress failures	All
False updates	All
Network service and protocol attacks	HW, Driver, Proto
Distributed coordinated attacks	All
Man-in-the-middle	HW, Proto
Replay attacks	Proto, App, and up
Error insertion and analysis	All
Reflexive control	All
Dependency analysis and exploitation	All
Interprocess communication attacks	OS, Lib, Proto, App
Below-threshold attacks	All
Peer relationship exploitation	Proto, App, and up
Piggybacking	All
Collaborative misuse	All
Race conditions	All
Kiting	App and up
Salami attacks	App and up
Repudiation	App and up

Models of Deception of More Complex Systems

Larger cognitive systems can be modeled as being built up from smaller cognitive subsystems through some composition mechanism. Using these combined models, we may analyze and create larger scale deceptions. To date, there is no really good theory of composition for these sorts of systems and attempts to build theories of composition for security properties of even relatively simple computer networks have proven rather difficult. We can also take a top-down approach, but without the ability to link top-level objectives to bottom-level capabilities and without metrics for comparing alternatives, the problem space grows rapidly and results cannot be meaningfully compared.

Human Organizations

Humans operating in organizations and groups of all sorts have been extensively studied, but deception results in this field are quite limited. The work of

Karrass[88] (described earlier) deals with issues of negotiations involving small groups of people, but is not extended beyond that point. Military intelligence failures make good examples of organizational deceptions in which one organization attempts to deceive another. Hughes-Wilson describes failures in collection, fusion, analysis, interpretation, reporting, and listening to what intelligence is saying as the prime causes of intelligence blunders, and at the same time, indicates that generating these conditions generally involved imperfect, organizationally oriented deceptions by the enemy.[89] John Keegan details a lot of the history of warfare and along the way described many of the deceptions that resulted in tactical advantage.[90] Dunnigan and Nofi detail many examples of deception in warfare and, in some cases, detail how deceptions have affected organizations.[91] Strategic military deceptions have been carried out for a long time, but the theory of how the operations of groups lead to deception has never really been worked out. What we seem to have, from the time of Sun Tzu[92] to the modern day[93] is sets of rules that have withstood the test of time. Statements like: *"It is far easier to lead a target astray by reinforcing the target's existing beliefs,"*[94] are stated and restated without deeper understanding, without any way to measure the limits of its effectiveness, and without a way to determine what beliefs an organization has. It sometimes seems we have not made substantial progress from when Sun Tzu originally told us that "All warfare is based on deception."

The systematic study of group deception has been under way for some time. In 1841, Mackay released his still famous and widely read book titled *Extraordinary Popular Delusions and the Madness of Crowds*[95] in which he gives detailed accounts of the history of the largest scale deceptions and financial "bubbles" of history to that time. It is astounding how relevant this is to modern times. For example, the recent bubble in the stock market related to the emergence of the Internet is incredibly similar to historical bubbles, as are the aftermaths of all of these events. The self-sustaining unwarranted optimism, the self-fulfilling prophecies, the participation even by the skeptics, the exit of the originators, and the eventual bursting of the bubble to the detriment of the general public, all seem to operate even though the participants are well aware of the nature of the situation. While Mackay offers no detailed psychological accounting of the underlying mechanisms, he clearly describes the patterns of behavior in crowds that lead to this sort of group insanity.

Charles Handy[96] describes how power and influence work in organizations. This leads to methods by which people with different sorts of power create changes in the overall organizational perspective and decision process. In deceptions of organizations, models of who stands where on which issues and methods to move them are vital to determining who to influence and in what manner in order to get the organization to move (Figure 6.5).

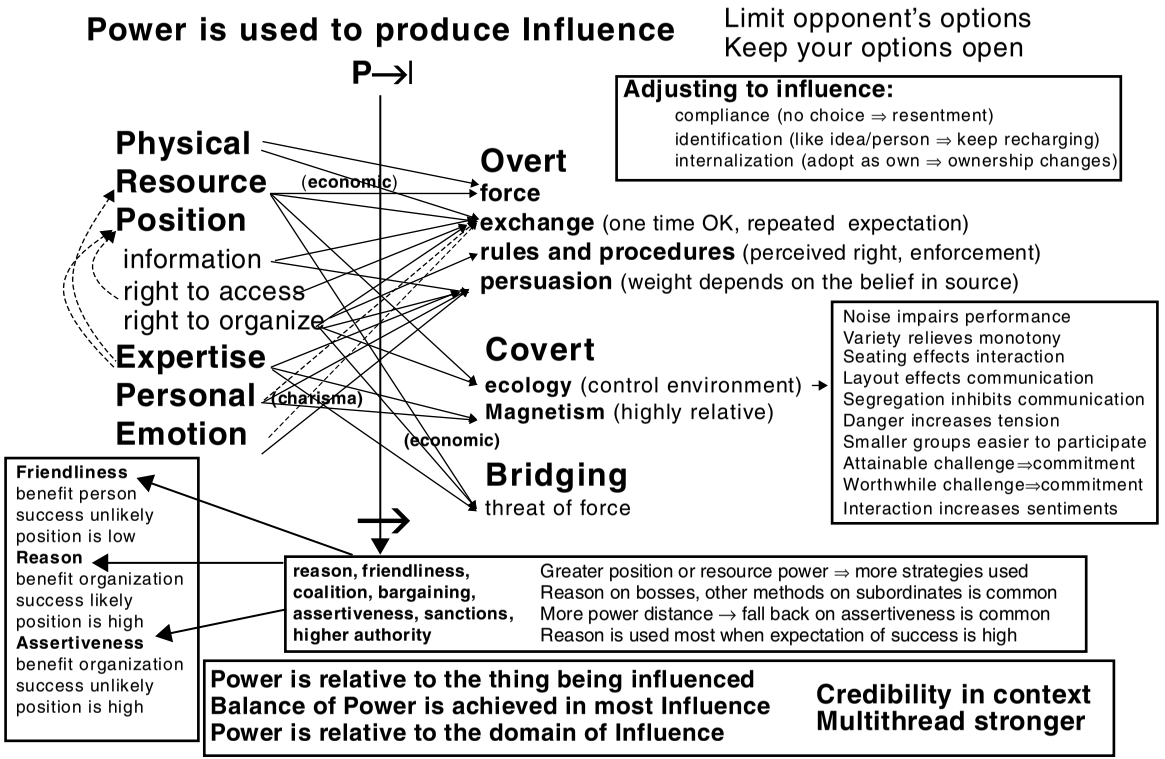


Figure 6.5 Power is used to produce influence.

Power and Influence in Human Organizations

These principles have been applied without rigor and with substantial success for a long time.

> Example: In World War II Germany, Hitler was the target of many of the allied strategic deceptions because the German organs of state were designed to grant him unlimited power. It didn't matter that Rommel believed that the allies would attack at Normandy because Hitler was convinced that they would strike at Pas de Calais. All dictatorial regimes tend to be swayed by influencing the mind of a single key decision maker. At the same time we should not make the mistake of believing that this works at a tactical level. The German military in World War II was highly skilled at local decision making and field commanders were trained to innovate and take charge when in command.

Military hierarchies tend to operate this way to a point; however, most military juntas have a group decision process that significantly complicates this issue. For example, the Revolutionary Armed Forces of Columbia (FARC) have councils that make group decisions and cannot be swayed by convincing a single authority figure. Swaying the U.S. is a very complex process, whereas swaying Iraq is considerably easier, at least from a standpoint of identifying the target of deceptions. The previously cited works on individual human deception certainly provide us with the requisite rational for explaining individual tendencies and the creation of conditions that tend to induce more advantageous behaviors in select circumstances, but how this translates into groups is a somewhat different issue.

Organizations have many different structures, but those who study the issue[97] have identified four classes of organizational structure that are most often encountered and which have specific power and influence associations: hierarchy, star, matrix, and network. In hierarchies, orders come from above and reporting is done from lower level to higher level in steps. Going "over a supervisor's head" is considered bad form and is usually punished. These sorts of organizations tend to be driven by top-level views and it is hard to influence substantial action except at the highest levels. In a star system, all personnel report to a single central point. In small organizations, this works well, but the center tends to be easily overloaded as the organization grows or as more and more information is fed into it. Matrix organizations tend to cause all of the individuals to have to serve more than one master (or at least manager). In these cases, there is some redundancy, but the risk of inconsistent messages from above and selective information below exists. In a network organization, people form cliques and there is a tendency for information not to get everywhere it might be helpful to have it. Each organizational type

has its features and advantages, and each has different deception susceptibility characteristics resulting from these structural features. Many organizations have mixes of these structures within them.

Deceptions within a group typically include: (1) members deceive other members, (2) members deceive themselves (e.g., "group think"), and (3) leader deceives members. Deception between groups typically include (1) leader deceives leader and (2) leader deceives own group members. Self-deception applies to the individual acting alone.

> Example: "Group think", in which the whole organization may be mislead due to group processes/social norms. Many members of the German population in World War II became murderous even though under normal circumstances they never would have done the things they did.

Complex organizations require more complex plans for altering decision processes. An effective deception against a typical government or large corporation may involve understanding a lot about organizational dynamics and happens in parallel with other forces that are also trying to sway the decision process in other directions. In such situations, the movement of key decision makers in specific ways tends to be critical to success, and this in turn depends on gaining access to their observables and achieving focus or lack of focus when and where appropriate. This can then lead to the need to gain access to those who communicate with these decision makers, their sources, and so forth.

> Example: In the roll-up to the Faulkland Islands war between Argentina and the United Kingdom, the British were deceived into ignoring signs of the upcoming conflict by ignoring the few signs they say, structuring their intelligence mechanisms so as to focus on things the Argentines could control, and believing the Argentine diplomats who were intentionally asserting that negotiations were continuing when they were not. In this example, the Argentines had control over enough of the relevant sensory inputs to the British intelligence operations so that groupthink was induced.

Many studies have shown that optimal group sizes for small tightly knit groups tend to be in the range of four to seven people. For tactical situations, this is the typical human group size. Whether the group is running a command center, a tank, or a computer attack team, smaller groups tend to lack cohesion and adequate skills, whereas larger groups become harder to manage in tight situations. It would seem that for tactical purposes, deceptions would be more effective if they could be successful at targeting a group of this size. Groups of this sort also have a tendency to have specialties with cross-limited training. For example, in a computer attack group, a different individual will likely be an expert on one OS as opposed to another. A hardware expert, a fast systems

programmer/administrator, appropriate OS and other domain experts, an information fusion person, and a skilled Internet collector may emerge. No systematic testing of these notions has been done to date, but personal experience shows it to be true. Recent work in large group collaboration using information technology to augment normal human capabilities has shown limited promise. Experiments will be required to determine whether this is an effective tool in carrying out or defeating deceptions, as well as how such a tool can be exploited so as to deceive its users.

The National Research Council[98] discusses models of human and organizational behavior and how automation has been applied in the modeling of military decision making. This includes a wide range of computer-based modeling systems that have been developed for specific applications and is particularly focused on military and combat situations. Some of these models would appear to be useful in creating effective models for simulation of behavior under deceptions and several of these models are specifically designed to deal with psychological factors. This field is still very new and the progress to date is not adequate to provide coverage for analysis of deceptions; however, the existence of these models and their utility for understanding military organizational situations may be a good foundation for further work in this area.

Computer Network Deceptions

Computer network deceptions essentially never exist without people involved. The closest things we see to purely computer-to-computer deceptions have been feedback mechanisms that induce live locks or other denial of service impacts. These are the result of misinformation passing between computers.

> Examples include the electrical cascade failures in the U.S. power grid,[99] telephone system cascade failures causing widespread long distance service outages,[100] and intersystem cascades, such as power failures bringing down telephone switches required to bring power stations back up.[101]

But the notion of deception, as we define it, involves intent, and we tend to attribute intent only to human actors at this time. There are, of course, programs that display goal directed behavior, and we will not debate the issue further except to indicate that, to date, this has not been used for the purpose of creating network deceptions without human involvement.

Individuals have used deception on the Internet since before it became the Internet. In the Internet's predecessor, the ARPAnet, there were some rudimentary examples of email forgeries in which email was sent under an alias — typically as a joke. As the Internet formed and became more widespread,

these deceptions continued in increasing numbers and with increasing variety. Today, person-to-person and person-to-group deception in the Internet is commonplace and very widely practiced as part of the notion of anonymity that has pervaded this media. Some examples of papers in this area include:

> "Gender Swapping on the Internet"[102] was one of the original "you can be anyone on the Internet" descriptions. It dealt with players in MUDs (Multi-User Dungeon), which are multiple-participant virtual reality domains. Players soon realized that they could have multiple online personalities, with different genders, ages, and physical descriptions. The mind behind the keyboard often chooses to stay anonymous, and without violating system rules or criminal laws, it is difficult or impossible for ordinary players to learn many real-world identities.
>
> "Cybernetic Fantasies: Extended Selfhood in a Virtual Community" by Mimi Ito, from 1993,[103] is a first-person description of a Multi-User Dungeon (MUD) called Farside, which was developed at a university in England. By 1993 it had 250 players. Some of the people using Farside had characters they maintained in 20 different virtual reality MUDs. Ito discusses previous papers, in which some people went to unusual lengths, such as photos of someone else, to convince others of a different physical identity.
>
> "Dissertation: A Chatroom Ethnography" by Mark Peace,[104] is a more recent study of Internet Relay Chat (IRC), a very popular form of keyboard-to-keyboard communication. This is frequently referred to as Computer Mediated Communication (CMC). Describing first-person experiences and observation, Peace believes that many users of IRC do not use false personalities and descriptions most of the time. He also provides evidence that IRC users do use alternate identities.
>
> Daniel Chandler writes, "In a 1996 survey in the U.S., 91% of homepage authors felt that they presented themselves accurately on their web pages (though only 78% believed that other people presented themselves accurately on their home pages!)"[105]

Criminals have moved to the Internet environment in large numbers and use deception as a fundamental part of their efforts to commit crimes and conceal their identities from law enforcement. While the specific examples are too numerous to list, there are some common threads, among them that the same criminal activities that have historically worked person-to-person are being carried out over the Internet with great success.

Identity theft is one of the more common deceptions based on attacking computers. In this case, computers are mined for data regarding an individual

and that individual's identity is taken over by the criminal who then commits crimes under the assumed name. The innocent victim of the identity theft is often blamed for the crimes until they prove themselves innocent.

One of the most common Internet-based deceptions is an old deception of sending a copier supply bill to a corporate victim. In many cases, the internal controls are inadequate to differentiate a legitimate bill from a fraud and the criminal gets paid illegitimately.

Child exploitation is commonly carried out by creating friends under the fiction of being the same age and sex as the victim. Typically, a 40-year-old pedophile will engage a child and entice them into a meeting outside the home. In some cases, there have been resulting kidnappings, rapes, and even murders.

During the cyber conflict between the Palestinian Liberation Organization (PLO) and a group of Israeli citizens that started early in 2001, one PLO cyber terrorist lured an Israeli teenager into a meeting and kidnapped and killed the teen. In this case, the deception was the simulation of a new friend made over the Internet.

> The Internet "war" assumed new dimensions here last week, when a 23-year-old Palestinian woman, posing as an American tourist, apparently used the Internet to lure a 16-year-old Israeli boy to the Palestinian Authority areas so he could be murdered.
>
> Hanan Sher, *The Jerusalem Report, 2001/02/10*

Larger scale deceptions have also been carried out over the Internet. For example, one of the common methods is to engage a set of "shills" who make different points toward the same goal in a given forum. While the forum is generally promoted as being even handed and fair, the reality is that anyone who says something negative about a particular product or competitor will get lambasted. This has the social effect of causing distrust of the dissenter and furthering the goals of the product maker. The deception is that the seemingly independent members are really part of the same team or, in some cases, the same person. In another example, a student at a California university made false postings to a financial forum that drove down the price of a stock that the student had invested in derivatives of. The net effect was a multimillion dollar profit for the student and the near collapse of the stock.

The largest scale computer deceptions tend to be the result of computer viruses. Like the mass hysteria of a financial bubble, computer viruses can cause entire networks of computers to act as a rampaging group. It turns out that the most successful viruses today use human behavioral characteristics to induce the operator to foolishly run the virus, which, on its own, could not reproduce. They typically send an email with an infected program as an attachment. If the infected program is run it then sends itself in email to

other users this user communicates with, and so forth. The deception is the method that convinces the user to run the infected program. To do this, the program might be given an enticing name, or the message may seem like it was really from a friend asking the user to look at something, or perhaps the program is simply masked so as to simulate a normal document.

> In one case a computer virus was programmed to silently dial out on the user's phone line to a telephone number that generated revenues to the originator of the virus (a 900 number). This example shows how a computer system can be attacked while the user is completely unaware of the activity.

These are deceptions that act across computer networks against individuals who are attached to the network. They are targeted at the millions of individuals who might receive them and, through the viral mechanism, distribute the financial burden across all of those individuals. They are a form of a "Salami" attack in which small amounts are taken from many places with large total effect.

Implications

These examples would tend to lead us to believe that effective defensive deceptions against combinations of humans and computers are easily carried out to substantial effect, and indeed that appears to be true, if the only objective is to fool a casual attacker in the process of breaking into a system from outside or escalating privilege once they have broken in. For other threat profiles, however, such simplistic methods will not likely be successful and certainly not remain so for long once they are in widespread use. Indeed, all of these deceptions have been oriented only toward being able to observe and defend against attackers in the most direct fashion and not oriented toward the support of larger deceptions, such as those required for military applications.

There have been some studies of interactions between people and computers. Some of the typical results include the notions that people tend to believe things the computers tell them, humans interacting through computers tend to level differences of stature, position, and title, that computer systems tend to trust information from other computer systems excessively, that experienced users interact differently than less experienced ones, the ease of lying about identities and characteristics as demonstrated by numerous stalking cases, and the rapid spread viruses as an interaction between systems with immunity to viruses (by people) for limited time periods. The Tactical Decision Making Under Stress (TADMUS) program is an example of a system designed to mitigate decision errors caused by cognitive overload, which have been documented through research and experimentation.[106]

Sophisticated attack groups tend to be small, on the order of four to seven people in one room or operate as a distributed group perhaps as many as 20 people can loosely participate. Most of the most-effective groups have apparently been small cells of four to seven people or individuals with loose connections to larger groups. Based on activities seen to date, but without a comprehensive study to back these notions up, less than a hundred such groups appear to be operating overtly today, and perhaps a thousand total groups would be a good estimate based on the total activities detected in openly available information. A more accurate evaluation would require additional research, specifically including the collection of data from substantial sources, evaluation of operator and group characteristics (e.g., times of day, preferred targets, typing characteristics, etc.), and tracking of modus operandi of perpetrators. In order to do this, it would be prudent to start to create sample attack teams and do substantial experiments to understand the internal development of these teams, team characteristics over time, team makeup, develop capabilities to detect and differentiate teams, and test out these capabilities in a larger environment. Similarly, the ability to reliably deceive these groups will depend largely on gaining understanding about how they operate.

We believe that large organizations are only deceived by strategic application of deceptions against individuals and small groups. While we have no specific evidence to support this, ultimately it must be true to some extent because groups do not make decisions without individuals making decisions. While there may be different motives for different individuals and group's insanity of a sort may be part of the overall effect, there nevertheless must be specific individuals and small groups that are deceived in order for them to begin to convey the overall message to other groups and individuals. Even in the large-scale perception management campaigns involving massive efforts at propaganda, individual opinions are affected first, small groups follow, and then larger groups become compliant under social pressures and belief mechanisms.

Thus, the necessary goal of creating deceptions is to deceive individuals and then small groups that those individuals are part of. This will be true until targets develop far larger scale collaboration capabilities that might allow them to make decisions on a different basis or change the cognitive structures of the group as a whole. This sort of technology is not available at present in a manner that would reduce effectiveness of deception and it may never become available.

Clearly, as deceptions become more complex and the systems they deal with include more and more diverse components, the task of detailing deceptions and their cognitive nature becomes more complex. It appears that there is regular structure in most deceptions involving large numbers of systems because the designers of current widespread attack deceptions have limited resources. In such cases, it appears that a relatively small number of factors

can serve to model the deceptive elements; however, large-scale group deception effects may be far more complex to understand and analyze because of the large number of possible interactions and complex sets of interdependences involved in cascade failures and similar phenomena. If deception technology continues to expand and analytical and implementation capabilities become more substantial, there is a tremendous potential for highly complex deceptions wherein many different systems are involved in highly complex and irregular interactions. In such an environment, manual analysis will not be capable of dealing with the issues and automation will be required in order to both design the deceptions and counter them.

Experiments and the Need for an Experimental Basis

One of the more difficult things to accomplish in this area is meaningful experiments. While a few authors have published experimental results in information protection, far fewer have attempted to use meaningful social science methodologies in these experiments or to provide enough testing to understand real situations. This may be because of the difficulty and high cost of each such experiment and the lack of funding and motivation for such efforts. We have identified this as a critical need for future work in this area.

If one thing is clear from our efforts, it is the fact that too few experiments have been done to understand how deception works in defense of computer systems and, more generally, too few controlled experiments have been done to understand the computer attack and defense processes and to characterize them. Without a better empirical basis, it will be hard to make scientific conclusions about such efforts.

While anecdotal data can be used to produce many interesting statistics, the scientific utility of those statistics is very limited because they tend to reflect only those examples that people thought worthy of calling out. We get only "*lies, damned lies, and statistics.*"

Experiments to Date

From the time of the first published results on honey pots, the total number of published experiments performed in this area appears to be very limited. While there have been hundreds of published experiments by scores of authors in the area of human deception, refereed articles on computer deception experiments can be counted on one hand.

Experiments on Test Subjects at Sandia National Laboratories

Originally, a few examples of real world effects of deception were provided,[107] but no scientific studies of the effects of deception on test subjects were performed. While it did provide a mathematical analysis of the statistics of

deception in a networked environment, there was no empirical data to confirm or refute these results.[108] Subsequent experiments produced a series of results that have not been independently verified, but appear to be accurate based on the available data. In these experiments, forensically sound images of systems and configurations were used to create repeatable configurations that were presented to groups of attackers. These attack groups were given specific goals for their efforts and were measured by a number of metrics using a combination of observations by experiment monitors, videotaping of sessions, which were analyzed, and forms that were filled out as individuals and then as a group at the end of each 4-hour session. Attack progress was measured over time relative to an attack graph with progress toward the deception indicated as negative progress and progress toward the real objective indicated as positive progress. These were all open-ended experiments designed so that the attack group would never be able to complete the task, but so that progress could be measured. An example result shows attackers not under deception and attackers under deception (Figure 6.6).

In the example provided here, the deception was extremely effective, but it was not as effective in all examples. Nevertheless, deception was shown to be very effective in all of the experiments with attackers generally taking longer to make progress and making less progress over time under deception than attackers not under deception. But results were far more interesting than this when repetition of a single experiment was undertaken with the same groups for week after week (Figure 6.7).

In this sequence of experiments, the same attack groups were run through the same situation for 3 weeks in a row. After the first week, one of the groups

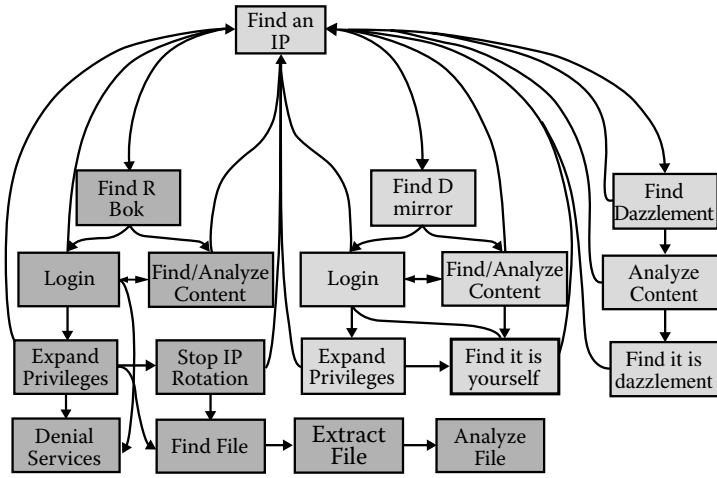


Figure 6.6

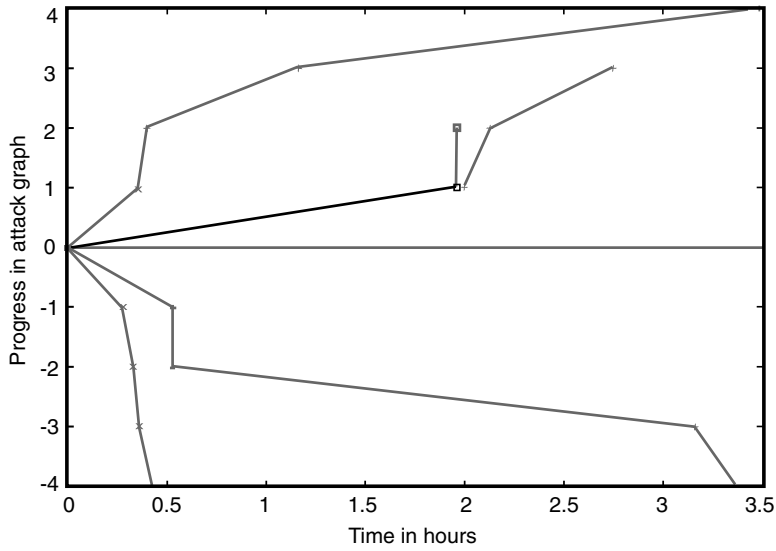


Figure 6.7 Progress of attacks over time—week 1.

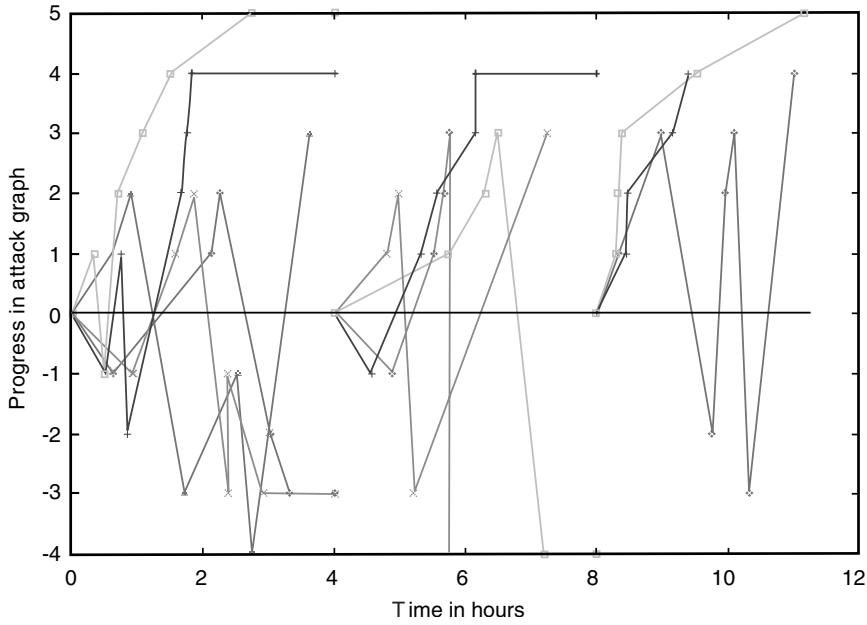


Figure 6.8 Progress of attacks in hopes 4–6 as a single time sequence.

undergoing deception decided that they did not wish to continue their work in this area. The experimenters allowed them to resign, thinking that this was to be expected after 4 straight weeks of 4-hour sessions. But the next week, the same thing happened again with a second attack group undergoing deception. By the end of the third week of this sequence, out of 24 original attackers, 10 in two groups under no deception and 15 in three groups under deception, only 11 remained. And nine of those were under no deception. Subsequent analysis of forms filled out by the groups and behavioral analysis of the motions and actions of individuals indicated that a number of psychological factors were present. In particular, groups under deception started out enjoying the work equally with other groups, but ended up enjoying the work less, maintained less group cohesion, reduced trust in leadership, and generally ended up going slower and slower over time, despite the learning that was successful at improving progress over time for groups not under deception. This seems to be consistent with results on learning in children where inconsistent feedback reduces performance.

The HoneyNet Project

The HoneyNet Project[109] is a substantial effort aimed at placing deception system in the open environment for detection and tracking of attack techniques. As such, they have been largely effective at luring attackers. These lures are real systems placed on the Internet with the purpose of being attacked so that attack methods can be tracked and assessed. As deceptions, the only thing deceptive about them is that they are being watched more closely than would otherwise be apparent and known faults are intentionally not being fixed to allow attacks to proceed. These are highly effective at allowing attackers to enter because they are extremely high fidelity, but only for the purpose they are intended to provide. They do not, for example, include any user behaviors or content of interest. They are quite effective at creating sites that can be exploited for attack of other sites. For all of the potential benefit, however, the HoneyNet project has not performed any controlled experiments to understand the issues of deception effectiveness. In addition, over time the attackers appear to have learned about honey pots and now many of them steer clear of these systems by using indicators of honey pot computers as differentiators for their attacks. For example, they look for user presence in the computers and processes reminiscent of normal user behavior. These deceptions have not apparently been adapted quickly enough to ward off these attackers by simulating a user population.

Red Teaming Experiments

Red teaming (i.e., finding vulnerabilities at the request of defenders)[110] has been performed by many groups for quite some time. The advantage of red

teaming is that it provides a relatively realistic example of an attempted attack. The disadvantage is that it tends to be somewhat artificial and reflective of only a single run at the problem. Real systems get attacked over time by a wide range of attackers with different skill sets and approaches. While many red teaming exercises have been performed, these tend not to provide the scientific data desired in the area of defensive deceptions because they have not historically been oriented toward this sort of defense.

Several red teaming experiments against simplistic defenses were performed under a Defense Advanced Research Project Agency (DARPA) research grant in 2000 and these showed that sophisticated red teams were able to rapidly detect and defeat simplistic deceptions. These experiments were performed in a proximity-only case and used static deceptions of the same sort as provided by DTK. As a result this was a best-case scenario for the attackers. Unfortunately, the experimental technique and data from these experiments were poor and inadequate funding and attention was paid to detail. Defenders apparently failed to even provide false traffic for these conditions, a necessity in creating effective deceptions against proximate attackers, and a technique that was used in the Sandia experiments when proximate or enveloped attackers were in use. Only distant attacker models can possibly be effective under these conditions. Nevertheless, these results should be viewed as a cautionary note to the use of low-quality deceptions against high-quality attackers and should lead to further research into the range of effectiveness of different methods for different situations.

RAND Experiments

War games played out by armed services tend to ignore issues of information system attacks because the exercises are quite expensive and by successfully attacking information systems that comprise command and control capabilities, many of the other purposes of these war games are defeated. While many recognize that the need to realistically portray effects is important, we could say the same thing about nuclear weapons, but that does not justify dropping them on our forces for the practice value.

The most definitive experiments to date that we were able to find on the effectiveness of low-quality computer deceptions against high-quality, computer-assisted human attackers were performed by RAND.[111] Their experiments with fairly generic deceptions operated against high-quality intelligence agency attackers demonstrated substantial effectiveness for short periods of time. This implies that under certain conditions (i.e., short time frames, high tension, no predisposition to consider deceptions, etc.) these deceptions may be effective.

Experiments We Believe Are Needed at This Time

The total number of controlled experimental runs to date involving deception in computer networks appear to be less than 50, and the number involving the use of deceptions for defense are limited to the 10 or so from the RAND study and 35 from the Sandia studies. Furthermore, the RAND studies did not use control groups or other methods to differentiate the effectiveness of deceptions. Clearly, there is not experimental data enough to gain much in the way of knowledge and, just as clearly, many more experiments are required in order to gain a sound understanding of the issues underlying deception for defense.

The clear solution to this dilemma is the creation of a set of experiments in which we use social science methodologies to create, run, and evaluate a substantial set of parameters that provide us with better understanding and specific metrics and accuracy results in this area. In order for this to be effective, we must not only create defenses, but also come to understand how attackers work and think. For this reason, we will need to create red teaming experiments in which we study both the attackers and the effects of defenses on the attackers. In addition, in order to isolate the effects of deception, we need to create control groups, and experiments with double-blinded data collection. While the Sandia studies did this and their results are interesting, they are not adequate to draw strong or statistically valid conclusions, particularly in light of the results from subsequent DARPA studies without these controls.

Analysis and Design of Deceptions

A good model should be able to explain, but a good scientific model should be able to predict and a good model for our purposes should help us design as well. At a minimum, the ability to predict leads to the ability to design by random variation and selective survival with the survival evaluation being made based on prediction. In most cases, it is a lot more efficient to have the ability to create design rules that are reflective of some underlying structure.

Any model we build that is to have utility must be computationally reasonable relative to the task at hand. Far more computation is likely to be available for a large-scale strategic deception than for a momentary tactical deception, so it would be nice to have a model that scales well in this sense. Computational power is increasing with time, but not at such a rate that we will ever be able to completely ignore computational complexity in problems such as this.

A fundamental design problem in deception lies in the fact that deceptions are generally thought of in terms of presenting a desired story to the target, while the available techniques are based on what has been found to work. In other words, there is a mismatch between available deception techniques and technologies and objectives.

A Language for Analysis and Design of Deceptions

Rather than focus on what we wish to do, our approach is to focus on what we can do and build up "deception programs" from there. In essence, our framework starts with a programming language for human deception by finding a set of existing primitives and creating a syntax and semantics for applying these primitives to targets. We can then associate metrics with the elements of the programming language and analyze or create deceptions that optimize against those metrics.

The framework for human deception then has three parts:

1. *A set of primitive techniques:* The set of primitive techniques is extensive and is described hierarchically based on the model shown above, with each technique associated with one or more of observables, actions, assessments, capabilities, expectations, and intent and causing an effect on the situation depicted by the model.
2. *Properties of those techniques:* Properties of techniques are multidimensional and include all of the properties discussed in this report. This includes, but is not limited to, resources consumed, effect on focus of attention, concealment, simulation, memory requirements and impacts, novelty to target, certainty of effect, extent of effect, timeliness of effect, duration of effect, security requirements, target system resource limits, deceiver system resource limits, the effects of small changes, organizational structure, knowledge, and constraints, target knowledge requirements, dependency on predisposition, extent of change in target mind set, feedback potential and availability, legality, unintended consequences, the limits of modeling, counter deception, recursive properties, and the story to be told. These are the same properties of deception discussed under The Nature of Deception earlier in the chapter.
3. *A syntax and semantics for applying and optimizing the properties:* This is a language that has not yet been developed for describing, designing, and analyzing deceptions. It is hoped that this language and the underlying database and simulation mechanism will be developed in subsequent efforts.

The astute reader will recognize this as the basis for a computer language, but it has some differences from most other languages, most fundamentally in that it is probabilistic in nature. While most programming languages guarantee that when you combine two operators together in a sequence you get the effect of the first followed by the effect of the second, in the language of deception, a sequence of operators produces a set of probabilistic changes in perceptions of all parties across the multidimensional space of the properties of deception. It will likely be effective to "program" in terms of desired changes in deception properties and allow the computer to "compile" those

desired changes into possible sequences of operators. The programming begins with a "firing table" of some sort that looks something like the following table, but with many more columns filled in and many more details under each of the rows. Partial entries are provided for technique 1 which, for this example, we will choose as "audit suppression" by packet flooding of audit mechanisms using a distributed set of previously targeted intermediaries.

Deception Property	Technique 1	...	Technique n
Name	Audit suppression		
General concept	Packet flooding of audit mechanisms		
Means	Using a distributed set of intermediaries		
Target type	Computer		
Resources consumed	Reveals intermediaries, which will be disabled with time		
Effect on focus of attention	Induces focus on this attack		
Concealment	Conceals other actions from target audit and analysis		
Simulation	Not applicable		
Memory requirements and impacts	Overruns target memory capacity		
Novelty to target	None — they have seen similar things before		
Certainty of effect	80% effective if Intel is right		
Extent of effect	Reduces audits by 90% if effective		
Timeliness of effect	Takes 30 seconds to start		
Duration of effect	Until ended or intermediaries are disabled		
Security requirements	Must conceal launch points and intermediaries		
Target system resource limits	Memory capacity, disk storage, CPU time		
Deceiver system resource limits	Number of intermediaries for attack, prepositioned assets lost with attack		
Effects of small changes	Nonlinear effect on target with break point at effectiveness threshold		
Organizational structure and constraints	Going after known main audit server, which will impact whole organization audits		
Target knowledge	OS type and release		
Dependency on predisposition	Must be proper OS type and release to work		
Extent of change in target mind set	Large change — it will interrupt them — they will know they are being attacked		
Feedback potential and availability	Feedback apparent in response behavior observed against intermediaries and in other fora		

Deception Property	Technique 1	…	Technique n
Legality	Illegal except at high intensity conflict — possible act of war		
Unintended consequences	Impacts other network elements, may interrupt other information operations, may result in increased target security		
The limits of modeling	Unable to model overall network effects		
Counter-deception	If feedback known or attack anticipated, easy to deceive attacker		
Recursive properties	Only through counter-deception		
Possible deception story	We are concealing something, they know this, but they do not know what		

Considering that the total number of techniques is likely to be on the order of several hundred and the vast majority of these techniques have not been experimentally studied, the level of effort required to build such a table and make it useful will be considerable.

Attacker Strategies and Expectations

For a moment, we will pause from the general issue of deception and examine more closely the situation of an attacker attempting to exploit a defender through information system attack. In this case, there is a commonly used attack methodology that subsumes other common methodologies and there are only three known successful attack strategies identified by simulation and verified against empirical data. We start with some background.

The pathogenesis of diseases has been used to model the process of breaking onto computers and it offers an interesting perspective.[112] In this view, the characteristics of an attack are given in terms of the survival of the attack method (Table 6.1).

This particular perspective on attack as a biological process ignores one important facet of the problem, and that is the preparation process for an intentional and directed attack. In the case of most computer viruses, targeting is not an issue. In the case of an intelligent attacker, there is generally a set of capabilities and intent behind the attack. Furthermore, survival (stability in the environment) would lead us to the conclusion that a successful attacker who does not wish to be traced back to their origin will use an intelligence process including personal risk reduction as part of their overall approach to attack. This in turn leads to an intelligence process that precedes the actual attack.

The typical attack methodology consists of:

1. Intelligence gathering, securing attack infrastructure, tool development, and other preparations
2. System entry (beyond default remote access)

Table 6.1

from "Emerging Viruses"	"Pathogenesis of Computer Viruses"	"Pathogenesis of Manual Attacks"
1. Stability in environment	1. Stability in environment	1. Stability in environment
2. Entry into host-portal of entry	2. Entry into host-portal of entry	2. Entry into host-portal of entry
3. Localization in cells near portal of entry	3. Localization in software near portal of entry	3. Localization near portal of entry
4. Primary replication	4. Primary replication	4. Primary modifications
5. Non-specific immune response	5. Non-specific immune response	5. Non-specific immune response
6. Spread from primary site (blood, nerves)	6. Spread from primary site (disk, comms)	6. Spread from primary site (privilege expansion)
7. Cells and tissue tropism	7. Program and data tropism	7. Program and data tropism (hiding)
8. Secondary replication	8. Secondary replication	8. Secondary replication
9. Antibody and cellular immune response	9. Human and program immune response	9. Human and program immune response
10. Release from host	10. Release from host	10. Release from host (spread on)

3. Privilege expansion
4. Subversion, typically involving planting capabilities and verifying over time
5. Exploitation

There are loops from higher numbers to lower numbers so that, for example, privilege expansion can lead back to intelligence and system entry or forward to subversion, and so forth. In addition, attackers have expectations throughout this process that adapt based on what has been seen before this attack and within this attack. Clean up, observation of effects, and analysis of feedback for improvement are also used throughout the attack process. The simplistic attack graph in the absence of deception (shown earlier) makes this easy to understand, whereas the more detailed complete picture with deception added (later) shows how deception (the downward direction from the starting point) interrupts the cognitive processes of the attacker and leads to ineffective attacks in the presence of deception. The complexity increases fourfold because the presence of deception leads not only to deception or not in reality, but also to deception or not in the view of the attacker. This the attacker can believe deception is present when it is not or believe it is absent when present as well as believe it is present when present and absent when absent.

Extensive simulation has been done to understand the characteristics of successful attacks and defenses.[113] Among the major results of this study were

a set of successful strategies for attacking computer systems. It is particularly interesting that these strategies are similar to classic military strategies because the simulation methods used were not designed from a strategic viewpoint, but were based solely on the mechanisms in use and the times, detection, reaction, and other characteristics associated with the mechanisms themselves. Thus, the strategic information that fell out of this study was not biased by its design, but rather emerged as a result of the metrics associated with different techniques. The successful attack strategies identified by this study included:

1. Speed
2. Stealth
3. Overwhelming force

Slow, loud attacks tend to be detected and reacted to fairly easily. A successful attacker can use combinations of these in different parts of an attack. For example, speed can be used for a network scan, stealth for system entry, speed for privilege expansion and planting of capabilities, stealth for verifying capabilities over time, and overwhelming force for exploitation. This is a typical pattern today.

Substantial red teaming and security audit experience has led to some speculations that follow the general notions of previous work on individual deception. It seems clear from experience that people who use computers in attacks:

1. Tend to trust what the computers tell them unless it is far outside normal expectations
2. Use the computer to automate manual processes and not to augment human reasoning
3. Tend to have expectations based on prior experience with their tools and targets

If this turns out to be true, it has substantial implications for both attack and defense. Experiments should be undertaken to examine these assertions as well as to study the combined deception properties of small groups of people working with computers in attacking other systems. Unfortunately, current data are not adequate to thoroughly understand these issues. There may be other strategies developed by attackers, other attack processes undertaken, and other tendencies that have more influence on the process. We will not know this until extensive experimentation is done in this area.

Defender Strategies and Expectations

From the deceptive defender's perspective, there also seem to be a limited set of strategies.

- *Computer only:* If the computer is being used for a fully automated attack, analysis of the attack tool or relatively simply automated response mechanisms are highly effective at maintaining the computer's

expectations, dazzling the computer to induce unanticipated processing and results, feeding false information to the computer, or in some cases, causing the computer to crash. We have been able to easily induce or suppress signal returns to an attacking computer and have them seen as completely credible almost no matter how ridiculous they are. Whether this will continue and to what extent it will continue in the presence of a sophisticated hostile environment remain to be seen.

- *People only:* Manual attack is very inefficient so it is rarely used except in cases where very specific targets are involved. Because humans do tend to see what they expect to see, it is relatively easy to create high fidelity deceptions by redirecting traffic to a honey pot or other such system. Indeed, this transition can even be made fairly early in an attack without most human attackers noticing it. In this case, there are three things we might want to do:
  - Maintain the attackers expectations to consume their time and effort
  - Slowly change their expectations to our advantage at a rate that is not noticeable by typical humans (e.g., slow the computer's response minute by minute till it is very slow and the attacker is wasting lots of time and resources)
  - Create cognitive dissonance to force them to think more deeply about what is going on, wonder if they have been detected, and induce confusion in the attacker.
- *People with poorly integrated computers:* This is the dominant form of efficient widespread attack today. In this form, people use automated tools combined with short bursts of human activity to carry out attacks.

The intelligence process is almost entirely done by scanning tools that (1) can be easily deceived and (2) tend to be believed. Such deceptions will only be disbelieved if inconsistencies arise between tools, in which case the tools will initially be suspected.

System entry is either automated with the intelligence capability or automated at a later time when the attacker notices that an intelligence sweep has indicated a potential vulnerability. Results of these tools will be believed unless they are incongruous with normal expectations.

Privilege expansion is either fully automated or has a slight manual component to it. It typically involves the loading of a toolkit for the job followed by compilation and/or execution. This typically involves minimal manual effort. Results of this effort are believed unless they are incongruous with normal expectations.

Planting capabilities is typically nearly automated or fully automated. Returning to verify over time is typically automated with time frames substantially larger than attack times. This will typically involve minimal manual

effort. Results of this effort will be believed unless they are incongruous with normal expectations.

Exploitation is typically done under one shot or active control. A single packet may trigger a typical exploit or, in some cases, the exploit is automatic and ongoing over an extended period of time. This depends on whether speed, stealth, or force is desired in the exploitation phase. This causes observables that can be validated by the attacker. If the observables are not present it might generate deeper investigation by the attacker. If there are plausible explanations that can be discovered by the attacker, they will likely be believed.

- *People with well-integrated computers:* This has not been observed to date. People are not typically augmenting their intelligence, but rather automating tasks with their computers.

As in the case with attacker strategies, few experiments have been undertaken to understand these issues in detail, but preliminary experiments appear to confirm these notions.

Planning Deceptions

Several authors have written simplistic analyses and provided rules of thumb for deception planning. There are also some notions about planning deceptions under the present model using the notions of low, middle, and high-level cognition to differentiate actions and create our own rules of thumb with regard to our cognitive model. But while notions are fine for contemplation, scientific understanding in this area requires an experimental basis.

According to Field Manual 90-02,[114] a five-step process is used for military deception: (1) Situation analysis determines the current and projected enemy and friendly situation, develops target analysis, and anticipates a desired situation; (2) deception objectives are formed by desired enemy action or nonaction as it relates to the desired situation and friendly force objectives; (3) desired (target) perceptions are developed as a means to generating enemy action or inaction based on what the enemy now perceives and would have to perceive in order to act or fail to act, as desired; (4) the information to be conveyed to or kept from the enemy is planned as a story or sequence, including the development and analysis of options; (5) a deception plan is created to convey the deception story to the enemy.

These steps are carried out by a combination of commander and command staff as an embedded part of military planning. Because of the nature of military operations, capabilities that are currently available and which have been used in training exercises and actual combat are selected for deceptions. This drives the need to create deception capabilities that are flexible enough

to support the commander's needs for effective use of deceptions in a combat situation. From a standpoint of information technology deceptions, this would imply that, for example, a deceptive feint or movement of forces behind smoke screens with sonic simulations of movement should be supported by simulated information operations that would normally support such action and concealed information operations that would support the action being covered by the feint.

Deception maxims are provided to enhance planner understanding of the tools available and what is likely to work:[115]

Magruder's principles, the exploitation of perceptions: It is easier to maintain an existing belief than to change it or create a new one.

Limitations of human information processing: The law of small numbers (once you see something twice it is taken as a maxim) and susceptibility to conditioning (the cumulative effect of small changes). These are also identified and described in greater detail in Gilovich.[116]

Cry-Wolf: This is a variant on susceptibility to conditioning in that, after a seeming threat appears again and again to be innocuous, it tends to be ignored and can be used to cover real threats.

Jones' Dilemma: Deception is harder when there are more information channels available to the target. On the other hand, the greater the number of "controlled channels," the better it is for the deception.

A choice among deception types: In "A-type" deception, ambiguity is introduced to reduce the certainty of decisions or increase the number of available options. In "M-type" deception, misdirection is introduced to increase the victim's certainty that what they are looking for is their desired (deceptive) item.

Axelrod's contribution, the husbanding of assets: Some deceptions are too important to reveal through their use, but there is a tendency to over protect them and thus lose them by lack of application. Some deception assets become useless once revealed through use or overuse. In cases where strategic goals are greater than tactical needs, select deceptions should be held in reserve until they can be used with greatest effect.

A sequencing rule: Sequence deceptions so that the deception story is portrayed as real for as long as possible. The clearest indicators of deception should be held until the last possible moment. Similarly, riskier elements of a deception (in terms of the potential for harm if the deception is discovered) should be done later rather than earlier so that they may be called off if the deception is found to be a failure.

The importance of feedback: A scheme to ensure accurate feedback increases the chance of success in deception.

The Monkey's Paw: Deceptions may create subtle and undesirable side effects. Planners should be sensitive to such possibilities and, where prudent, take steps to minimize these effects.

Care in the designed and planned placement of deceptive material: Great care should be used in deceptions that leak notional information to targets. Apparent windfalls are subjected to close scrutiny and often disbelieved. Genuine leaks often occur under circumstances thought improbable. Deception failures are typically associated with (1) detection by the target and (2) inadequate design or implementation. Many examples of this are given.[117] As a doctrinal matter, battlefield deception involves the integration of intelligence support, integration and synchronization, and operations security.[118]

Intelligence support: Battlefield deceptions rely heavily on timely and accurate intelligence about the enemy. To make certain that deceptions are effective, we need to know (1) how the target's decision and intelligence cycles work, (2) what type of deceptive information they are likely to accept, (3) what source they rely on to get their intelligence, (4) what they need to confirm their information, and (5) what latitude they have in changing their operations. This requires both advanced information for planning and real-time information during operations.

Integration and synchronization: Once we know the deception plan, we need to synchronize it with the true combat operations for effect. History has shown that for the greatest chance of success, we need to have plans that are (1) flexible, (2) doctrinally consistent with normal operations, (3) credible as to the current situation, and (4) simple enough to not get confused during the heat of battle. Battlefield deceptions almost always involve the commitment of real forces, assets, and personnel.

Operations Security: Operations security (OPSEC) is the defensive side of intelligence. In order for a deception to be effective, we must be able to deny access to the deceptive nature of the effort while also denying access to our real intentions. Real intentions must be concealed, manipulated, distorted, and falsified though OPSEC.

> OPSEC is not an administrative security program. OPSEC is used to influence enemy decisions by concealing specific, operationally significant information from his intelligence collection assets and decision processes. OPSEC is a concealment aspect for all deceptions, affecting both the plan and how it is executed[119]

In the DoD context, it must be assumed that any enemy is well versed in DoD doctrine. This means that anything too far from normal operations

will be suspected of being a deception even if it is not. This points to the need to vary normal operations, keep deceptions within the bounds of normal operations, and exploit enemy misconceptions about doctrine. Successful deceptions are planned from the perspective of the targets.

The DoD has defined a set of factors in deceptions that should be seriously considered in planning.[120] It is noteworthy that these rules are clearly applicable to situations with limited time frames and specific objectives and, as such, may not apply to situations in information protection where long-term protection or protections against nebulous threats are desired.

Policy: Deception is never an end in itself. It must support a mission.

Objective: A specific, realistic, clearly defined objective is an absolute necessity. All deception actions must contribute to the accomplishment of that objective.

Planning: Deception should be addressed in the commander's initial guidance to staff and the staff should be engaged in integrated deception and operations planning.

Coordination: The deception plan must be in close coordination with the operations plan.

Timing: Sufficient time must be allowed to (1) complete the deception plan in an orderly manner, (2) effect necessary coordination, (3) promulgate tasks to involved units, (4) present the deception to the enemy decision maker through their intelligence system and (5) permit the enemy decision maker to react in the desired manner, including the time required to pursue the desired course of action.

Security: Stringent security is mandatory. OPSEC is vital but must not prevent planning, coordination, and timing from working properly.

Realism: It must look realistic.

Flexibility: The ability to react rapidly to changes in the situation and to modify deceptive action is mandatory.

Intelligence: Deception must be based on the best estimates of enemy intelligence collection and decision-making processes and likely intentions and reactions.

Enemy capabilities: The enemy commander must be able to execute the desired action.

Friendly force capabilities: Capabilities of friendly forces in the deception must match enemy estimates of capabilities and the deception must be carried out without unacceptable degradation in friendly capabilities.

Forces and personnel: Real forces and personnel required to implement the deception plan must be provided. Notional forces must be realistically portrayed.

Means: Deception must be portrayed through all feasible and available means.

Supervision: Planning and execution must be continuously supervised by the deception leader. Actions must be coordinated with the objective and implemented at the proper time.

Liaison: Constant liaison must be maintained with other affected elements to assure that maximum effect is attained.

Feedback: A reliable method of feedback must exist to gage enemy reaction.

Deception of humans and automated systems involves interactions with their sensory capabilities.[121] For people, this includes (1) visual (e.g., dummies and decoys, camouflage, smoke, people and things, and false vs. real sightings); (2) olfactory (e.g., projection of odors associated with machines and people in their normal activities at that scale including toilet smells, cooking smells, oil and gas smells, and so forth); (3) sonic (e.g., directed against sounding gear and the human ear blended with real sounds from logical places and coordinated to meet the things being simulated at the right places and times); and (4) electronic (i.e., manipulative electronic deception, simulative electronic deception, and imitative electronic deception).

Resources (e.g., time, devices, personnel, equipment, and material) are always a consideration in deceptions as are the need to hide the real and portray the false. Specific techniques include feints, demonstrations, ruses, displays, simulations, disguises, and portrayals.[122]

A Different View of Deception Planning Based on the Model from This Study

A typical deception is carried out by the creation and invocation of a deception plan. Such a plan is normally based on some set of reasonably attainable goals and time frames, some understanding of target characteristics, and some set of resources which are made available for use. It is the deception planner's objective to attain the goals with the provided resources within the proper time frames. In defending information systems through deception, our objective is to deceive human attackers and defeat the purposes of the tools these humans develop to aid them in their attacks. For this reason, a framework for human deception is vital to such an undertaking.

All deception planning starts with the objective. It may work its way back toward the creation of conditions that will achieve that objective or use that objective to "prune" the search space of possible deception methods. While it is tempting for designers to come up with new deception technologies and turn them into capabilities without a clear understanding of the class of deceptions of interest, it will not be clear what capabilities would be desirable and without a clear understanding of the objectives of the specific deception,

it will not be clear how those capabilities should be used. If human deception is the objective, we can begin the planning process with a model of human cognition and its susceptibility to deception.

The skilled deception planner will start by considering the current and desired states of mind of the deception target in an attempt to create a scenario that will either change or retain the target's state of mind by using capabilities at hand. State of mind is generally only available when (1) we can read secret communications, (2) we have insider access, or (3) we are able to derive state of mind from observable outward behavior.

Understanding the limits of controllable and uncontrollable target observables and the limits of intelligence required to assure that the target is getting and properly acting (or not acting) on the information provided to them is a very hard problem.

Deception Levels

In the model depicted earlier (Figure 6.9) and characterized by Table 6.2, three levels can be differentiated for clearer understanding and grouping of available techniques. They are characterized here by mechanism, predictability, and analyzability.

Deception Guidelines

This structuring leads to general guidelines for effective human deception. In essence, they indicate the situations in which different levels of deception should be used and rules of thumb for their use.

Low level	Higher certainty can be achieved at lower levels of perception
	Deception should be carried out at as low a level as feasible
	If items are to be hidden and can be made invisible to the target's sensors, this is preferred
	If a perfect simulation of a desired false situation can be created for the enemy sensors, this is preferred
	Do not invoke unnecessary midlevel responses and pattern matching
	Try to avoid patterns that will create dissonance or uncertainty that would lead to deeper inspection
Mid level	If a low-level deception will not work, a midlevel deception must be used
	Time pressure and high stress combine to keep targets at midlevel cognitive activities
	Activities within normal situational expectations tend to be handled by midlevel decision processes
	Training tends to generate midlevel decision processes
	Mid level deceptions require feedback for increased assurance
	Remain within the envelope of high-level expectations to avoid high-level analysis
	Exceed the envelope of high-level expectations to trigger high-level analysis

High level	If the target cannot be forced to make a midlevel decision in your favor, a high-level deception must be used
	It is easiest to reinforce existing predispositions
	To alter predisposition, high-level deception is required
	Movement from predisposition to new disposition should be made at a pace that does not create dissonance
	If target confusion is desired, information should be changed at a pace that creates dissonance
	In high-level deceptions, target expectations must be considered at all times
	High-level deceptions require the most feedback to measure effect and adapt to changing situations

Just as Sun Tzu created guidelines for deception, there are many modern pieces of advice that probably work pretty well in many situations. And like Sun Tzu, these are based on experience in the form of anecdotal data. As someone once said: *The plural of anecdote is statistics.*

Deception Algorithms

As more and more of these sorts of rules of thumb based on experience are combined with empirical data from experiments, it is within the realm of plausibility to create more explicit algorithms for decision planning and evaluation. Here is an example of the codification of one such algorithm. It deals with the issue of sequencing of deceptions with different associated risks identified earlier.

Let us assume you have two deceptions, A (low risk) and B (high risk). Then, if the situation is such that the success of either means the mission is accomplished, the success of both simply raises the quality of the success (e.g. it costs less), and the discovery of either by the target will increase the risk that the other will also fail, then you should do A first to assure success. If A succeeds you then do B to improve the already successful result. If A fails, you either do something else or do B out of desperation. On the other hand, if the situation is such that the success of both A and B are required to accomplish the mission and if the discovery of either by the target early in execution will result in substantially less harm than discovery later in execution, then you should do B first so that losses are reduced if, as is more likely, B is detected. If B succeeds, you then do A. Here this is codified into a form more amenable to computer analysis and automation:

GIVEN: Deception A (low risk) and Deception B (high risk).
IF [A Succeeds] OR [B Succeeds] IMPLIES [Mission Accomplished, Good Quality/Sched/Cost]
AND [A Succeeds] AND [B Succeeds] IMPLIES [Mission Accomplished, Best Quality/Sched/Cost]

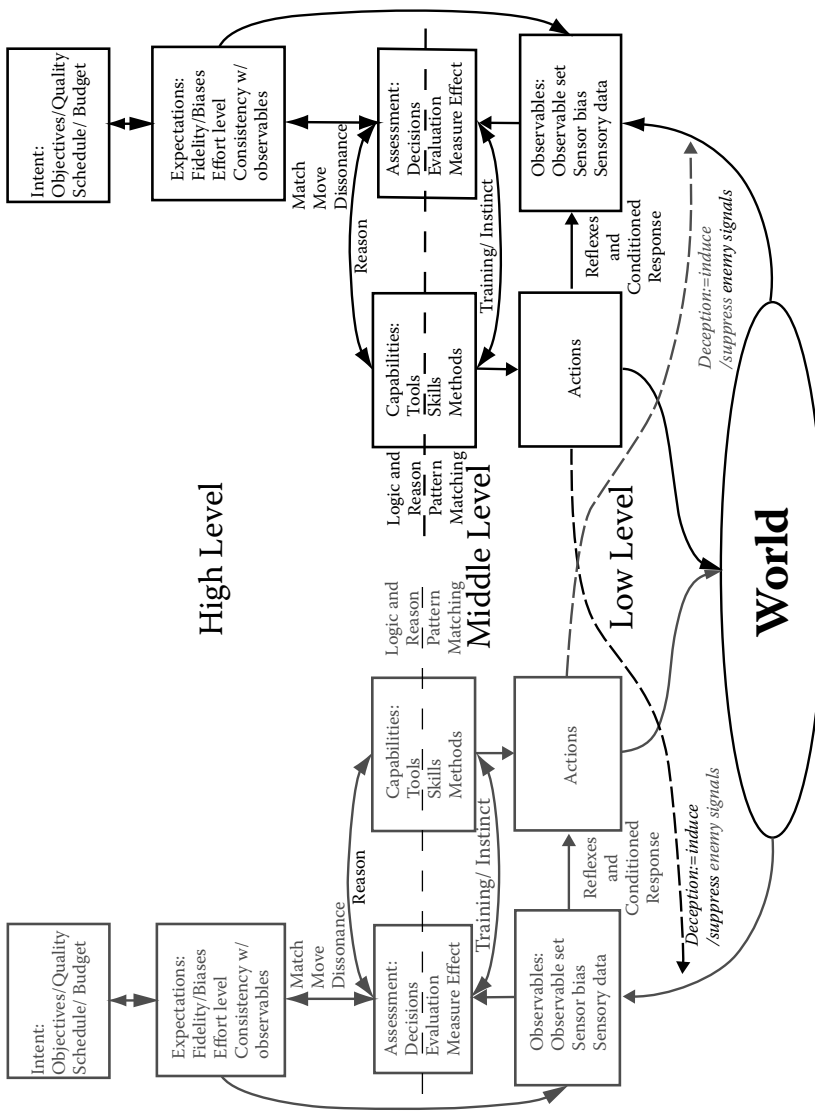


Figure 6.9 A human/ human organization model of deception.

Table 6.2 Human Deception Levels

Level	Mechanism	Predictability	Analysis	Summary
Low level	Low-level deceptions operate at the lower portions of the areas labeled observables and actions. They are designed to cause the target of the deception to be physically unable to observe signals or to cause the target to selectively observe signals.	Low-level deceptions are highly predictable based on human physiology and known reflexes.	Low-level deceptions can be analyzed and very clearly characterized through experiments that yield numerical results in terms of parameters, such as detection thresholds, response times, recovery times, edge detection thresholds, and so forth.	Except in cases where the target has sustained physiological damage, these deceptions operate very reliably and predictably. The time frames for these deceptions tend to be in the range of milliseconds to seconds and they can be repeated reliably for ongoing effect.
Mid-level	Mid-level deceptions operate in the upper part of the areas labeled observables and actions and in the lower part of the areas marked assessment and capabilities. They are generally designed to either (1) cause the target to invoke trained or pattern matching based responses and avoid deep thought that might induce unfavorable (to us) actions, or (2) induce the target to use high-level cognitive functions, thus avoiding faster pattern matching responses.	Mid-level deceptions are usually predictable, but are affected by a number of factors that are rather complex, including but not limited to socialization processes and characteristics of the society in which the person was brought up and lives.	Analysis is based on a substantial body of literature. Experiments required for acquiring this knowledge are complex and of limited reliability. There are a relatively small number of highly predictable behaviors. These relatively small numbers of behaviors are common and are invoked under predictable circumstances.	Many mid-level deceptions can be induced with reasonable certainty through known mechanisms and will produce predictable results if applied with proper cautions, skills, and feedback. Some require social background information on the subject for high surety of results. The time frame for these deceptions tends to be seconds to hours with lasting residual effects that can last for days to weeks.

(*continued*)

Table 6.2 Human Deception Levels (Continued)

Level	Mechanism	Predictability	Analysis	Summary
High level	High-level deceptions operate from the upper half of the areas labeled assessment and capabilities to the top of the chart. They are designed to cause the subject to make a series of reasoned decisions by creating sequences of circumstances that move the individual to a desired mental state.	High-level deceptions are reasonably controlled if adequate feedback is provided, but they are far less certain to work than lower-level deceptions. The creation and alteration of expectations has been studied in detail and it is clearly a high skills activity where greater skill tends to prevail.	High-level deception requires a high level of feedback when used against a skilled adversary and less feedback under mismatch conditions. There is a substantial body of supporting literature in this area, but it is not adequate to lead to purely analytical methods for judging deceptions.	High-level deception is a high skills game. A skilled and properly equipped team has a reasonable chance of carrying out such deceptions if adequate resources are applied and adequate feedback is available. These sorts of deceptions tend to operate over a time frame of hours to years and in some cases have unlimited residual effect.

AND [A Discovered] OR [B Discovered] IMPLIES [A (higher risk) AND B (higher risk)]
THEN DO B [comment: Do high-risk B first to insure minimal loss in case of detection]
IF [B Succeeds] DO A (Late) [comment: Do low-risk A second to improve outcome]
ELSE DO Out #1 [comment: Do higher-risk A because you're desperate.]
OR ELSE DO Out #n [comment: Do something else instead.]
IF [A Succeeds] OR [B Succeeds] IMPLIES [Mission Accomplished, Good Quality/Sched/Cost]
AND [A Detected] OR [B Detected] IMPLIES [Mission Fails]
AND [A Discovered Early] OR [B Discovered Early] IMPLIES [Mission Fails somewhat]
AND [A Discovered Late] OR [B Discovered Late] IMPLIES [Mission Fails severely]
THEN DO B [comment: Do high-risk B first to test and advance situation]
IF [B Early Succeeds] DO A (Late) [comment: Do low-risk A second for max chance of success]
IF [A Late Succeeds (likely)] THEN MISSION SUCCEEDS.
ELSE [A Late Fails (unlikely)] THEN MISSION FAILS/in real trouble.
ELSE [B Early Fails] [Early Failure]
DO Out #1 [comment: Do successful retreat as preplanned.]
OR DO Out #m [comment: Do another preplanned contingency instead.]

We clearly have a long way to go in codifying all of the aspects of deception and deception sequencing in such a form, but just as clearly, there is a path to the development of rules and rule-based analysis and generation methods for building deceptions that have effect and reduce or minimize risk or perhaps optimize against a wide range of parameters in many situations. The next reasonable step down this line would be the creation of a set of analytical rules that could be codified and experimental support for establishing the metrics associated with these rules. A game theoretical approach might be one of the ways to go about analyzing these types of systems.

Summary, Conclusions, and Further Work

This chapter has summarized a great deal of information on the history of deception in general and the historical, current, and emerging use of deception for information protection in specific. While there is a great deal to know about how deception has been used in the past, it seems quite clear that there will be far more to know about deception in the future. The information protection field has an increasingly pressing need for innovations that change

the balance between attack and defense. It is clear from what we already know that deception techniques have the demonstrated ability to increase attacker workload and reduce attacker effectiveness while decreasing defender effort required for detection and providing substantial increases in defender understanding of attacker capabilities and intent.

Modern defensive computer deceptions are in their infancy, but they are moderately effective, even in this simplistic state. The necessary breakthrough that will turn these basic deception techniques and technologies into viable long-term defenses is the linkage of social sciences research with technical development. In specifics, we need to measure the effects and known characteristics of deceptions on the systems comprising of people and their information technology to create, understand, and exploit the psychological and physiological bases for the effectiveness of deceptions. The empirical basis for effective deception in other arenas is simply not available in the information protection arena today and in order to attain it, there is a crying need for extensive experimentation in this arena.

To a large extent this work has been facilitated by the extensive literature on human and animal deception that has been generated over a long period of time. In recent years, the experimental evidence has accumulated to the point where there is a certain degree of general agreement in the part of the scientific community that studies deception about many of the underlying mechanisms, the character of deception, the issues in deception detection, and the facets that require further research. These same results and experimental techniques need to be applied to deception for information protection if we are to become designers of effective and reliable deceptions.

The most critical work that must be done in order to make progress is the systematic study of the effectiveness of deception techniques against combined systems with people and computers. This goes hand in hand with experiments on how to counter deceptions and the theoretical and practical limits of deceptions and deception technologies. In addition, codification of prior rules of engagement, the creation of simulation systems and expert systems for analysis of deceptions sequences, and a wide range of related work would clearly be beneficial as a means to apply the results of experiments once empirical results are available.

Acknowledgment

Many have contributed to this work and they are referenced in the cited papers herein. Special thanks go to Charles Preston, Eric Thomas, Deanna Koike, Irwin and Jeanne Marin, Fred Feer, Garrett Gee, Anthony Carathimas, and Dave Lambert for their outstanding efforts to help produce many of the results as part of my work in this area.

References

1. This chapter is largely based on a series of other papers published at http://all.net/ under the "*Deception for Protection*" section and portions of this and related papers have appeared in a number of journal articles, conference papers, and elsewhere. The reader is also referred to "*Frauds, Spies, and Lies and How to Defeat Them*" (ASP Press, 2005) and "*World War 3: We are losing it and most of us didn't even know we were fighting in it—Information Warfare Basics*" (ASP Press, 2006) for further details on many of these subjects.
2. Tzu, S., *The Art of War* (Translated by James Clavell), Dell Publishing, New York, 1983.
3. Kahn, D., *The Code Breakers*, MacMillan Press, New York, 1967.
4. Huber, R.E., Information Warfare: Opportunity Born of Necessity, News Briefs, September– October 1983, Vol. IX, Num. 5, Systems Technology (Sperry Univac), pp. 14–21.
5. Tzu, S., *The Art of War.*
6. Keaton, T., *A History of Warfare*, Vintage Books, New York, 1993.
7. Mitchell, R.W. and Thompson, N.S., *DECEPTION: Perspectives on human and nonhuman deceit*, SUNH Press, New York, 1986.
8. Wilson, A., *The Bomb and the Computer*, Delacorte Press, New York, 1968.
9. Field Manual 90–02, *Battlefield Deception*, U.S. Department of Defense, 1998.
10. Whaley, B., *Stratagem: Deception and Surprise in War*, MIT Center for International Studies, Cambridge, 1969.
11. Dunnigan, J.F. and Nofi, A.A., *Victory and Deceit: Dirty Tricks at War*, William Morrow and Co., New York, 1995.
12. Dewar, M., *The Art of Deception in Warfare*, David and Charles Military Books, 1989.
13. Knowledge Systems Corporation, C3CM Planning Analyzer: Functional Description (Draft) First Update, RADC/COAD Contract F30602-87-C-0103, Dec. 12, 1987.
14. Griego, W.L., Deception—A 'Systematic Analytic' Approach, slides from 1978, 1983.
15. Stein, G., *Encyclopedia of Hoaxes*, Gale Research, Inc., 1993, p. 293.
16. Dewar, M., *Art of Deception in War.*
17. Whitlock, C., *Scam School*, MacMillan, 1997.
18. Faron, F., *Rip-Off: a writer's guide to crimes of deception*, Writers Digest Books, Cincinnati, OH, 1998.
19. Fellow, S., *Easily Fooled, Mind Matters*, Minneapolis, 2000.
20. Ibid., p. 14.
21. Gilovich, T., *How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life*, Free Press, New York, 1991.

22. West, C.K, *The Social and Psychological Distortion of Information*, Nelson-Hall, Chicago, 1981.
23. Seckel, A., *The Art of Optical Illusions*, Carlton Books, U.K. 2000.
24. Hoffman, D.D., Visual Intelligence: How We Create What We See, Norton, New York, 1998.
25. Deutsch, D., *Musical Illusions and Paradoxes*, Philomel, La Jolla, CA, 1995.
26. Karrass, C.R., *The Negotiating Game*, Thomas A. Crowell, New York, 1970.
27. Cialdini, R.B., *Influence: Science and Practice*, Allyn and Bacon, Boston, 2001.
28. Ibid.
29. Robertson, R.J. and Powers, W.T., Eds., Introduction to Modern Psychology, The Control-Theory View. The Control Systems Group, Inc., Gravel Switch, KY 1990.
30. Lambert, D., A Cognitive Model for Exposition of Human Deception and Counter-Deception, NOSC Technical Report 1076, Oct. 1987.
31. Handy, C., Understanding Organizations, Oxford University Press, New York, 1993.
32. National Research Council, Modeling Human and Organizational Behavior, National Academy Press, Washington, D.C., 1998.
33. Greene, R., *The 48 Laws of Power*, Penguin Books, New York, 1998.
34. Various documents: A list of documents related to MKULTRA can be found on the Internet.
35. Heuer, R.J., Jr., Psychology of Intelligence Analysis, History Staff Center for the Study of Intelligence, Central Intelligence Agency, 1999.
36. Vrij, A., *Detecting Lies and Deceit*, John Wiley & Sons, New York, 2000.
37. Cheswick, B., An Evening with Berferd, 1991.
38. Cohen, F., Operating System Protection Through Program Evolution Computers and Security, 1992.
39. Cohen, F., Internet holes — Internet lightning rods, *Net. Sec. Mag.*, July 1996.
40. Cohen, F., A note on distributed coordinated attacks, *Comp. Sec.*, 1996.
41. Cohen, F., A note on the role of deception in information protection, *Comp. Sec.*, 1999.
42. Cohen, F., The unpredictability defense, *Manag. Net. Sec.*, Apr. 1998.
43. Cohen, F., Method and Apparatus for Network Deception/Emulation, International Patent Application No PCT/US00/31295, Filed October 26, 2000.
44. Cohen, F., A Mathematical Structure of Simple Defensive Network Deceptions, 1999. http://all.net (InfoSec Baseline Studies).
45. Gerwehr, S., Rothenberg, J., and Anderson, R.H., An Arsenal of Deceptions for INFOSEC (OUO), PM-1167-NSA, Oct. 1999, RAND National Defense Research Institute Project Memorandum, Santa Monica, CA.
46. Gilovich, T., *How We Know What Isn't So.*
47. Field Manual 90-02, *Battlefield Deception*, U.S. Department of Defense, 1998.

48. Gerwehr, S., Weissler, R., Medby, J.J., Anderson, R.H., and Rothenberg, J., Employing Deception in Information Systems to Thwart Adversary Reconnaissance-Phase Activities (OUO), PM-1124-NSA, Nov. 2000, RAND National Defense Research Institute, Santa Monica, CA.
49. Cohen, F., A Mathematical Structure of Simple Defensive Network Deceptions, 1999.
50. Cohen, F., Method and Apparatus for Network Deception/Emulation, 2000.
51. Cohen, F., A note on the role of deception in information protection, 1999.
52. Fellows, B., *Easily Fooled, Mind Matters*.
53. Dewar, M., *Art of Deception in War*.
54. Cohen, F., Deception ToolKit, Mar. 1998.
55. Weiner, N., Cybernetics, 1954.
56. Cialdini, R.B., *Influence*.
57. Whitlock, C., *Scam School*.
58. Faron, F., *Rip-off*.
59. Kahn, D., *The Code Breakers*.
60. Field Manual 90-02, *Battlefield Deception*, U.S. Department of Defense, 1998.
61. Cohen, F., Simulating Cyber Attacks, Defenses, and Consequences, IFIP TC-11, Computers and Security, 1999.
62. Ibid.
63. Ibid.
64. Cohen, F., A Note on the Role of Deception in Information Protection, 2000.
65. Cohen, F., A Mathematical Structure of Simple Defensive Network Deceptions, 1999.
66. Vrij, A., *Detecting Lies and Deceit*.
67. Kalbfleisch, P.J., The language of detecting deceit. *J. Lang. Soc. Psychol.*, 13 (4), 469, 28p, 1 chart. (Provides information on the study of language strategies that are used to detect deceptive communication in interpersonal interactions. Classification of the typology; strategies and implementation tactics; discussions on deception detection techniques; conclusion.)
68. Karrass, C.R., *The Negotiating Game*.
69. Vrij, A., *Detecting Lies and Deceit*.
70. Lambert, D., *A Cognitive Model*.
71. Robertson, R.J. and Powers, W.T.
72. Seckel, A., *The Art of Optical Illusions*.
73. Hoffman, D.D., *Visual Intelligence*.
74. Deutsch, D., *Musical Illusions and Paradoxes*.
75. Cialdini, R.B., *Influence*.
76. Karrass, C.R., *The Negotiating Game*.

77. Gilovich, T., *How We Know What Isn't So.*
78. Karrass, C.R., *The Negotiating Game.*
79. Handy, C., *Understanding Organizations.*
80. Cialdini, R.B., *Influence.*
81. Cohen, F., The Structure of Intrusion and Intrusion Detection.
82. Cohen, F., A Note on the Role of Deception in Information Protection, 2000.
83. Cohen, F., A Mathematical Structure of Simple Defensive Network Deceptions, 1999.
84. National Technical Baseline, Intrusion Detection and Response, Lawrence Livermore National Laboratory, Livermore, CA, Sandia National Laboratories, Albuquerque, NM, Dec. 1996.
85. Cohen, F., A Mathematical Structure of Simple Defensive Network Deceptions, 1999.
86. Cohen, F., A Note on the Role of Deception in Information Protection, 2000.
87. Cohen, F., Phillips, C., Swiler, L.P., Gaylor, T., Leary, P., Rupley, F., Isler, R., and Dart, E., A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model, The Encyclopedia of Computer Science and Technology, 1999.
88. Karrass, C.R., *The Negotiating Game.*
89. Wilson, J.H., *Military Intelligence Blunders*, Carol & Graf, New York, 1999.
90. Keegan, J., *A History of Warfare*, Vintage Books, New York, 1993.
91. Dunnigan, J.F. and Nofi, A.A., *Victory and Decit.*
92. Tzu, S., *The Art of War.*
93. Danial, D. and Herbig, K., Eds., *Strategic Military Deception*, Pergamon Books, Elmsford, NY, 1982.
94. Ibid., p. 42.
95. Mackay, C., *Extraordinary Popular Delusions and the Madness of Crowds*, Templeton Publications, Cooperstown, NY, 1989 (originally Richard Bently Publishers, London, 1841).
96. Handy, C., *Understanding Organizations.*
97. Ibid.
98. National Research Council, Modeling Human and Organizational Behavior.
99. Western Systems Coordinating Council (WSCC) Preliminary System Disturbance Report Aug. 10, 1996, DRAFT (This report details the August 10, 1996 major system disturbance that separated the WSCC system into four islands, interrupting service to 7.5 million customers for periods ranging from several minutes to nearly 6 hours.)
100. Pekarske , B., Restoration in a Flash — Using DS3 Cross-Connects, Telephony. Sept. 10, 1990. (This paper describes the techniques used to compensate for

network failures in certain telephone switching systems in a matter of a millisecond. The paper points out that without this rapid response, the failed node would cause other nodes to fail, causing a domino effect on the entire national communications networks.)

101. Ibid.
102. Vanderheiden, H., Gender swapping on the Net?, Boston University, http://web.aq.org/tigris/loci-virtualtherapy.html
103. Ito, M., Cybernetic Fantasies: Extended Selfhood in a Virtual Community, 1994. URL: http://lucien.berkeley.edu/MOO/Mlto-1.ps.
104. Peace, M., Ph.D. Dissertation: A Chatroom Ethnography, May 2000.
105. Chandler, D., Personal Home Pages and the Construction of Identities on the Web, 2001.
106. SSCD Tactical Decision Making Under Stress, SPAWAR Systems Center, San Diego, CA.
107. Cohen, F., A Note on the Role of Deception in Information Protection, 2000.
108. Cohen, F., A Mathematical Structure of Simple Defensive Network Deceptions, 1999.
109. The HoneyNet Project website (www.honeynet.org).
110. Cohen, F., Red teaming and other aggressive auditing techniques, *Manag. Net. Sec.*, Mar. 1998.
111. Gerwehr, S., Weissler, R., Medby, J.J., Anderson, R.H., and Rothenberg, J., Employing Deceptions.
112. Cohen, F., Red Teaming and Other Aggressive Auditing Techniques.
113. Cohen, F., Simulating Cyber Attacks, Defenses, and Consequences.
114. Field Manual 90-02., *Battlefield Deception*, U.S. Department of Defense, 1998.
115. Ibid.
116. Gilovich, T., *How We Know What Isn't So.*
117. Field Manual 90-02, *Battlefield Deception*, U.S. Department of Defense, 1998.
118. Ibid.
119. Ibid.
120. Ibid.
121. Ibid.
122. Ibid.

7 Critical Infrastructure Protection: Issues and Answers

FRED COHEN

Contents

Introduction

According to http://dictionary.reference.com/search?q=infrastructure, infrastructure is defined as:

1. An underlying base or foundation, especially for an organization or system.
2. The basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, and prisons.

Infrastructures and Consequences

Infrastructures are all the things we depend on for the things we do. Infrastructures are critical when their use in specific time frames is necessary in order for some critical function to take place. For example, a road is a critical infrastructure if it is the only path for an ambulance to bring someone to a hospital. If it is blocked and there is no alternative path, the person at risk may die. Because of the consequences of failures of critical infrastructures, it becomes critical to protect them and more critical when more consequences depend on them.

Threats

Threats are actors, including individuals, groups, and nature that have capabilities and intents. Threats to critical infrastructures are threats that have capabilities and intents that lead them to cause critical infrastructures to fail. These failures may be direct or indirect, intentional or accidental, and critical or noncritical. Critical infrastructure protection is concerned with protection against threats causing failures, regardless of whether they are accidental, intentional, direct, or indirect.

Attacks and Defenses

Attacks are often described as sequences of actions taken by threats. There are many methods within the capabilities of threats, and these capabilities may be exercised in combinations and sequences in order for threats to achieve their objectives. Threats can join forces for joint operations as well. Most threats plan and train with the notion that defenders will try to defeat their attempts, thus plans tend to be flexible and have many possible sequences. Defenders can act to reduce threats, sever the link between threats and vulnerabilities they seek to attack, reduce vulnerabilities, reduce the link between vulnerabilities and consequences, or mitigate consequences. The resulting structure

can be thought of as a multiparty conflict. This is typically called a game for the purposes of theoretical analysis and is often modeled in military simulations, also called war games.

Some Analysis

Because criticality is a function of time, location, and other factors, perfect protection can never be attained, there are many options for protection, and resources are always finite. Prioritization is necessary in order to allocate resources efficiently and to decide on protective measures in critical infrastructure protection. For example, when the president is in a city, the routes used become more critical to protection of the political system than they are normally. Advance teams come to prepare for such visits, and their preparations create sets of defenses designed to mitigate threats and consequences over only those periods of time that are critical. But other infrastructure elements, like the power systems, must be continuously protected because they are continuously critical.

As the risk and risk management situation is analyzed further, a common conclusion seems to emerge; better intelligence on the threats would make the problem a lot easier. Of course, this is a common trap that people fall into. Better intelligence is indeed an advantage, but intelligence involves a lot of complex issues: personal rights, technological limitations, language and cultural differences, differentiating relevant from irrelevant material, the difficulties of human intelligence, and countering enemy deception and counterintelligence efforts. While we can expect a lot from good intelligence, we cannot expect to be successful if we depend too heavily on it for our decisions, for several reasons. Perhaps, the best reason is that intelligence reflects information that is, at best, true today. Defenses sometimes take considerable time to construct and implement. Tomorrow the threats may change their approach and the defensive reaction may take too long for intelligence-based adaptation to be effective. Defenses are also often detectable by threats. Unless the defender uses very effective counterintelligence techniques including deceptions, the threats will be able to gain intelligence on defenses just as defenders try to gain intelligence on threats. Indeed, this may lead to the ability of the attacker to use the defender's intelligence service against the defender through feeding of false information. Since threats tend to use deception far more than defenders, there is an asymmetry that favors the attacker. Threats may cause defenders to "cry wolf," thus creating added costs and reduced credibility, if the intelligence capability is too active. All of this is expensive and imperfect and depends on an analytical capability that does not exist except in human beings, and even this capability is inherently limited by well-known factors that limit human cognition.

Another approach is to identify all of the targets for attack, but, of course, the nature of infrastructure is that it is ubiquitous and tends to cover vast distances. There are millions of miles of power lines and water lines, hundreds of thousands of gas stations, chemical-carrying trucks, and similar targets, thousands of chemical plants, power plants, government buildings, and similar targets of all sorts. A threat near any of them can easily cause select elements to fail catastrophically. Threats can attack anywhere, but defenders cannot reasonably defend everywhere. Even if threat capabilities are limited, they can still have substantial effect, but if defenses are not prepared for all of the skill sets of all the threats, the defenses will be defeatable by a threat that happens to have a mismatch, that is, the attackers have the advantage. Targets must be prioritized, typically in terms of consequences, and many will necessarily be left unprotected by preventive measures. In these cases, detection and response are the approaches of necessity, and time factors will determine distances of response teams from targets.

Vulnerabilities can be sought and closed, but again, the number of links is enormous and the number of possible specific vulnerabilities to different sorts of capabilities is too large to even enumerate. Defenses can be overwhelmed, combinations and sequences can be used for increased effect, reflexive controls can be used against response regimes, and asymmetric advantage is always sought.

Is This an Unsolvable Problem?

The situation may indeed look grim from this perspective, but a reasonable person would be forced by sheer force of reason to ask why it is that every element of infrastructure is not under constant attack and how we can possibly be doing as well as we are doing. The answer is pretty simple. The vast majority of people in the world are not trying to destroy the infrastructure. The actual threats that have adequate capabilities and intents to do serious harm are fairly limited. There may be millions of people who, given the chance, would push a button and disable the U.S. from any influence over their life situation. But these millions of people are not all ready to risk their lives and spend time and effort to do so. Perhaps, tens of thousands of people and several military organizations are of a serious enough bent that they would actually take actions to do such damage, but of those, only a few thousand probably have current access to the U.S. And of those, fewer still have insider knowledge, adequate skills, and workable plans. Of those, at any given moment, only a few are ready to act, fewer are positioned to act, and, of course, these relatively few people are fighting against many people who are defending these systems. Of course, there are many attempts to do harm, most of which are defeated. Most people only hear about those that succeed in a spectacular way and a small portion of those that fail.

While the critical infrastructure problem may seem to be unsolvable on its own and made greatly more difficult in an open, multicultural, multiracial society, the reality is not as grim as all that. While a perfect defense has never been feasible, a combination of efforts across the full spectrum of protective actions can be largely effective. Threats can be greatly reduced by changing social conditions and managing the underlying conflicts that create the threats, interdicting threats early, reducing funding sources and increasing traceability, creating indirect pressures against governments and substate actors, creating other enemies, seeding distrust and breaking up group cohesion, and a wide range of other techniques. The link between threats and vulnerabilities can be reduced by interdicting threat intelligence efforts, reducing the availability of information required for planning, creating deceptions to aid in the detection and misdirection of threats, finding key indicators for indications and warnings during the attacker intelligence efforts, and similar efforts. Vulnerabilities can be reduced by a wide range of methods ranging from selecting different software for control systems to changing travel paths for vehicles. The link between vulnerabilities and consequences can be mitigated by increased redundancy, target hardening, and consequence-limiting designs and similar techniques. And consequences can be reduced by reducing the interdependencies between systems and subsystems, locating potential targets farther from civilians, and a wide range of other similar efforts.

Even with all of these defensive efforts being done in a mixed strategy, it is also critical to identify and understand clearly the real situation both in terms of attack and defense. With precious few resources available for defense, spending must be done widely in order to avoid having insufficient resources for truly critical needs. Analysis of attack graphs is often done poorly and with an inadequate understanding of the real issues, using approximations that may lead to gross errors in protection selection. Theoretical attacks are not matched up with reality in order to make realistic assessments, and inadequate testing for validation of results is done. Databases in support of these analytical efforts are poor when they exist at all, and time issues are generally ignored. People who do not have true understanding are often placed in responsible positions and convinced by those with something to gain by the outcome that defending one thing is more important than defending another.

The Real Limits on Risks

As a starting point to this discussion, risks come from the simultaneous combination of threats, vulnerabilities, and consequences. Threats are actors who are motivated (or, in the case of nature, behave without specific motive) and able to do something, vulnerabilities are things that threats can exploit to produce consequences, and consequences are the outcomes of interest.

Unless there simultaneously exists a specific threat capable of exploiting a specific vulnerability to produce a specific consequence, the presence of these three elements cannot produce risk. As you will see, a lack of understanding of this principle is often at the heart of why risks are misperceived.

Electrical Power

Nightmare scenario: If electrical power throughout the U.S. or major regions thereof go out and stay out for a long time, the consequences could be dire. For example, having no power in the Northeastern U.S. for a month could cause a substantial number of people to lose their lives, cost a lot of money, displace a lot of people, etc. This is largely because power is needed for heat and for most sorts of profitable work that people engage in. If there is no such outage, the consequences are not only far less, but well within the normal experience we have due to nature. For example, outages of several days to a week or more are fairly common because of winter storms, regional outages have happened several times in the Northeastern U.S. as well as across the Pacific, and rolling blackouts have happened many times. None of these have produced dire outcomes requiring unusual precautions.

The power grid and the generating stations are not so computer dependent that the grid cannot work without all of these computers being operational.

> Example 1: Suppose I use a computer-controlled power grid element to shut off a critical feeder line into a major city? Solution: A linesman shows up at the junction where the power has been disabled and switches that station to manual override, turns the power back on and power is restored. The grid is not as efficient this way, but the power works just fine.
>
> Example 2: By exploiting a cascade failure similar to the ones that occurred in California in the mid 1990s (twice), an attacker disables a region and uses computer attacks to keep it down. Solution: In a few days, linesmen restore all of the power using manual overrides, some of the power stations don't come up as soon, but most power is restored in a few days, and the automated controls are not operated until the problem is found and fixed. There are a few other examples, and some cause some permanent physical damage to select parts of infrastructures, but none keep major portions of the power grid out of service for very long or can be repeated many times.

Water

Nightmare scenario: The water is poisoned for a major city by a cyber attack changing the chemical mix put into the water supply (too much chlorine,

for example) or water supplies are cut off to a region of the country by computers disabling the flow of water. The nightmare result of the former is that millions of people get poisoned with a resulting panic that causes everyone to fear with every drink. For the latter, everyone has to leave the city within a few days for lack of water.

> Problem 1: Other than the chemicals already in the water or in the water purification system, without physical attack, there is no way to add poisons by computer program. Maybe you are convinced you could break into some supplier computer and change the chlorine order or manufacturing process to send out LSD or something like that, but I think that the quality control is a bit better than this both at the water companies and at the suppliers. And chlorine (or other chemicals used to purify drinking water) has a tendency to kill almost anything you put in the water. If you put too much chlorine in the water it starts to smell of chlorine and people tend not to drink it. If you prevent the chlorine from going in to allow other agents to get through, the water also starts to smell bad.
>
> Problem 2: How is a cyber attack going to stop water from flowing downhill? You probably didn't know it, but there is a reason that reservoirs are on hills and water storage tanks are on stilts. It's because the vast majority of water supply is fed by gravity. Other than closing valves through the Supervisory Control and Data Acquisition (SCADA) system, computers are unlikely to counter the effects of gravity. And those computer- controlled valves all have manual overrides — and the computers are easily disabled — and the valves manually controlled. It is not quite as efficient, but the water will still flow. Even the pumps used to move water from lower points to higher points can be manually operated. In fact, the water systems used to be operated manually and the operators occasionally have to do it anyway because of computer outages.

It turns out that a clever attacker could probably damage some pipes here and there using computer-based attacks, but pipes are damaged in earthquakes and similar events all the time, and yet we have not yet abandoned any of those cities because of lack of drinking water. There is a far greater groundwater crisis facing us, but it has nothing to do with computer network attacks.

Natural Gas

Nightmare scenario: A cyber attack causes the release of all gas from the gas pipelines.

The safety measures in gas pipelines are not so weak that there is a way to get a computer to ignite the pipeline. This is because the computer typically controls a valve and the valve itself is designed to do its job without igniting things on fire.

A release event could potentially happen from opening a valve to vent to the air or perhaps the excess packing of gas into the pipeline creating an overpressure and a pipeline burst. In either case, the drop in pressure is rather obvious and results in an investigation before too long.

If gas is shut off near the source, the residual pressure in the pipe will allow continued flow for hours to days, depending on the specifics. In this time, the source will be repaired and service restored. If gas is shut off near the destination, relatively few people will be affected and this is not much different from normal events in gas pipe maintenance.

Gasoline and Fuel Oil

Nightmare scenario: No gas can be delivered to local filling stations (or no fuel oil to residences) for an extended period of time, causing loss of transportation capacity and spiraling collapse of the economy, eventually food shortages and starvation, etc. Nobody can really explain how a computer attack can cause this, of course, so we will simply move on.

Emergency Response

Nightmare scenario: 911 service is disabled by modems dialing 911 due to a computer virus, OR, break-in into 911 computers causes misinformation to the attendants inducing poor or lost service and inability to coordinate at times of disaster.

Emergency response typically includes radio backups, digital links for computer-relayed information, and, of course, the primary communications radios or land lines. In addition, local phone service is usually available in case someone has to place a call for help. Disaster recovery centers exist for most 911 services at the state level so that a massive failover uses redundant systems, circuits, and people to handle calls.

While serious problems can be induced by this sort of attack, a common technique for mitigation is increased telephone bandwidth and call screening by telecommunications providers. This has been successful in all recent large-scale attacks on 911 and similar services. In the case of misinformation in emergency response systems, this has happened with resulting loss of life. A small number of people died in the new emergency response systems installed in London several years ago, and a very recent failure may have contributed to the loss of life of boaters in Long Island Sound.

Financial Systems

Nightmare scenario: All financial records are lost for all bank accounts in the U.S. — and while we are at it — all brokerage accounts and stock records.

When the World Trade Centers were attacked, the telephone outages caused automated teller machines to be unable to communicate with their banks. As a result, the machines fed out money without checking. There was a substantial fraud-related loss (some small number of millions of dollars in all, I understand), but the system did not collapse. And even though the New York Stock Exchange ceased to exist for a week, the rest of the global financial systems continued to operate, the Chicago mercantile exchange did not collapse, and all records were not lost. If you wonder why, you need to read about disaster recovery planning. The question remains as to whether a large-scale cyber attack could somehow change this. I will assert that the answer is, practically speaking, no. Of course, theoretically it is possible, so let us see where it goes.

The theory is that all of the redundant systems of many of the major financial institutions in the U.S. are simultaneously disrupted in such a way that records are corrupted and unrecoverable for long enough to lead to economic collapse. If some of the redundant systems are still operating properly, the content is recoverable relatively quickly and they can go on. If only a few of the companies collapse it will be a problem but not a total disaster. Recent monthly statements and records from other banks and records given to the government in response to their reporting requirements and similar records will allow much of the lost content to be recovered, but it will be painful for a few million citizens. And yet the system will compensate — one way or another.

In addition, financial institutions, despite their appearance of incompetence now and then, are really quite good at detecting and countering frauds and corruptions — even by insiders. After all, they have been under constant attack by insiders for hundreds of years, long before computers came into play, and they handle very large sums of money every day under constant attacks without collapsing. Sure, Barings, (Britain's oldest merchant bank) will occasionally collapse from a risk management failure, but overall, the combination of redundant systems and massive diversity combined with the global nature of the market and the redundant nature of the records makes it very hard to collapse.

In this case, the problem is not that the potential for the consequence does not exist or that the vulnerabilities do not exist to allow such a consequence to occur. The problem is that in order for so many things to simultaneously be affected in so many different ways as to produce a massive collapse requires a threat that does not exist. Yes, strange as it sounds, there is no threat today that has the capability of achieving such a large-scale consequence to the global financial systems that we depend on.

Governmental Control

Nightmare scenario: Total government collapse results from information system attacks and outages.

In 2001, many experts started to be concerned about the potential for the use of electronic voting machines because of their increased use after the 2000 presidential elections. The following guidelines were suggested to the Institute of Electrical and Electronics Engineers (IEEE), and many of them were subsequently turned into critical components of the recommendations for electronic voting.

In order for any practical election process to really gain assured trust, it must have several properties.

1. It must be sufficiently simple and open so that the average person on the street can clearly see exactly how it works, understand it clearly and fully, and participate in it.
2. It must be observable by all parties at all times, so that there can be no real question about its legitimacy that cannot be answered by the individuals who were present at the scene.
3. It must produce evidence that cannot be easily altered or destroyed, that can be judged by nonexperts examining it, and that is not separate from the actual vote — they must be one and the same.
4. It must be very inexpensive to purchase, maintain, and operate. The lifecycle cost must be on the order of pennies per vote or less and it must be easily maintained by untrained people.
5. It must not depend on anything outside itself to operate and accept a valid vote, like electrical power, telephone lines, servers, etc.
6. There must not be significant spoilage of supplies or recorded results — either before or after the fact.
7. It must be physically securable on a local basis by local officials and police officials.
8. Each voting location must be able to function independently of all others in every vital aspect of the operation other than the summarizing of overall votes that cross localities.
9. Each voting location must be able to have unique vote layouts and candidates to accommodate the wide range of elections that run both simultaneously and sequentially.
10. The voters must believe that the systems work.

At this point in time, and for the foreseeable future, computerized and, particularly, Internet-based voting machines and networked voting systems do not, and will not, fulfill the majority of these requirements.

1. They are far too complex and full of details for the average person on the street to understand at all. In fact, analysis of these systems has shown that the designers and implementers made many mistakes that would allow for systematic information attacks against these systems.
2. The vote goes into a mystery thing and comes out somewhere else as a total. Nobody at the scene sees it go in or come out. There is an electronic card in many such systems, but no way to tell what is or is not on the card.
3. The evidence they produce is easily altered and destroyed and it requires substantial expertise to even view any evidence it leaves. Furthermore, that evidence is not in any physical way linked to the original vote. For example, the studies of current voting machines provided demonstrations of how large numbers of false votes that would be indifferentiable from real votes could be easily created.
4. They are expensive to purchase, maintain, and operate. The lifecycle cost is on the order of dollars per vote and they can only be properly maintained by experts. Indeed, the experts who maintain one of the major voting machine companies are hired and fired by a company president who has declared that he would do anything to assure that one particular candidate would win in a particular election.
5. They depend on electricity, network connections, servers, and so forth. It turns out that it is pretty easy to make each voting machine sustainable without power, but in several elections with these machines, voters were turned away at the poles because of power failures.
6. There are no supplies (except power and hardware components that require maintenance and replacement), but spoilage cannot universally be detected. Indeed, there is only electronic evidence of a vote and no way for the voter to verify what really happened or was counted.
7. The votes are not physically securable on a local basis by local officials and police officials in some systems because these systems are networked. One such system was wisely pulled from service because of such flaws.
8. In networked systems, each voting location cannot function independently of others. This is not a problem in most electronic voting systems requiring physical presence at polling place.
9. Each voting location can have unique vote layouts and candidate selections.
10. I do not believe that the systems work and many other experts feel the same way. But most voters may be fooled into that belief by a sufficient perception management process.

So, in the area of control of government, there are many valid scenarios in which electronic voting systems can be exploited to change the body

politic, and this is a very real threat to democracy. The Carter Center (http://www.cartercenter.org/) is an organization that seeks to, among other things, foster fair elections, and it has never certified that the U.S. has fair elections because these elections do not meet the criteria of the center. Electronic voting machines currently fail to meet these criteria as well.

Telecommunications

Nightmare scenario: If a cyber attack disables most of the national telecommunications capacity and keeps it disabled for a period of weeks, commerce will grind to a halt, emergency services and other safety-related failures will happen, and other side effects will ripple through the world we live in. Outages of a day or two for large portions of the infrastructure will not mean collapse, and this has happened before without collapse. Two good examples were loss of all telephony in major cities and all long distance telephony in the early 1990s. These were both due to a few bit errors in telephone system control software. The net effect was negligible.

> Problem 1: While taking out a telephone switching system or two might be feasible by cyber attack, there are many thousands of these systems in the US, and taking out a few here and there will not have any real effect. There is no commonality that would allow large numbers of them to be disabled without a large number of simultaneous attacks. This means many attackers well coordinated, but, of course, they can only coordinate for cyber attacks as long as they have telecommunications operating. In some sense cyber attack against these systems is self-limiting. The more of them you take down the less connectivity you have to attack the rest.
>
> Problem 2: A large portion of telephony runs through leased lines, which are more or less physically controlled at thousands of switching centers. While there is electronic equipment involved, changing many of the circuits involves moving a physical fiber or wire from one place to another. This cannot be done by cyber attack. Things such as perception management won't do it either because humans are involved and while you could probably fool them into switching a wire here or there, you will not get them to quickly switch the hundreds to thousands of them in every local switching center.
>
> Problem 3: There are other things besides switching centers. There are cell sites that are physically distributed throughout urban areas, and there is Internet telephony that runs over cable systems, and there are radio communications for emergency services, and so forth.

Problem 4: There are hundreds of thousands of dedicated professionals that run these systems. They are not perfect, but they will try very hard to restore services and they do know what they are doing. It took a few hours to a few days to identify and resolve the problems that have had large-scale effects on telephony in the past and the magnitude of effects has gone down with telephone diversification resulting from deregulation.

As with financial systems, the number of actors that would be required to carry a large enough scale outage and sustain it would be so high that there is no such threat, even though there are vulnerabilities and consequences that in the aggregate could produce worst case consequences.

Internet

Nightmare scenario: A "zero-day" virus with a highly destructive payload takes out all of the susceptible systems in the Internet in a matter of an hour or less and does damage that cannot be repaired for weeks to months. For example, one recent virus spread to many of the Internet's Windows systems in only an hour or so and it disrupted services to some extent. If it had a combination of the ability to delete all of the files on all of those systems, a trigger to deny services by sending out packets on all interfaces at maximum bandwidth, and exploited vulnerabilities on several types of systems at once, it could have disabled most of the Internet. But, as usual, this will only partly work.

Problem 1: The Internet operates in a distributed manner — in fact, it evolved from the original Advanced Research Projects Agency (ARPANET) that was designed to be able to withstand nuclear attack. That means that when you take part of it out, the rest of it just keeps going. Even if you could completely destroy the entire infrastructure between organizations, the 'intranets' within organizations would be largely unaffected for at least days and more likely weeks. The problem of making a virus that penetrates deeply enough into all of the hundreds of thousands of intranets is one that has never really been solved.

Problem 2: The mechanisms of attack are programs, not people. As clever as programmers may be, they are still no match for people. Once launched, lots of people can spend lots of time figuring out what the virus does and finding ways to defeat it. Of course, attackers can start virus after virus in a running battle, but while tracking a single virus release to its source may not be very easy, as the pressure on the continuity of the Internet grows, efficiency will be sacrificed and IP address forgery will be prevented,

> even at the expense of some bandwidth. Large numbers of sensors will be placed and focused within days, and the response to new viruses will be the harsh and rapid shut down of the assets that induced them. It will not take long before the weaker systems are weeded out and the stronger ones will continue to operate. And don't imagine that there are no strongly defended systems on the Internet.
>
> Problem 3: Destruction is limited by the presence of backups. Restoration of most systems takes less than a day and the loss of data from one day is typically not that extensive. For systems where loss of such data is critical and the consequences are high, there are typically adequate real-time backup and restoration processes in place to mitigate most such attacks. And each system owner does things their own way. As a result, systems without backups will collapse until forensic restoration is done, but systems with reasonable disaster recovery plans in place will recover rapidly and have the services causing the problems disabled.

And, of course, the final problem always remains that we have hundreds of thousands of trained experts who have a great deal invested in keeping the Internet operating. In times of crisis, they come together and fix things. In fact, the student program I used to run produced about five students a year that, on their own, could rebuild everything required to recreate a functional Internet in a matter of days. I have bootable CD-ROMs that can create functional Internet capabilities in minutes from bootup. The notion that any threats that exist will be able to defeat the efforts of all of these people is simply unrealistic.

The Internet is perhaps the weakest of the critical infrastructures — probably because it is the newest and in the rush to develop it the usual engineering expertise was abandoned in favor of time to market. Reduced cost was selected over increased assurance with the result of large-scale weaknesses that can be exploited in serious ways.

Interdependencies and Amplification

I was one of the first people to publish on the issues related to the growing interdependencies of critical infrastructures in the U.S. Of course, military planners have understood this since the days of Sun Tzu and, in World War II, it was grown into a mathematical discipline called operations research, but the increased use of information technology and its widespread embedding in critical infrastructure operations caused this to become a far more serious issue in the 1990s. The fundamental questions to be asked are these: (1) how do the interdependencies of infrastructures change the nature of what we have been discussing, and (2) how can information technology be

used to amplify effects and to what extent does this change the nature of what has been discussed here?

Interdependencies

The interdependencies of critical infrastructures have a substantial meaningful effect on the analysis of how attacks on infrastructures can work. It makes it a lot more complicated to understand the precise effects of combined simultaneous attacks on different infrastructure elements. For example, if there is a power failure induced by a cyber attack, the loss of power may disable the control systems for water systems, causing a loss of water to hospitals and resulting in patient deaths. These questions are very complex to analyze when you are considering small scale or effects, but they simplify greatly when you only consider high magnitude consequences.

In essence, the scenarios above show that very few of these interactions can have really high consequences. For example, if the power goes out for a few days, this will not prevent water from flowing. In fact, many water systems have their own power generation stations to recover energy from the gravity-fed water flow. These systems do not need external power at all and become energy providers. Similarly, local water outages will not prevent power from flowing because power is sent across entire regions on a continual basis to balance the generation capacity with the use across seasonal variations (more power for heat in the winter to the colder areas, more power for air conditioning in summer to the hotter areas). Telecommunication depends heavily on power, but as a result, major telecommunications systems like the telephone system have their own backup power, as do major Internet hubs and switching stations. That is why you can make a phone call during a power outage to get power restored. Unless you can keep power out for several days to a week, you cannot degrade these capabilities. It turns out that there are combinations of things you can attack that cause more damage than others, and as a result, a really skilled attacker can optimize effects by using combinations across infrastructures, but it also turns out that the limits on consequences described earlier for each infrastructure are essentially unaffected by attacks on other infrastructures.

Amplification

Amplification of effects by information attack is a much more interesting area. The notion here is that a physical attack could have its effects amplified by well-timed information attack. This is a very real issue and amplification is often possible through information attack. A good nontechnical example is the degradation of civil rights (governmental effects) generated by information "attacks" (perception management via the media) in association with the airliner hijacking attacks of September 11, 2001. Many of the components of the U.S. Patriot Act were already in the list of desirable legal changes for

many in the nation before the attacks took place, but once the attacks happened, the barriers to getting these legal changes made were greatly reduced, thus there was a synergistic effect. It turns out that the reduction in civil rights in the U.S. is a desirable side effect for those who practice terrorism. The new alert system in the U.S. magnified the terror effect by keeping the presence of the threat on our minds day after day, and the news media uses fear to keep more eyes glued to their shows. It creates a positive feedback effect: Increased viewing that increases fear that increases viewing — the net effect being an increase in revenue for the media. The increased fear also increases the ability to create more governmental changes that in turn induce more fear, and so forth. While there is a debate about the rationality of where the current balance is set, there is no doubt that informational methods amplified the physical attack to produce rapid political changes.

This essay is an example of how you counter this amplification effect. It should have a damping effect on the exaggerated claims about an electronic Pearl Harbor, that effect being achieved through some more in-depth examination of the facts. The effect of this essay can also be amplified, for example, by others choosing to cite it or it becoming popular in the media. Actually, there has been some recent trend in this direction as more and more experts have come out to say that these sorts of claims are being exaggerated.

Amplification is possible in every system described earlier. For example, by combining cyber attack with poisoning of a water system it is possible to increase the effects of a poisoning, by combining a cyber attack on the telephone system with blowing up some of the key switching centers, its effects can be prolonged, by disrupting the 911 emergency telephone system via cyber attack while doing a series of bombings, the response process can be impacted, and so forth. But while informational amplification can increase the effects of other attacks, those increases do not change the fundamentals of the limits on consequences. Water will still flow, electricity will still be repaired, financial systems will still function, and so forth.

Amplification and Interdependencies Combined

When you combine the interdependencies with amplification effects, it has a tendency to increase effects, but there are also feedback systems that kick in and tend to limit the amplification and inherent limits on rapid interdependency effects. In addition, for an attacker to exploit the combined effects in a controlled manner is likely beyond the current capacity of any threat. A major technological breakthrough and a large-scale research and development effort would be required to get a handle on early prediction and control of such an attack, and it would necessarily involve characterizing human behavior beyond the current capacity to do so.

In Context

Before concluding, I want to put all of this in context by comparing these scenarios to the ones associated with weapons of mass destruction — nuclear, biological, and chemical weapons. I do this because all of these cyber attack scenarios are somehow put into direct comparison with the serious consequences of these other sorts of attacks in order to get the cyber threat to be taken seriously. Here is how it stacks up.

Nuclear attack: Nominal consequences of a single nuclear attack using a common weapon of today set off at the same place as the planes hit the World Trade Center are on the order of 1000 times as bad in every way. Estimate 3 million dead or injured, most of Manhattan gone and not reusable for a long time, perhaps, 10 to 20% effect on the U.S. economy for years.

Biological threat: In natural disease outbreaks, up to 30% of the population of densely populated regions have been killed in the past. AIDS exceeds this in some areas of Africa and the influenza epidemic of the early 20th century in America and the plague in Europe are examples of what a biological weapon could do.

Chemical threat: This is the least lethal of all, with potential for killing up to hundreds of thousands of people in the area near the release.

Each of these involves a single use of a single weapon of its sort. The biological is extreme compared to likely effects of modern bioweapons against modern medicines and methods, but not unrealistic. Now if we look back at the impacts of cyber attack, in what rational way can we compare even the worst-case information attack scenarios (if they could even happen at all) to the deaths of hundreds of thousands to many millions of people? The answer is simple. Cyber weapons are not weapons of mass destruction, or disruption, or even worthy of comparison to nuclear, biological, or chemical weapons. While they are a serious issue to be considered, they should not be exaggerated.

What Terrorists Do in Cyberspace

If we are going to look out for the cyber terrorists, it will probably be helpful to know what to look for. Nobody can accurately tell you what will happen in the future. If I knew, I would probably keep it to myself anyway. So all we can really do is understand the past and predict the future. Recent history shows that terrorists do the following things in cyberspace.

- *Planning:* Information technology is used to plan terrorist operations. This generally includes intelligence gathering, analysis, coordination of personnel and equipment, and other aspects of operations.

- *Finance:* Information technology is one of the keys in the financial system of terrorist organizations. They use information systems to get funding, track books, move money around, coordinate financial actions, and make purchases. Funding often goes through so-called charitable donations, through computer crimes like credit card theft, through solicitations of any sort, and naturally, through the drug trade. The drug trade is facilitated by information technology in the money laundering and funds transfer arenas as well as acting as a communications media for the sales and delivery process. In cases involving computer crimes, it is important to report to authorities so they can coordinate the actions of groups across many small activities to see the bigger picture.
- *Coordination and operations:* Many activities are coordinated through information technology. This ranges from the transmission of "go" signals for coordinated starts of operations, to synchronization of global activities, to arrangements to meet incoming shipments, to digital versions of dead drops. The convenience of information technology on a global scale makes it ideal for small groups to act on a globally coordinated basis with relative safety through encryption and steganographic technologies combined with anonymity. Information technology in the form of radios, telephones, and pagers is used as an operational tool all the time. Computers are also used in real time for activities ranging from checking identities to determine who to keep in a kidnap operation to satellite links for tracking ongoing operations via the media. With increasing frequency, information systems are being exploited to facilitate operations or as the objective of an operation.
- *Political action:* One of the key efforts of terrorist groups is the use of information technology to gain political action and attention. This ranges from high profile web sites that urge supporters to contact their congressman to sites that give detailed instructions on how to hold protests for maximum media effect. These sites are legal, as long as they are created in a legal manner. They are interesting to read because they clearly show that these organizations are oriented toward media attention and that most, if not all, of the street protests and similar activities are not spontaneous — they are planned media events.
- *Propaganda:* Many web sites are used by terrorist organizations as part of their propaganda machines. These sites actively promote the ideals of the movements, provide selected facts and lots of misleading statements, include pictures that are identified as one thing when they are, in fact, something else, and so forth. They include smear campaigns, pictures of blown up bodies, ancient propaganda as the basis for current propaganda, and so forth. For the most part, these sites are legal and designed to support current and future membership

> by providing support for their pre-existing notions and giving them "facts" to back up their beliefs. The vast majority of the information is not directly false, but is clearly slanted.

Although there are some other ways that terrorist groups might use information technology, the vast majority of activities to date have been in the areas described earlier. There have been outliers — ranging from the use of a chat room by a Palestinian group to lure and kill an Israeli teenager to the attempts to break into U.S. energy companies by middle Eastern groups to the sale of software to run police systems by the Aum Shinrikyo group in Japan to the exploitation of laser-based remote bomb controls by the IRA. Obviously, if you encounter anything like this you would want to report it to federal authorities right away.

The Relationships between Critical Infrastructures

It would be a bit of fantasy to imagine that all infrastructures are created equal. For example, the power grid is certainly a critical infrastructure for most of modern society around the world. It produces failures in very short time frames, can have widespread effects, has a history of massive cascade failures, and underlies most other elements of critical infrastructure at differing time scales running from immediate to a week or more. Recovery times can be days to weeks in some cases, and the power infrastructure runs largely above ground in easily identified and reached wiring. Compare this to most water systems that are largely independent of other water systems, have enough supply in most cases to operate for a day or more, and independent capacity to produce output for quite a bit longer if they need to. They tend to fail in time frames of hours and recover in similar time frames, are not very susceptible to cascade failures, tend to affect small areas with populations in the tens of thousands or less, and have a long history of reliable operation and graceful degradation over periods of many years. While speculations about poisoning tend to run rampant, the volumes involved make realistic large-scale poisonings fairly difficult to accomplish and relatively easy to mitigate once detected. Water tends to run underground and even when pipes are damaged, the failures tend not to be catastrophic.

Some Interdependencies

It seems clear that protecting power supplies is a far more time-critical operation than protecting water supplies and that the amount of effort required for power protection will be far greater because of ease of physical access, ease of location and characterization of facilities, and the ability to destroy power grid elements at a distance with rifles and similar equipment.

With this notion, some seek to create a hierarchy of infrastructure systems, but most attempts fail because infrastructures are codependent.

While power infrastructure has very short time constants, financial system failure could stop much of the power system over a somewhat longer time period by destroying the mechanisms used to generate funds that pay the employees who work for the power companies. A payment system failure might prevent international payments that bring in the oil needed to fuel cars that bring people to work in the other infrastructures. Similarly, a direct attack against the oil and gas infrastructure would make the transportation required in order to bring fuel to fossil fueled power plants to those plants impossible, thus breaking the power system. The transportation system is, of course, critical in this process, but without communications operating properly, the processes used to get the transportation system working are not present. And, of course, without communications, the power system runs open loop, goes out of control, and cascade failures result. Communication is also critical to government and civil order. For example, police and fire crews cannot serve emergency needs unless their communications systems operate properly. Of course, they also need gasoline for their vehicles, water for their fire trucks, and so forth. While water is on the table, people typically die after a few days without water, and water systems, while less dependent than many other infrastructures, require supplies over time frames of days to weeks in order to keep purification systems operating properly.

So either directly or indirectly, all of the different components of critical infrastructures are interdependent. While select failures in each sector are survivable, the aggregate failure of a whole sector or enough independent parts can cause extremely high consequences. While we can try to characterize all of these interdependencies and some efforts to do so are underway today, creating the ultimate map of critical systems is itself a serious problem for several reasons. Of course, these infrastructures are constantly changing, so tracking those changes would be problematic, but an even bigger concern comes from the potential for abuse that such a system would have. As an attack-planning tool, such a system could provide exactly the information necessary to determine optimal attack sequences and maximize harm while minimizing attack costs.

Models of Interdependencies

This may seem speculative to many, but there is a good model for just how effective such techniques can be. Of course, efforts for optimization of military planning have been underway since World War II. As a result of the mathematical analysis of military operations, the field of operations research emerged with its optimization algorithms now used across all industries to analyze financial and operational decisions. Every business school student

and most graduate students in scientific fields are taught algorithms for optimizing mathematical programming problems of various sorts. Software packages in support of this analysis are commonplace and widely used. What started as a military approach to optimization of resources in a global war became commonplace in business. But this is not the end of the story.

The transportation problem is one of the most well-known problems of this sort. It is essentially the problem of finding the optimal routing of a set of loads between places on a map. Think of cities as nodes and roads as links in a graphical depiction, like a roadmap. Transit times for different paths on the map are gathered based on experience and written down. The problem is to figure out the best possible routing for efficient use of trucks. This particular problem, like so many similar problems in optimization, is well known to be mathematically complex and, thus, very hard to solve for large numbers of nodes. As a result, a great deal of time and effort is spent in finding better algorithms for use in parallel computers to allow the reductions in costs associated with these algorithms to be gained by improved use of computers.

One of the most recent examples of the use of such systems was the first Gulf war in the early 1990s. In this war, well-developed logical maps of Iraqi critical infrastructures were analyzed to optimize bomb target selection. Every night, the results of bomb damage assessments from the previous day's bombings were fed into a computer system and analyzed against critical interdependencies of the Iraqi war capacity. And each night a new prioritized target selection list was generated to optimize the next day's efforts. This resulted in far more efficient bombings and reductions in the Iraqi war capacity and was part of the reason that the war went so quickly and so well for the allies aligned against Iraq.

Model Effectiveness for Attack and Defense

Models are very effective in some applications, such as launching attacks. With a decent model of interdependencies, optimal sets of targets can be identified for strikes. As a result, we know that models are outstanding for threats from those who wish to optimize the effect of their efforts. But does this make them useful in defense? Unfortunately, defenders have a far harder time finding effective uses for models than threats. Of course, a defender can model to find an optimal attack against and use that as a guide to defenses, but suppose the threats have a different optimization criterion? In this case, the wrong defense might be put in place for the attack actually planned. And, of course, even if the models are identical, not all threats have the same objectives. And even if they did, they might try for less than optimal attacks because of opportunities that arise.

When it comes to modeling for nontrivial systems with multiple sequential actions by opponents, we enter the realm of gaming and simulation. Game

theory addresses a variety of game parameters and provides mathematical analysis methods for game analysis and optimization.

Conclusions

Just as business has prospered in the Internet era because of the efficiencies associated with deeply embedded information technology, criminal and terrorist groups have taken advantage of the technology to their own ends. Technology brings efficiency to all who use it.

From the perspective of the security manager, cyber terrorism has not changed much about the way one operates, but it does produce some changes in the way one might respond to incidents. In particular, it should produce changes in the response processes and policies with regard to Internet use. Clearly, understanding how to successfully defend critical infrastructures against the threats that they face is an ongoing process that will never really be complete. But just as clearly, there is a need for thoughtful experts to create a considered approach to protection that rationally examines the situation and presents a balanced view. Otherwise, foolish decisions will be made with financial interests of select parties resulting in failed protection and wasted lives and fortunes. This unsettled field cries out for university research and an exciting multifaceted educational environment.

Information Warfare, Netwar, and Cyber Intelligence[1]

8

FRED COHEN

Contents

What Is Iwar and Why Is It Important?

Information warfare (iwar) has been studied in various forms for a very long time, and yet the definitions of it are still varied across a wide spectrum. Let us start with a definition that has some merit.

> Information is symbolic representation in the most general sense. Warfare is high-intensity conflict between opposing parties. Information warfare is about manipulating and protecting the symbolic representations used and targeted in high-intensity conflicts.

Now, this probably seems like a really strange definition to most readers who are not familiar with the field and somewhat less strange to those within the field, but I will explain it by discussing other views and relating them.

Network-Centric Warfare

The most common perception in the public of iwar is what some in the U.S. military came at some point to call *network-centric warfare*. This is where warriors use computer systems and networks to attack opposing computer systems and networks while trying to keep their opponents from doing the same to them.

It is important to note the common threads: There is always attack and defense in warfare and there are always at least two sides (them and us). Network-centric warfare focuses on computers and the content they bring to use. It is the utility of the content that is ultimately at issue here.

- Attack
- Defense

There are always at least two sides:

- Them
- Us

Objectives

For example, if the attack is intended to disrupt network operations, the real goal is to deny the enemy the utility they would normally have from the content and perhaps to consume their resources in trying to regain that utility. If the attack is corruptive in nature, the idea might be to alter the utility of the content to favor us. If the goal is to leak information, then we are trying to gain the utility that access grants us and perhaps reduce the utility of the same information to them. An attack designed to defeat accountability is typically used

to manipulate the results of applying content so as to gain a financial or power advantage without them knowing who did it. And an attack designed to defeat use control grants us the ability to use their content to gain utility against them and keep them from using it to gain utility against us. On the defensive side, we are trying to prevent them from doing all of these things to us.

Objectives include either protecting or defeating:

- Integrity
- Availability
- Confidentiality
- Use control
- Accountability

In order to understand this more clearly and deeply, we need to understand how content is used in warfare. What is its utility? This, of course, depends a lot on the specific them and us involved. The U.S. military, and most military organizations in the world, use content in an enormous variety of ways. For example, automated weapons systems like missiles use content to determine where the missile goes. Thinking in terms of the defensive objectives of integrity, availability, confidentiality, use control, and accountability, failure to meet those objectives could result in retargeting the weapon against our own troops, making the weapon fail to arm when deployed, alerting the targets that the weapon is aimed at prior to deployment, causing the weapon to explode just before deployment, or being able to take and sell the weapon to them or others without getting caught.

Mismatches

Definitions are very important to iwar because the way people think about the issues drives the allocation of resources and the focus of attention they place on different things. Because winning battles and wars is very often about creating mismatches and because military organizations tend to be hierarchical, a poor or improperly matched definition by a high-ranking individual can drive a military down the path to defeat. A good definition can, of course, bring strategic advantage and victory after victory.

The Spectrum of Conflict

As a basic principle, it is important to understand that not all warfare is totally destructive. More generally, conflict ranges over a broad spectrum from almost completely cooperative and friendly with the most minor of

disagreements to the sort of rage seen in hand-to-hand combat and the extreme violence of nuclear weapons. All war is not total war, and iwar in one form or another exists at all levels of intensity.

Conflict also tends to wax and wane with time. People have only so much energy. They can get enraged, but they long for peace, and many people cannot stand to live in peace and calm all of the time and seek adventure and excitement. Societies become anxious for conflict when properly prepared, but they tire of them over time, they exhaust resources, tire their fighters, create enormous burdens on the society, and wear down resolve.

> "If the campaign is protracted, the resources of the State will not be equal to the strain.… There is no instance of a country having benefited from prolonged warfare." Sun Tzu, *The Art of War*, 1910 translation of 5000-year-old ancient texts.

Certainty and Intelligence

Many view iwar as inextricably tied to intelligence, and certainly intelligence in warfare is about gathering useful content about the enemy. But countering the enemy's intelligence efforts is also a critical element of iwar. From an offensive standpoint, the goal is to gather, fuse, analyze, and evaluate information so as to increase your certainty of the realities you face, both about the enemy and about yourself. In addition, I will call it *offense* to decrease the certainty with which the enemy knows the realities about you; however, this is a great simplification in that there are certain realities that are intended to be projected toward the enemy. On the defensive side, the goals are to prevent the enemy from decreasing your certainty about the reality and to prevent the enemy from increasing their certainty.

Iwar has been described by many in terms of the impact of information technology on warfare. This comes in several major areas from an offensive standpoint. One of the most important areas is the implications for time and the tempo of operations. Tempo is the rate at which things can be done, and as Boyd pointed out in his work on the Boyd cycle, the rate of the decision cycle along with its accuracy determine to a large extent who wins and who loses battles. If you can observe, orient, decide, and act faster than the enemy and do it with the same or greater precision and accuracy, you will win almost every time and by a great margin. The Boyd cycle:

Tempo and Time

Offense:

- Increase your certainty
- Decrease theirs

Defense:

- Retain your certainty
- Don't let them keep theirs
- Observe
- Orient
- Decide
- Act

Nowhere was this more clearly demonstrated than in the first Gulf War in a particular battle called "*The Battle of 73 Easting*." In this particular battle, several U.S. tanks came up over a small berm, and as they emerged they encountered scores of Iraqi tanks, all loaded, fully manned, and ready to fight. Over the following minutes, these U.S. tanks killed every one of the enemy tanks and did not suffer even one death by enemy fire. They did it because they had faster tempo. They were able to observe the situation, orient themselves to it, make decisions about what to do, and act before the Iraqi tank commanders could target them. And they were able to keep moving while firing accurately at target after target. This was the direct result of the use of information and information technology in their tanks and of their training in how to do battle at this pace. The ability to act faster and more accurately is an advantage brought about by information technology that is so great that 10 to 1 odds are no problem to overcome with a significant tempo advantage. Looking at relative casualty counts, the advantage in that war was even greater, on the order of more than 100 to 1. Clearly, information war in these terms is fundamental to success.

Targeting

In describing the Boyd cycle, we have described another enormous advantage relative to the fog of war. It was not only the rate at which U.S. war fighters could act that won this and many other battles, it was the ability to identify, locate, and hit targets with higher accuracy and more often that also won the day. And again, this is a place where information technology has dramatically altered the nature of armed conflict.

> The ability to find and kill distant targets using complex infrastructures, in real time, is unparalleled in history.

The ability to target a particular weapon on a particular location where you know the objective lies, without expending excess resources while limiting collateral damage is also an incredible advantage in terms of both efficiency and perception. This is largely the result of advancements in information technology. The current situation is incredibly complex, but a simplified example should help to clarify it.

Suppose I want to find and kill enemy weapons that might be interfering with my plan to take the next hill. The process involves data collection in the form of everything from ground troops in hiding to satellite imagery in real time. From these data, there is a fusion up and across different echelons until the lowest echelon that can have access to all of the data required to identify and locate targets. Targets may be identified and located by people and their systems at a location far distant from my group, and the fused data are presented on a display that shows me everything within a few miles of my position. I then select the targets of choice and make a request for weapons systems located miles away to put weapons on these targets within the next few minutes. Those systems take the targeting information, send off their weapons, and coordinate the activity across hundreds of different similar simultaneous activities, landing the right weapons on the right targets so that when I go over the next hill, I will face little or no resistance.

Interdependencies and Brittleness

All of this complicated stuff that has to happen in order for this war fighting result to take place means that there are a lot of opportunities for failure. If the signals detected are wrong, the analysis incorrect, the fusion corrupted, the presentation in the wrong color, if any element of the communications or computation is unavailable, if the targeting is in error in any way, if the missiles have an error, or if the enemy finds out what is happening, the game is up and the overall system fails to accomplish its mission. The result is that the soldiers going over the top of the hill meet strong resistance and there are dead and wounded on both sides instead of just on their side, or even worse, all of the casualties on our side of the hill and the enemy occupying it.

This returns to the previous harkening to integrity, availability, confidentiality, accountability, and use control. These protection objectives are absolutely central to winning the information war. But this example is, of course, highly limited compared to all of the elements requiring effective information for success in war. Supply and logistics, battle damage assessment, procurement, troop deployments, strategic decisions, tactical decisions, everything in modern and historic military activity depends critically on the content and its proper use.

> The same infrastructures that support the military support our whole society . . . This makes them legitimate military targets.

Lest you come to believe that this is only a military issue, consider that the information infrastructures that support military operations are integrated at every level with the infrastructure elements that all members of modern society depend on for their survival. The same power supply that supports military communications supplies civilian populations. The same information infrastructures support both military and civilian communications. The same supply and

logistics chains form the back end of both military and civilian societies. We stand together or fall together. These infrastructures are legitimate military targets.

Economic War

If winning the war involves swaying the hearts and minds of the enemy, the Cold War was an example of winning the war without firing a shot. Some shots were fired in the Cold War, but for the most part, it was a war with no battles. It was fought with pure strategy because neither side was willing to assure its own destruction by attacking the other directly. In the end, it was an economic war, not a nuclear war, and the Soviet Union literally lost its capacity to fight as it lost its ability to sustain itself. The U.S. is having a similar conflict with China and is having problems sustaining itself as did the Soviet Union. Sun Tzu had it right when he said:

> … if the campaign is protracted, the resources of the State will not be equal to the strain … when your weapons are dulled, your ardor damped, your strength exhausted and your treasure spent, other chieftains will spring up to take advantage of your extremity. Then no man, however wise, will be able to avert the consequences that must ensue.

While most wars are about economics in one way or another, in the information age, as information has literally replaced other fungible financial instruments, that information is subject to direct attack in the form of network-centric warfare. National economies can be ruined by successful attack on computer systems. Move all of the balances in all of the accounts so that transactions fail, the rich become poor, the poor become less poor, and a few people here and there end up with the representations of wealth. The tangle gets so deep that nobody can undo it. Ask the Japanese company that recently lost almost $300 million in a day when an error in a computer entry that could not be repaired by the Japanese stock exchange in time resulted in enormous numbers of shares being sold for 1 Yen each — almost a millionth of the desired offered value.

Intensity Levels of Information War

Iwar, as all warfare, varies in intensity over time and by situation and location. Low-intensity warfare is often associated with political disputes that get out of hand, protests, and perhaps even riots. Different sorts of things come into play as the intensity ratchets up and they are put back away as the intensity ratchets back down. In addition, the lessons of high-intensity warfare are of enormous value in understanding and winning lower intensity conflicts. Indeed, if we get good enough at dealing with these issues, there may not have to be high intensity conflict any more.

The Spectrum

The electromagnetic spectrum, as well as sonic and time domains, afford a lot of potential for exploitation in what is sometimes called electronic warfare, but is simpler to think of as low-level iwar. In essence, information operates at all levels from the lowest levels of physics where information is intimately tied to the very heart of atomic particles and how they work through the signals level wherein communications and storage of signals are used to encode content and apply it, through the linguistic level where content takes the form of defined syntax and semantics, through the levels of behavioral detection and response, and all the way to the level of human, animal, and automated thought processes, and presumably beyond even these.

> Theoretical and practical understanding of fields, waves, and the theories of electromagnetic systems can be very useful in information warfare.

Because, in general, gravitational effects exist at arbitrary distance across the entire universe, it is, in theory, possible to derive information at any point in the universe about the situation in any other point in the universe, with delays associated with the speed of light. So, again in theory, there is nothing that can ever be done to perfectly prevent anyone anywhere from knowing anything anywhere else a very short time later. But in practice, the world does not work as well as it does in theory or, rather, there are advanced theories that tell us more about how the world works, including the limits of the ability to actually derive this information and the practical limits associated with mechanisms that we use to do so.

The basic notion that wave forms are required for storage and manipulation of information content and that it is impossible to perfectly assure that those wave forms are under your control means that there is a wide range of potential for exploitation. This in turn makes a capability to control the spectrum valuable in conflict.

> The equities issue rears its ugly head again in electronic warfare.

From an offensive standpoint, weapons have been developed to allow corruption, denial, and leakage of electromagnetic signals at a distance. From a defensive standpoint, there are methods that allow the defender to make the offensive methods a lot harder to accomplish. But defense is typically harder to do because the attacker may attack anything using any capability, whereas the defender may have to defend against a lot of things and may miss the thing the offense came up with. Thus, secrecy of the offense allows defeat of the defense, while a good offense allows the defense to know what the other side's offense is. Hence, even if there is the potential for conflict,

the defense must press the offense to get the information it needs to defend, whereas the offense must not provide too much information to the defense or the defense will be able to defeat the offense.

At a more practical level, all defenses have holes, but they can often be reduced if we understand them. Meanwhile, offenses are highly susceptible to deceptions but defenders are typically not as good as they should be at using them because of cultural issues. Once attackers are detected, they can be eliminated to limit their attempts. This is the place the defenders should focus their iwar efforts if they want to change their equities in their favor.

Waveforms

In general, electromagnetic or sonic disturbances take the form of waves. The form of those waves, the manner in which they rise and fall with time, has everything to do with the information they carry and their effect on the world around them. The folks that work on electronic warfare spend their time developing mechanisms to sense, create, and alter these waveforms to advantage. For example, a wave form could

- Cause the power supply of specific types of computers to fail without affecting other similar types.
- Cause a display to become over charged and need to be degaussed, producing a few seconds to minutes of lost utility.
- Cause speakers to produce harsh sounds resulting in listeners being distracted or even having their ears affected for a period of time.
- Cause printers to seize up.
- Be used to open or close a garage door without the owner pressing the button.
- Be used to break starters or alternators on cars or even to stop cars in their tracks by disabling their internal electrical systems.
- Cause wireless systems to fail over areas controlled by the attacker while their radio equipment continues to operate.
- Cause cellular telephones to fail. A waveform could be used to cause radio frequency identification tags to fail or identify themselves.
- Be used to alter signals between systems so as to cause remote systems to report the wrong data.
- Be used to change your television channel from your neighbor's house or across the street.
- Be used to cause your cellular telephone to turn on and start transmitting whatever is said in its presence.
- Be used to cause all of the pagers in an area to go off at the same time.
- Be used to cause location systems on airplanes and cars to go awry and report the wrong locations.

- Be used to light up a target for aiming a missile at it.
- Be used to prevent sounds from passing a barrier or to induce other sounds at the barrier.
- Be used to order audio inputs to computers to take actions even though the user could not hear the commands being made.
- Be used to detect the presence or absence of materials on or within people passing a barrier.
- Be used to detect movement in an area.
- Be used to detect changes to wiring or attempts to add external wire tapping devices to a wire.
- Be used to cause troops to become temporarily blinded in a military situation.
- Be used to cause intelligence systems and sensors to target the wrong locations.
- Be used to take over control of remotely operated vehicles.
- Be used to detect how fast vehicles are traveling or to counter devices that do that.
- Be used to cause groups of people to have to immediately go to the bathroom, feel sick, throw up, have intense skin pain, or become disabled.

Every one of the items described earlier has been done in the real world and is part of either a commercial or military capability in use today. And this may only be the beginning.

EMP Weapons

Electromagnetic pulse (EMP) weapons are sexy in the sense of having gotten some public interest as a result of their effect on normal everyday folks when atomic weapons testing was underway and subsequent hyperbole surrounding their potential use in other venues. Of course, EMP weapons are real and do exist, but understanding them requires a bit more than just fear.

> EMP resulting from nuclear weapons use is one of the side effects of these weapons that was not anticipated by the original designers.

EMP effects of nuclear weapons were discovered when nuclear testing in the atmosphere wiped out power in a substantial land area in the 1950s. At that time, a fairly intensive research effort was undertaken to understand the issue both from an offensive and a defensive standpoint.

The concept behind EMP is that a pulse of the right magnitude and rise and fall time will cause many devices to fail, including most radios, computers, storage media, power, and communications systems. Thus, an EMP weapon

of sufficient magnitude could wipe out most of the technological information capabilities of an opponent over some areas of space for some period of time.

The Russians are best known for developments in this area during the Cold War when they created weapons that could be used in relatively small areas such as battlefields. This was a strong counter to the U.S. increased use of technology in their weapons systems.

Since that time EMP weapons are rumored to have been used in many other contexts, ranging from causing outages in banks to wiping out all of the data in computers at an abortion clinic from the parking lot. Most of these rumors are just that. EMP weapons must produce a very high level of energy in order to destroy computers because they are relatively gross in terms of their waveform design.

Taking Out Swaths of the Earth

A very different approach to disruption of information systems stems from an effort to understand the field lines of the Earth. The Earth has electromagnetically charged poles that cause magnetic compasses to work. These fields generally run from magnetic pole to magnetic pole over the entire Earth and, in addition to protecting the Earth from Solar flares and other similar outer space effects, these poles change over time because they are induced by the electromagnetic currents arising out of the hot metallic components of the Earth's core. Every once in a while, they even flip so that North and South magnetic poles change.

> Energy weapons taking advantage of Earth's fields may achieve enormous changes to the way many systems work. But the side effects may be large as well, and the ability to control effects is vital to their use.

It also turns out that these fields surrounding the Earth can be altered by the systematic induction of energy near where they enter the surface of the Earth. Since Alaska has access to many of these locations, the U.S. government has done experiments and developed installations to use positive feedback in the electromagnetic field lines. Apparently, it is possible to change the underlying electromagnetic parameters for a substantial swath of the Earth by this sort of activity, causing essentially all electromagnetic functions in those areas to act quite differently than they normally do, including biological functions.

Such an attack could have devastating effects on any country that is highly dependent on information technology, but there is substantial question about whether it can be selectively targeted tightly enough to be a useful weapon.

Extensions of the scientific results from this sort of research and development to energy weapons, the required energies, and how to produce and direct them are likely to be highly applicable to other weapons systems.

Tempest

Tempest is a U.S. military term that has become widely adopted for describing emanations security. We will be discussing the broader issue of limiting the introduction or emanation of signals associated with content. The EMP weapons and similar waveform approaches are often used to disrupt or disable systems, but in the more insidious approach, waveforms are injected or examined to produce content, the stuff that has utility in information systems and technologies.

There are a wide range of methods for producing signals that result in comprehension by the systems they are directed toward. For example, by using the proper frequencies and projecting sound waves, a person can quite literally be made to hear voices coming from within their head. Similarly, frequencies that dogs hear but people do not can be used to *command* animals without people suspecting there is even communication underway. High frequency sound can sometimes be used to command computers with sonic inputs as well. Similar approaches allow surreptitious introduction of control signals into wireless systems, such as Bluetooth interfaces to computers.

Tempest also involves the ability to listen to content from afar. So-called van Eck bugging is an approach published (then removed from printed copies, but some still got through) in *Computers and Security* in the 1980s. It describes how a simple television tuner could be tuned to the proper frequency and observe the content of a distant computer display because the computer display emanated signals from its high-powered cathode ray tube indicating what was being displayed. This was demonstrated from a panel van that was able to show what was on the screens of New Scotland Yard in London. It made quite a splash that police computer access could be observed from outside of the building, but the military folks of the world were well aware of these issues before the van Eck demonstration. For a long time, they had been concerned about these sorts of emanations compromising national security secrets.

It turns out that it is quite difficult to stop emanations because they come in so many forms from so many places in so many ways. For example:

- A researcher recently demonstrated that the visible light from a display screen (all types) reflects off of glossy wall paints over several bounces and can be detected and used to reconstruct what was on the screen, even around corners, through windows, and at a substantial distance.

- Another researcher demonstrated that by inducing specific graphics on a screen, the display could be made to emanate AM radio signals of the display generator's choice.
- Many researchers have shown that power supplies allow high-frequency information to pass through them resulting in picking up instructions and data from computer central processor units and bus activities.
- Different sounds have been detected from different keys of a keyboard allowing a carefully used listening device to detect what is being typed by the different sounds.
- Timing of keystrokes also provides information on what is being typed to the point where it has been used to extract passwords from timing information alone.
- Conversations can be picked up from shining laser beams at window glass at long distances and observing the phase differences in returned light, which correspond to the glass movements resulting from the audio waves in the room.
- Many displays emit sounds at high frequency associated with what is on the screen and these sounds may be reassembled into meaningful signals.
- People mumble to themselves and careful listening with directional microphones can pick up what people "*say to themselves*" as they think through things.

There are many other examples of Tempest releases that affect people, computers, and systems of all sorts.

Countering Tempest

The problem from a defensive standpoint is how to counter tempest attack methods. There are basically three things you can do at a generic level to defeat tempest attacks. You can

- Suppress the emanations of signals.
- Increase the distance between the source of signals and their capture point.
- Introduce false signals to make it harder to understand what is sensed.

Suppressing emanations has theoretical limits. Reducing power levels of sources help a lot, as does the use of a Faraday cage or properly absorbent materials. A Faraday cage is a wire mesh cage. According to the wave nature of electromagnetic phenomena, if the frequency is such that the wavelength is greater than the mesh size, the waves will not pass through the mesh. But computer signals in particular use square waves, which are composed of large numbers of sin waves of different frequencies in different proportions.

The higher frequency harmonics tend to get through Faraday cages that have enough mesh size to allow air through. So if a full enclosure is used, it has to either enclose the air the people breath and the power needed to operate or there will be emanations at some frequency through some channel. Absorbent material is used to reduce emissions in wireless networks to substantial effect, but this is far more effective at directing waves and limiting interference of primary signals than for reducing emanations. It is also used in things like stealth aircraft for similar effect.

Distance in the form of perimeters can be used if it can be assured that the listening devices are outside the perimeter. This then begs the question of Trojan horse hardware and its use in listening to emanations and retransmit via covert channels. Generally, the available signal reduces as distance increases and in unrestricted space with an electromagnetic signal emitted from a point source, this reduction in available energy for detection for a given sized detector goes down as the square of the distance from the source. For different shaped emitters, different spaces, and different types of signals the reduction may be more or less. For example, material that reflects or absorbs energy in the wavelengths of interest will reduce the signal at a point, while a laser or wave-guide can keep energies higher at longer distances in the direction of the path. Radio emissions at very low power, for example, can reflect off of the ionosphere, ionized layers, or different air density regions and bounce across the World while reception within only a few miles of the same source may be impossible for the same receiver and transmitter.

Introduced signals include such things as noise generators and false information interlaced with real information, frequency hopping with noise injection, and similar techniques, all of which make picking the true signal out from false signals harder for the receiver. For example, for people trying to listen to sounds, a set of recordings of thousands of people at parties having conversations could be introduced into a perimeter area so that the desired set of voices become far harder to discriminate. Similar signal injection can be used for signals from computers and other media; however, this is not an easy task to do well, even for the highly educated and experienced among us. The Russians introduced a piece of equipment called "*The Thing*" in a gift to the U.S. embassy in Moscow. It was a seal of the U.S. with an embedded cavity with a metal rod protruding into it, all concealed within the wood of the gift. It turned out that by transmitting microwaves into the embassy, the device would produce different returns based on the sounds in the room vibrating the rod within the space and the Russians could listen to the discussions underway. It also turns out that with a predictive receiver that picks out the number of available messages from a select number of messages being sought, very high quality of reception can be done. Speech patterns of individuals may be put into a predictive receiver to detect their speech, even

from within a crowd. And directionality can be used to dramatically reduce noise levels. It is all part of the tempest world of the information warrior.

Deceptions

The introduction of false signals begs the question of deception in those signals as well as elsewhere. While the general topic of deception is clearly embedded throughout iwar, the use of deceptions in the direct analysis and injections associated with the spectrum is somewhat more limited today. In general, while everything has a representation in the electromagnetic spectrum, including all matter and energy, the complexity of generating arbitrary sets of waveforms in an area of space is, at least for now, way beyond any foreseeable future.

> As deceptions become more accurate, higher fidelity, and more complex, they also become far more expensive and harder to do.

On the other hand, the quality of the deception and its effectiveness are driven largely by the fidelity with which the deception is carried out. A cocktail party sound effect may say "*go away*" to a listener, but a serious attacker may also become all the more determined to isolate the voices of the subjects of the surveillance. A more serious defender may realize that this could happen and create far more elaborate deceptions involving the transmission of realistic information content so that even once received and analyzed, it becomes impossible to tell the fake secrets from the real ones. The use of special words and codes in communications may also augment the counter-surveillance effort to make the utility of signals intelligence far more limited.

Defenders can create fictitious targets for attack so that the incoming signals appear to suppress an activity when they only really drive it underground and give warnings to the defenders of the presence of attackers. All of this, of course, depends on the capacity to create realistic deceptions at a level of quality such that the attacker is unable to tell the deceptions from the realities, even as they actively attack the overall system using the spectrum as only part of their overall effort.

Sounds and Silence

One of the most interesting developments in the sonic spectrum of late comes in the form of Boze headphones. These are active noise cancellation headphones that listen to the outside noise and other sounds, analyze those wave forms, and compensate for them by generating their own counter waveforms that just cancel out the incoming waveforms at the ear, so that when you wear them the sounds do not get to your ears. On airliners, this dramatically

reduces much of the unpleasant nature of the experience and makes listening to quiet music at high fidelity possible where it was not before.

The technique is so good that the airliners even use it on the engines of their planes in some cases to cancel out the sounds of the engines for the passengers and those on the ground. This produces quieter engines and similar technologies may even reduce turbulence for smoother and less expensive flying.

> Cancellation is limited in electromagnetic systems by the speed of light.

If it works for airplanes, why not use it for meeting rooms? You can, of course, and it works well for the sounds in a proper environment. However, this approach does not work for electromagnetic systems. The reason is really simple. Electromagnetic phenomena happen at the speed of light, and the electronic analysis is impossible to do faster than the speed of light, so the cancellation can never keep up with the signals unless the signals are known in advance. In the sonic world, sound travels at only 300 m/sec, so a lot of calculations can be done between the time a sound wave reaches a sensor at the edge of the headphone and when the same sound wave reaches the speaker inside the headphone a quarter of an inch away. At 300 m/sec, a millimeter is 1/300,000th of a second, while a computer can compute at a rate of billions of computations per second, or perform more than 3000 computations between the microphone and the speaker.

Covert Channels

Most of the spectrum issues discussed end up being important because they create covert channels for information flow. These examples have been accidental covert channels that the defender wishes they could eliminate and the attacker takes advantage of because they happen to be present. But there are a lot of covert channels also available for those who wish to intentionally induce them. All it takes is the ability to plant some hardware or software of your own design within a system, and you can readily create all sorts of covert channels that intentionally use signaling systems to transmit the information accessible by the hardware device to the outside world.

> Covert channels are ways to communicate that are not fully announced and explained to all parties involved.

Any time a resource is shared by parties that should not be allowed to communicate, it can be exploited for communications. When this shared resource is used without explicit notice that it is a communications media

or when the communications method in all of its detail is not specified, there are covert channels — channels that are not overt or announced. These include the electromagnetic spectrum, the sound spectrum, and the signaling protocols and paths used by these spectra to communicate.

In network traffic, covert channels are available even in the most secure of operating systems when the network is shared. These covert channels include all of the variations in valid packet headers, settings, and fragmentations, time to live settings, source ports in sessions, packet timings, packet sequencing, and error responses.

This example points out several of the key issues here. It turns out that in addition to the self-signaling nature of the content passed in the syntax of the communications protocol, all of the variations remaining in the protocol, including all unspecified or underspecified components, are potentially covert channels. If the protocol specifies power in the range of a to b then variations from a to b can be intentionally generated as a covert signaling method. For example, lower power can be used to indicate a "0" and higher power to indicate a "1." Or more values can be encoded in the range from a to b. Similarly, the timing of signals and delay characteristics of responses can be varied. Another example, sending out a response in less than a microsecond for a "0" and more than 2 μsec for a "1." And just like power levels, timing can range over a wider variation for more values to be encoded. The content of packets in a network typically includes a variety of header options and value that can be modified en route and even returned to their original or suitable values later on, so that a pair of devices inside an installation and outside an installation can be used to encode covert information that only runs between the two devices and the intervening infrastructure and does not impact anything at the two ends.

> Steganography intentionally uses the allowed variations in content to encode data. For example, in pictures, minor color changes are not noticeable by the viewer, but can encode large messages surreptitiously.

With a bit of thought, a lot of variations on these themes arise. For example, because an efficient algorithm optimizes operations so that results come as soon as they are available, the same efficient algorithm will produce faster results for some operations when there is a "1" than a "0" bit in any given location in the content being processed. By simply examining timing for operations, covert information about the "1s" and "0s" being processed may be gleaned. This has been used to decode passwords sent in encrypted packets and to break cryptographic systems by figuring out the keys when they are used to encode known content. Responses to login prompts with different timing for valid and invalid user identities and partial passwords have produced similar results. The presence of large numbers of pizza orders

when a military attack is pending is a strong indicator at the Pentagon for the attack to start very soon.

Information Attack Tactics

Many people who discuss information war, in fact, are discussing the subfield that is now commonly called computer network attack (CNA). This is a fairly narrow field that gets a lot of attention in the media, but that is obviously only a small part of the attack space. Many of the people who work in the CNA area do not recognize how CNA fits into the bigger picture of full spectrum information attack and, as a result, they tend to think in terms of single-step attacks rather than sequences of events that produce the desired results. In full spectrum information attack, CNA is used as an element in a larger strategy to gain desired effects. The typical issues in attack include:

- *General approach:* The general approaches most often used include outside in, inside out, and networked or middle out approaches.
- *Direct attack on computers over networks:* This involves sending signals into computers and generating responses. It generally breaks down into distant, proximate, and enveloped methods.
- *Perception management approaches:* These are approaches in which systems or people are given to believe things that result in desired behaviors. This includes elicitations and some sorts of deceptions.
- *Indirect intelligence gathering:* This includes all attempts to gather information on the target without any direct contact with the target. For example, looking them up in the library would be an indirect intelligence effort.
- *Direct intelligence gathering:* This includes direct attempts to gather intelligence on the target by interacting with them. For example, calling up and asking for a catalog.
- *Garbage collection and other physical intelligence:* Generally, waste products are less well cared for than the same material before being put in the waste basket, thus dumpster diving is a popular sport among attackers.
- *Physical entries and appearances:* In many cases, members of the attacking side show up at the target sites and do direct physical attacks to gain entry. This is usually surreptitious in iwar.
- *Trojans and plants:* Via one delivery mechanism or another, Trojan horse hardware and software, planted human operatives, and other corruptions are engaged in.
- *Combinations and sequences:* These things can be combined and sequenced so as to produce desired effects when and where desired.

These are typical combinations used by reasonably sophisticated attackers that are realistic threats to all defenders in the iwar arena. In addition to the mix of techniques, there is generally a pattern of behavior that attackers follow. The pattern is rather simple in its basic form.

- *Gather intelligence:* This involves all efforts to get information on the target that can be exploited either directly for the objectives of the effort or indirectly for gaining those objectives.
- *Gain entry:* This involves getting a foothold somewhere on the path from where you are to where you want to be, either logically via computer entry or physically by getting on the next step of your path to success.
- *Exploit privileges gained:* Entry grants privileges of one form or another. Physical entry may grant visibility, information entry may grant capabilities to alter content, and so forth. Exploitation is gaining desired objectives either for this step of the attack process or for the overall objectives of the effort.
- *Expand privileges:* Using the new capabilities granted by the entry, additional attacks may be attempted to get to new places from the old places.

At every step, previous steps can be augmented and the process occurs simultaneously and recursively over time in the attack.

Approaches and Attack Graphs

Nontrivial attacks are based on the notion of taking multiple steps toward attaining goals. The combination of these sets of steps produces sets of paths from the source of the attacks to the destinations of those attacks. The set of all paths is typically characterized as an *attack graph* and consists of a set of nodes that are logical places in the attack sequences and links between those places that represent different ways of reaching those logical places.

For example, in order to gain the objective of economic advantage over a company, we might want to get the details of what they pay their suppliers and what they charge their customers so we can negotiate better deals with suppliers and undercut their prices. Suppose this demands that we gain ongoing access to their internal bidding content so we can track individual bids that are competitive with ours and that we gain access to what they pay by any of a host of locations where portions of that information resides. We cannot realistically just walk up to the front door and ask for these, and, if we launch an attack on their web site, it is unlikely that we will get the information that we need from there. Rather, we will need a more complex plan that involves gaining access to the desired information at the desired time without the target's knowledge.

> At the extremes, approaches to targets include outside in and inside out. All other approaches are essentially networked approaches in which sets of capabilities are put in place and they interact with each other to provide paths through the attack graph from source to destination.

The outside-in approach is to start attacking at the perimeter and work your way into the core of the parts of the enterprise that have the information you need. From there, the information is then extracted back along the path of entry or through some other means available from there. This might involve an external physical penetration followed by planting a device on their network, which is then remotely exploited via a wireless link to attack internal systems, eventually gaining the desired content and sending it out. The inside-out approach is to start by planting or gaining resources inside the target. For example, if the target is advertising for a sales representative, the attacker can submit a range of resumes under different names and try to plant an intelligence operative in one of the positions. This individual can then use their inside access to get at the system or information desired more directly and find ways to work it back out without getting caught. They might even get on the bidding committee for the work of interest and have access to pricing information as part of the bidding process.

> The middle-out networked approach provides more attack graphs to the attacker while affording redundancy against defenders defeating individual attacks.

The middle out or networked approach is more successful in most cases when there are substantial resources available. In this approach, a set of capabilities are planted against the target and involve whatever can be easily planted wherever it can be planted along with things that are harder to get in, placed in locations where they are critically needed in order to gain the objective. These resources network with each other to form a set of overall attack graphs that provide paths from attacker to target and back. When one fails, alternatives are available, and of course each can be leveraged to add new capabilities.

In most of the efforts we use against corporations, we perform a set of independent demonstrations and posit attackers and capabilities planted in a variety of places with different goals. This is far more effective at understanding the nature of the protection situation within the enterprise and is a far more realistic approach to understanding the protection program and its limits against real attackers than the processes we often see from tool-based solutions.

In studies of actual attacks launched against high-valued targets, we rarely find an example of a successful attacker using a single strategy or a linear approach. Combined attacks are the norm.

Direct Attack on Computers over Networks

Of course, combined attacks involve many individual attacks, and these individual attacks are commonly directed against information infrastructure and endpoint computer systems. In these attacks, we find three different situations.

1. *Distant:* Distant attacks are attacks that come from a location in which the only efforts available are sending information in and awaiting responses through intervening infrastructure. As the attack progresses, more and more proximate and enveloped attacks become feasible for the remote individual, but these are not distant attacks and will not be included here. This includes a wide range of technical attack types including, but not limited to:
   - Call forwarding fakes
   - Content-based attacks
   - Data aggregation
   - Distributed coordinated attacks
   - False updates
   - Illegal value insertion
   - Imperfect daemon exploits
   - Induced stress failures
   - Input overflow
   - Network service and protocol attacks
   - Password guessing
   - Reflexive control attacks
   - Viruses
2. *Proximate:* Proximate attacks are attacks where the attacker and defender or system under attack is in the same position with respect to observing and affecting information. In this environment, both sides can observe and alter information approximately equally leading to the ability of the attacker to passively watch what is going on as well as actively alter states or induce behaviors. There are far more proximate attacks than distant ones because of the strong positional situation. This involves a wide range of techniques including, but not limited to:
   - Cascade failures
   - Collaborative misuse
   - Covert channel induction
   - Data diddling
   - Desychronization and time-based attacks
   - Error-induced misoperation
   - Excess privilege exploitation
   - Infrastructure interference

- Infrastructure observation
- Invalid values on calls
- Multiple error inducement
- Observation in transit
- Privileged program misuse
- Process bypassing
- Replay attacks
- Residual data gathering
- Resource availability manipulation
- Simultaneous access exploitations
- Sympathetic vibration
- Trojan horses
- Undocumented or unknown function exploitation

3. *Enveloped*: In the enveloped situation, inputs and outputs are controllable for some pair of parties or for an individual party. In this case, different attack mechanisms are available in addition to those available from the proximate position. These include, but are not limited to:
   - Audit suppression
   - Backup theft, corruption, or destruction
   - Below-threshold attacks
   - Insertion in transit
   - Man-in-the-middle attacks
   - Modification in transit
   - Piggybacking
   - Spoofing and masquerading

More information on these attack mechanisms can be found in the security database at: www.all.net, my web site.

Information Warfare Defenses

I know that I have given inadequate attention to defenses against iwar attacks along the way through this chapter, and I did not want to leave them out entirely. So the remainder of this chapter is dedicated almost entirely to defenses and how the people of the world can protect themselves from the horrors of iwar.

> There are many defensive methods and approaches and they come in a wide range of areas and types.

Defenses are particularly problematic for a number of reasons, not the least of which is that the uncommonality of objectives means that by defending one side it may actually help the other side. Defense takes resources, so

if one side can cause the other to expend resources on defense, they will gain advantages in efficiency by not having to defend themselves. This means that a good defense will also have an offense that forces the opponents to defend themselves so as to not lose the advantage of inefficiency to the other party. So the successful strategic defense will force the opponents to also defend by including an attack component strong enough to force the other parties to defend as well.

Many of the mechanisms of offense are also viable mechanisms for defense. For example, censorship is used to suppress undesired ideas as part of propaganda, but counter-propaganda also uses the same technique to reduce the amount of information provided by the propagandist.

Defenses can be strategic or tactical, long term or short term, preventive, detective, and reactive, or adaptive. They can address life-cycle issues with businesses, systems, people, or content. They can be in the form of business protections, psychological protections, political mechanisms, or any of a wide range of other things. Defenses, like attacks, are strategies that combine many methods together in a coordinated protective effort.

Technical Defenses

Technical defenses constitute an enormous range of methods designed to deter, prevent, detect, and react to attack and to adapt over time to improve those defenses. The database of defenses at www.all.net includes 140 classes of techniques. For presentation, I will divide technical defenses into four different categories: structure, perception, content, and behavior. These four categories represent only one way of looking at these issues. Generally speaking, these defenses are the mechanisms that come into direct contact with the content or the mechanisms that store, process, or communicate it.

> Creating and operating a set of technical defenses requires a serious effort over a long time and involves a lot of specialized expertise and resources commensurate with the risks being addressed.

Many of these defenses are crosscutting so that they have effects in more than one of the identified areas and beyond the direct contact with content. A lot of controls are directed at people and processes. People controls are discussed throughout this chapter while process controls are used to assure that systematic and repeatable methods are used to increase the chances of things operating as designed. Many of these techniques can be found in the all.net database, and I will only quickly review some of them here.

At the governance level, policy development, the creation of control standards, compliance with laws and regulations, business continuity and

disaster recovery planning, risk acceptance, transfer, avoidance, the integration of multifaceted defenses, the creation and operation of internal controls, fusion of multiple disciplines into a cohesive approach, the timeliness of detection and response, a tracking process for evaluating performance, and a desire to keep things simple all help to build a meaningful program. This governance is necessary in order for protection programs to be effective, and it is best covered in another book of mine titled "*The CISO ToolKit Governance Guidebook*."

Technical Structural Defenses

These defenses generally include mandatory and discretionary access and flow controls, firewalls, and other barrier mechanisms. They are generally associated with the separation of one thing from another so that they do not interact or so that they interact only in well-defined places and ways. This is an appealing approach because there is good reason to believe that separation prevents causes in one area from producing effects in the other. If we can find the proper way to separate things, they will be protected from each other. The techniques include:

- Authorization limitation is used to limit what an authenticated party is authorized to do.
- Automated protection checkers and setters detect and report on deviations from authorization policy and correct them.
- Chinese walls are used to separate functions that must not link.
- Classifying information as to sensitivity is used to bundle information with different properties together for handling in bulk.
- Controlling physical access is used to enforce separation.
- Disconnection of maintenance access prevents its exploitation.
- Drop boxes and processors are used to securely hold content.
- Effective mandatory access control enforces logical separation.
- Faraday boxes prevent electromagnetic information leakage.
- Fault isolation limits the effects of faults to a locality.
- Fine-grained access control allows detailed control over access.
- Fire doors, firewalls, and asbestos suits prevent fire damage.
- Increased or enhanced perimeters increase attack difficulty.
- Independent computer and tool use by auditors prevents internal exploitations from going undetected.
- Independent control of audit information prevents authorized users from corrupting audit trails.
- Information flow controls limit where content can go.
- Isolated subfile-system areas restrict content within file systems.
- Limited sharing restricts what can be shared with whom.

- Limited transitivity prevents giving away received content.
- Lockouts prevent risky actions during maintenance periods.
- Locks are used to prevent access to areas for those without keys.
- Minimizing traffic in work areas prevents exposure to threats.
- Minimizing copies of sensitive information reduces the chances for leakage or damage.
- Multiperson controls limit possibly harmful acts by individuals.
- Multiversion programming prevents single faults from causing systemic failures.
- Path diversity provides redundancy to compensate for faults.
- Periods processing and color changes prevent mixing of content that must be separated.
- Physical switches or shields on equipment limit harm to that equipment from outside sources.
- Placing equipment and supplies out of harms way limits the sources of failure.
- Secure or trusted channels provide assurance that communicating parties are who each thinks the other is.
- Suppression of incomplete, erroneous, or obsolete data prevents its reuse or replay when not appropriate.
- Separation of duties limits the effects of individuals.
- Separation of equipment limits damage from localized events.
- Separation of function limits the functional impacts of faults in any given component.
- Tempest protection prevents waveforms from going where they do not belong.
- Temporary blindness separates systems from each other during periods when trust cannot be reliably established.
- Trunk access restriction limits the exploitation of communications trunks.
- Trusted system technologies provide separation mechanisms with defined levels of surety.
- Waste data destruction provides coverage for the end of the life cycle for content.

These defenses exemplify the range and utility of separation mechanisms for limiting the effects of attacks and accidents on content and its utility.

Technical Perception Defenses

These defenses focus on how content, systems, situations, people, and things are viewed by the different people and systems viewing them. They generally involve understanding how people and systems view of their environment

leads to their behaviors and controlling these views so as to control the behaviors. These defenses include, but are not limited to:

- Accountability creates the impression that what is done is accounted for and things undone or overdone will be found and attributed to the responsible party.
- Awareness of implications provides the means by which individuals can understand the personal and nonpersonal implications of their actions.
- Clear lines of responsibility for protection provide the ability to identify who should do what so that the promise of punishment can be fulfilled.
- Concealed services prevent potential exploiters from determining that exploitable functions are present.
- Deceptions are used in a wide range of ways to induce or suppress signals so that the attacker becomes ineffective.
- Document and information control procedures provide clarity as to who has what so that others can see when someone else does something inappropriate.
- Effective protection mind-set provides the awareness and understanding necessary to allow people to act to protect the interest of the enterprise.
- Feeding false information is a deceptive method that causes others to consume resources wastefully.
- Improved morality increases the likelihood that people will not act in ways that are knowingly harmful to others.
- Individual accountability for all assets and actions links the individual directly to their actions, placing a guarantee that they are aware of, that when they act inappropriately, they will get caught.
- Infrastructure-wide digging hotlines provide information on where not to dig to avoid breaking communication lines.
- Jamming creates the impression that signals are not present or are inaccessible if present.
- Legal agreements provide formal notice of obligations and intent to carry out those obligations with explicit remedies for failure to meet obligations.
- Low building profile reduces the interest in specific facilities and makes their import less obvious to potential attackers.
- Noise injection changes the signal-to-noise ratio so that signals appear not to be present or are hard to identify and gather.
- Numbering and tracking of all sensitive information provides a clear and obvious means for identifying when something is missing, who last had it, and where it is supposed to be.

- Protection of names of resources makes it more difficult to identify what is what and its import or meaning.
- Retaining confidentiality of security status limits the ability of the attacker to determine what may or may not work in what circumstance, and, therefore, what attack mechanisms to apply in which circumstances.
- Security marking and/or labeling provides clearly readable and obvious identification of the sensitivity of content and through association with badges and location, whether the holder should have the content in the particular place.
- Spread spectrum is used to spread the signal over a broader electromagnetic spectrum, thus concealing it within a broader range of waveforms.
- Training and awareness provide the perception of what individuals should do and the ability for them to identify when individuals are doing things they should not be doing.
- Universal use of badges provides identification and marking that associates individuals with access and belonging.

Together, these and other similar methods provide effects on the perception of attackers and defenders that produce behavioral characteristics more likely to result in effective protection.

Technical Content Defenses

These defenses address the meaningful utility of the material being sent, stored, or used. The nature of this challenge implies that such defenses will be imperfect because content without utility has only one legitimate outcome. If there are more legitimate outcomes, then there is no way to tell which of them is correct for the situation. The utility of the content lies in its differentiation between legitimate options. Content defenses include, but are not limited to:

- Change management limits the ability to make changes to approved sets of individuals who go through appropriate processes to verify that those changes are appropriate to the need.
- Authenticated information is used to increase the certainty with which the content can be determined to be as assumed.
- Authentication of packets provides low-level authentication of the source and content of packets of information containing useful content.
- Configuration management is used to identify inappropriate configurations according to technical security policies and to correct those configurations to the appropriate settings.

- Content checking provides independent verification that content is as it is supposed to be.
- Encrypted authentication provides hard to forge verification that content is authentic as to source and not modified in transit or storage.
- Encryption provides concealment of content from those unable to decrypt the content without a proper key and those with proper keys, but not in possession of the proper decryption capabilities.
- Filtering devices are used to remove undesired content from information flows.
- Inspection of incoming and outgoing materials provides assurance that those materials are free from hazards and are suitable and appropriate to their movement.
- Integrity checking provides verification as to source, authenticity, and propriety in context, nonmodification, and reflection of reality.
- Integrity shells are real-time integrity checking mechanisms used to detect alteration between verification and use.
- Known-attack scanning detects known attack mechanisms before they can cause further harm.
- Out-of-range detection detects variations outside of expected values for the context so that they can be investigated further before being trusted.
- Protection of data used in system testing provides for independence of tests and limits the ability of attackers to make alterations that pass tests even though they are inappropriate. It is also used to limit the potential for leakage of content.
- Searches and inspections are used to periodically or upon identification of due cause, do in-depth verifications of the propriety of content.

These sets of defenses provide particular attention to the useful content to assure its utility. None of them are or can be perfect in the sense of assuring that all systems always do the proper things. Rather, they provide a defined level of certainty associated with specific properties of that content within a select context. Unlike structural defenses that have a physics or similar hard scientific basis, content and perception defenses are based on less certain facets and properties of information and are more directly tied to context.

Technical Behavioral Defenses

These defenses work by seeking to understand and differentiate legitimate from illegitimate behaviors. They deal with people and systems and are typically designed to detect and react to events or as overriding controls over behaviors.

- Anomaly detection seeks to detect things that just do not look right according to the normal behavioral patterns of the environment.
- Alarms provide announcements of detected events defined as relevant to the defender.
- Auditing provides reviews of behaviors of systems and individuals to detect deviations from identified legitimate activities.
- Conservative resource allocation allows behaviors of resources to be better predicted and avoids deadlocks and most resources starvation failure modes.
- Detection before failure uses an indications and warnings methodology to identify indicators of failures before they occur and warn of the impending failures in time to mitigate the resulting harm.
- Detection of waste examination is used to determine when someone is trying to use waste products to gain content or intelligence information.
- Disabling unsafe features limits the available features that can be exploited so as to limit the behaviors of the system.
- Least privilege is a sort of behavioral constraint that limits the capabilities or privileges of an individual and the processes acting on their behalf to the minimum privileges required for them to do their work.
- Limited function applies special purpose devices instead of general purpose ones to perform specific functions, thus limiting the potential for exploitations to those functions designed into the mechanisms.
- Misuse detection seeks to identify and report unauthorized or inappropriately applied uses.
- Over-damped protocols are protocols that automatically reduce the quantity of content on each subsequent round of exchange so as to prevent resource exhaustion and expanding loops.
- Properly prioritized resource usage applies mechanisms to assure that more urgent and important things have priority over less urgent and important things.
- Quotas are used to limit the consumption of resources by individuals and groups.
- Redundancy provides a means by which behaviors can be assured even in the presence of failed components.
- Rerouting of attacks is used to prevent attempts at interference from causing interference by handling the attacks in a different part of the infrastructure.
- Secure distribution provides a means by which content can be distributed with increased certainty of arrival in tact and on time.
- Strong change control limits the mechanisms of change so that inappropriate change is harder to undertake.

- Testing provides independent verification that content and systems meet properties defined for them.
- Time or use variant augmented authentication provides increased certainty of authenticity as consequences increase.
- Time, location, function, etc. access limitations limit who, what, where, when, why, and how content can be used.
- Traps temporarily limit activities to localities under tight control.
- Trusted applications provide higher levels of certainty regarding specific properties of their operation.
- Trusted repair teams provide sets of people that are trusted to perform specific repair and maintenance functions.
- Uninterruptible power supplies provide assurance against momentary outages in power or disruption of the normal waveforms of power.

Behavioral defenses range broadly but in the extreme, reach the least certainty of any technical defenses available. As such, the more extreme behavioral defenses are very soft, and yet they also provide the sorts of uncertainties for the attacker that makes them interesting and useful.

Concluding Remarks

Iwar is a broad and complex subject involving many aspects. This chapter has brought out many of the issues in iwar and has put them in context, but it is hardly comprehensive.

To get a sense of what comprehensive coverage might look like, consider that every page of this chapter could easily be the overview of a 500-page book on the more limited subject and still not definitively cover the subject matter. People study warfare for their entire lives and never fully understand it and researchers work on subfields for whole careers without completing even the work in that subfield. And yet, the great classics of the field, such as Sun Tzu and Dewar,[2] summarize it all in a few pages.

This is the nature of conflict. It is simple at its heart. But try to settle the conflict between Israel and its neighbors and you could spend a lifetime making relatively little progress. That war now lasting more than 60 years is indeed a tremendous example of an information war. It is full of propaganda, and the violence increases and decreases with time, but the underlying information war goes on. When it is hot, it ranges from advanced electronic targeting systems to cyber attacks, and cell phone locations are used to target enemy leaders who are then bombed from above with "smart" bombs. Deception is commonplace, and people on all sides use every skill they have in the information arena. It is simple at its heart, and yet try to capture it and you

get swamped in complexity. Hopefully, this chapter has shed more light than it has introduced chaff.

References

1. This chapter is summarized from extracts of "*World War 3: We are losing it and most of us didn't even know we were fighting in it* — Information Warfare Basics," (ASP Press, 2006). With permission.
2. Dewar, M., *The Art of Deception in Warfare*, David and Charles Military Books, 1989.

Section III

National Security Strategy: Implications for Science, Law, and Technology

9 Geographic Information Systems as a Strategic Tool for Better Planning, Response, and Recovery

LUCY SAVITZ, ROBERTA P. LAVIN, AND ELISABETH ROOT

Contents

Objective

The objective of this chapter is to underscore the strategic contribution of effective cartography and map interpretation in national disaster planning, response, and recovery efforts for the support of civil defense. We use the events of Hurricane Katrina and repurposing of research databases prepared as part of a project funded by the Agency for Healthcare Research and Quality (AHRQ) to demonstrate how maps generated from a geographic information system (GIS) can support monitoring and decision making during a disaster. This illustration is given context by first reviewing how disasters are currently managed at the federal level.

Managing a Disaster at the Federal Level

The Department of Homeland Security (DHS) became an official department on March 1, 2002 as required by the Homeland Security Act of 2002. The mission of the Department was to "(a) prevent terrorist attacks within the United States, (b) reduce the vulnerability of the United States to terrorism, (c) minimize the damage and assist in the recovery from terrorist attacks that do occur within the United States, (d) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning …" (Homeland Security Act, 2002). The implementation resulted in the reorganization of portions of 22 departments and agencies, including, personnel, equipment, and functions into the DHS. Consequently, it was necessary to revise both the Federal Response Plan (FRP), hereafter referred to by its' current title, the National Response Plan (NRP), and the Incident Command System, hereafter referred to by its' current title, the National Incident Management System (NIMS).

One might speculate as to how emergency management functions became so decentralized. When President Harry Truman established the Federal Civil Defense Administration (FCDA) in 1950, the expressed purpose was to monitor emergencies and not to manage emergencies that were considered the responsibilities of state and local governments (Tennessee Emergency Management Agency, 2002; Blanchard, 1985). As directed in the Federal Civil Defense Act of 1950, the responsibility for the civil defense was to be the responsibility of "several States and their political subdivisions," which lead to a "fuzziness" of who was responsible for what (Boykin, 1951) and concern about the quality of the products produced (Blanchard, 1985). Over the next 60 years, portions of the coordination of, and response to, emergencies were transferred from the Office of the President to the Office of Science and Technology Policy within the Executive Office of the President to the General Services Administration to Housing and Urban Development (while the Defense Department maintained the civil defense portions) to the Department of Commerce to the Federal Emergency Management Agency (FEMA) in 1979. President Carter's intent when establishing FEMA was to again centralize control in one agency and, thus, have a more streamlined and coordinated response.

Following the establishment of FEMA, work began on models of command and control. Multiple concepts were explored before the final development of the Federal Response Plan and the Incident Command System in response to work initiated by the National Governors' Association. These systems stood the test of time and were the basis of the current all-hazards approach to emergency planning within the U.S. They were considered fully adequate for most purposes until the events of September 11, 2001. Though

the intention when FEMA was established was, "coordinating federal efforts with state and local efforts" and to be the "lead federal agency for the national emergency management system," the system again became decentralized as departments responded to FEMA's inability to respond in a timely manner by building their own capabilities (Waugh, 2000, p. 28). Congress, who continued to provide line item funding for various departments, further exacerbated this decentralization.

After the events of September 11, 2001, multiple members of Congress and the president called for a more centralized coordinating body that could bring together not only response assets, but intelligence assets as well. The result was the passage of the Homeland Security Act of 2002, which established the DHS and, thus, combined many aspects involving national security, including border security, intelligence, research, and disaster response.

As a result of bringing portions of 22 departments and agencies together in one department and moving a vast quantity of assets, it was clear that the FRP would need to be revised to encompass the organizational and legislative changes that occurred. Portions of Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 were modified and would require additional changes to be considered in the FRP.

Starting points. The FRP was first drafted in 1992 as a provision of the Stafford Act. The Stafford Act gave the president the authority to provide financial and other assistance to state and local governments, nonprofit organizations, and individuals after a presidential-declared disaster. The FRP "lays out the manner in which the federal government responds to domestic situations in which the president has declared an emergency requiring federal disaster assistance" (Government Accounting Office, 2001, p. 28). Under the FRP, the Department of Health and Human Services (HHS) is the lead federal agency for Emergency Support Function 8 (ESF-8). As such, HHS is responsible for providing medical and public health assistance when a major disaster is declared and ESF-8 is activated. When terrorism is involved, Presidential Decision Directive (PDD) 39 declares the Federal Bureau of Investigations as the overall lead and PDD 62 clarifies the roles of many other agencies.

Supporting the FRP, the incident command system is "a model tool for command, control, and coordination of a response and provides a means to coordinate the efforts of individual agencies as they work toward the common goal of stabilizing the incident and protecting life, property, and the environment"(Federal Emergency Management Agency, 1999, pp. 1–2). Designed in the wake of devastating wildfires in 1970, the system was meant to address serious weaknesses in a response including: (1) lack of a common organization, (2) poor on-scene and interagency communications, (3) inadequate joint planning, (4) lack of valid and timely intelligence, (5) inadequate resource management, and (6) limited prediction capability (Auf der Heide,

1989). Two significant goals of the ICS system are that it is scalable from daily incidents to major disasters and that it be simple. One of its primary principles is the use of common language so that it is understandable to all involved in a response.

On February 28, 2003, President George W. Bush signed Homeland Security Presidential Directive 5 which was "to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system." Specifically, this policy was the initial guidance:

> To prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management. The objective of the United States Government is to ensure that all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management. In these efforts, with regard to domestic incidents, the United States Government treats crisis management and consequence management as a single, integrated function, rather than as two separate functions (HSPD-5, 2003, p. 1).

HSPD-5 mandated the development of the NRP, which replaced the Federal Response Plan.

Agency coordination. The NRP established "interagency and multijurisdictional mechanisms for Federal Government involvement in, and DHS coordination or, domestic incident management operations" (NRP, 2004, p. 3). The NRP is divided into four basic sections: (1) the base plan, (2) appendixes, (3) support annexes, and (4) the ESF, which provides details on responsibilities of federal agencies in coordinating a response.

ESF-8 addresses public health and medical services and is coordinated by the HHS as the primary agency. ESF-8 is available at www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf. As the primary agency, HHS "coordinates the provision of Federal health and medical assistance to fulfill the requirements identified by the affected state local, and tribal authorities" (NRP, 2004, ESF#8-2). ESF-8 assists in meeting "the public health and medical needs of victims of an Incident of National Significance" through assessment of the public health and medical needs, public health surveillance, medical personnel, equipment, and supplies (NRP, 2004, ESF #8-1). This responsibility is carried out in coordination with other federal agencies, state and local governments, and the private sector.

Data Needs

Disaster coordinators, researchers, and public health experts who conduct rapid needs assessments face difficulties in defining required data. Natural disasters, for example, are not predictable, and there are rarely more than a few days warning of an impending event. Time does not allow for testing and retesting of tools or analysis of definitions and measures. The nature of the event requires a rapid and timely response. Subject matter experts indicate that rapid needs assessments following floods or hurricanes should occur within 7 days of the disaster. This leaves little time for refining the processes. The uniqueness of each disaster further complicates coordination and research. Populations, socioeconomic status, healthcare availability, and environmental conditions are different in every community and, thus, the data needs may be different in every community. Moreover, data needs for critical infrastructure need to be addressed and collected in advance of an incident. Tracking down necessary information during a disaster is impractical and unreliable. Further, it is difficult to assess the status of infrastructure when no full assessment existed in advance of massive destruction.

It is important to adequately define data terms prior to collecting information. Waring et al. (2005) defined health needs as "households reporting at least one person needing pharmacy or medical attention" (p. 113) and did not include in the definition a need for counseling and special needs that is in the *Community Study: Rapid community needs assessment using modified cluster sampling methods* (CDC, 2003) and also did not include the healthcare infrastructure as in the *Rapid Assessment Format* (United Nations Development Program). Additionally, Malilay et al. (1996) indicated that the rapid needs assessment "may include environmental sampling to determine health outcomes and possible toxic exposures" (p. 403). It is also important to know if other factors have an effect on illness, injury, and healthcare needs other than those precipitated by the primary disaster event. Further complicating findings is the general lack of information on previously existing levels of illness, injury, or health needs per household in impacted areas.

Critical Infrastructure Data System

The issues addressed above indicate a need for standardized definitions and data elements that are collected prior to and during a disaster. From a very simplistic perspective, it is crucial to know what makes up the public health and healthcare infrastructure, what pieces of the infrastructure are critical, and where the infrastructure is located. Having this minimal dataset then allows the possibility to determine what elements of the critical infrastructure

were impacted by the disaster and what the operational status is of those elements.

Anyone who has ever tried to coordinate a disaster will realize why an up-to-date minimum dataset is essential. During a crisis, chaos is the norm. A crisis is both an "emotional reaction to a hazardous event" and an opportunity for growth (Infante, 1982, p. 11). It is logical that it is better to prevent a crisis than to respond to one once it has occurred, but like most complex issues in society, a disaster is typically not an either/or proposition. It is imperative that communities not only be prepared for and make efforts to prevent a crisis, but also have a response system in place in the event that the worst-case scenario does occur. The ability to focus one's efforts in a manner that will heed the best possible results can be enhanced by utilizing a standard approach to predefining the critical infrastructure and mapping the elements. Likewise, recognizing that moral, economic, social, and political values influence the decision making in regard to any scarce resource is critical to analyzing the criteria for inclusion and exclusion of specific resources. To answer the question of what values are evident, one must first identify the alternatives that are available or the choices one must make. The identification and inclusion of essential elements into a single database or critical infrastructure data system (CIDS) is then an essential first step.

Proposed elements for inclusion include:

- Pharmaceutical and biotechnology
- Medical supply chain
- Laboratories
- Fixed medical facilities (hospitals, nursing homes, etc.)
- Deployable medical units (NDMS, USPHS, Medical Reserve Corps)
- Workforce
- Medical research and academic health facilities
- Health information and medical technology
- Occupational health
- Public health
- Mortuaries
- Insurers and payers
- Blood banks

It is essential that the CIDS include data elements with standardized field's specifications that are compatible across local/regional systems. Consideration must also be given to how the data will be displayed. In the next section, we describe how GIS can be used as a strategic tool to support management of a disaster, which is followed by a discussion of what is needed to produce cartographic or map displays that translate these data into useful information.

GIS as a Strategic Tool

GIS essentially joins cartography, spatial statistical analysis, and the computer to create the opportunity for effective analysis of a complex variety of geographically referenced data (Ricketts et al., 1994). Many GIS software programs are available for personal computers (PC) and larger machines. The ready availability of inexpensive and powerful PC-based systems has made this technology accessible for both trained and untrained users.

GIS technology allows users to examine patterns and relationships in data through a process that includes input, storage, retrieval, manipulation, analysis, and output (i.e., maps, charts, and reports) of synthesized data (Twigg, 1990). This definition is further extended by (Cowen, 1990), whereby GIS can be viewed as "… a decision support system involving the integration of spatially referenced data in a problem solving environment (p. 54)."

GIS has become a central tool for geography-based planning, response, and recovery by government agencies involved in criminal justice and public health at all levels, policymakers, and researchers. GIS can expeditiously convey visual displays of information that simultaneously synthesizes and relates multiple layers of critical information — raster imagery, structures, land use, geopolitical boundaries, transportation routes, disaster attributes, etc. The capacity to rapidly transform such disparate data into usable information is an important advantage for planning, response, and recovery. Examples of this utility include (ESRI Homeland Security Team, 2005):

- *Planning* — Identification of vulnerabilities and/or potential targets (e.g., office buildings, stadiums) that could be selected for security checks, surveillance, gate controls, etc.
- *Response* — Locating available staging areas, triage sites, helicopter landing zones, and/or viable evacuation routes
- Recovery — Monitoring and modeling return to service and repopulation of impacted area

The primary output that facilitates these applications are maps.

Displaying GIS Data with Maps

Maps provide a high-utility GIS output. An important feature of maps is the ability to overlay multiple layers of data, synthesizing information into a comparative visual display. Geographic analysis is a specialty discipline that has been honed over time, applied rigorously to disease diffusion and spatial location of resources, and most recently upgraded through computer technology (Ricketts et al., 1994; Joseph and Phillips, 1984; Meade et al., 1988). Below we describe key considerations in producing map outputs.

Map style. Choroplethic maps are most commonly used; these are maps in which geographic units (e.g., counties) are shaded to represent different values of a variable. When the data are continuous in nature (e.g., percentage or ratio), data values are grouped into several ranges or classes. The legends located on each map page indicate the range of data values that each color represents. These maps are useful when data have been scaled or normalized in some way. When data are nominal in nature, data values are grouped into discrete categories and a different color is assigned to each category.

Titles, legends, captions. Most map titles list the geographic references (e.g., state name) and the theme of the map. Legend captions provide a more detailed explanation of the data displayed on the map.

Classes. There are many different methods for deciding class breaks, or data ranges, for choroplethic maps. For example, natural breaks use logical breaks, or clustering, in the data to group data values into classes.

Color. Color assists the reader in understanding the data and should reflect the subject matter of the map as well as the values of the data. The appropriate use of color is important because it reduces the chances of seeing patterns that do not exist or missing patterns that do. Brewer (1994) prepared a set of color schemes that were developed to be accessible to individuals who are colorblind and can be photocopied in black and white without loosing contrast. These color schemes can be accessed through a web-based application called ColorBrewer at www.colorbrewer.org. On many of the maps, colors are arranged from dark to light, with dark colors representing high values and light colors representing low values.

Symbols and shading. Occasionally, areas on a map are hatched or symbolized by diagonal lines. The addition of hatched lines, icons, graded circles, and/or shading is used to convey an additional piece of information, such as the presence of a physical feature, population density, and/or land use.

In the next section, we discuss how GIS and map displays can be used. This is done using recent experience during disaster response and relief in the aftermath of Hurricane Katrina.

Real-Time Application of Health Services Research in Disaster Recovery

Most healthcare preparedness planning efforts have been focused on hospital and first responder preparedness. For bioterrorism and other public health emergencies, the elderly population is particularly vulnerable. The potential role and question of preparedness on the part of nursing homes emerged in local and national preparedness discussions, but very little information existed on the extent to which nursing homes had planned for and/or been incorporated into regional planning efforts prior to Hurricane Katrina

and Hurricane Rita. The reported project sought to better understand the role that nursing homes could and should play with respect to regional preparedness by examining the current status of disaster planning and response readiness, elasticity of staff and licensed beds, space availability, and special needs. A cross-sectional study using GIS drew on a series of secondary datasets to assess nursing home location and capacity for the entire U.S. from an ecological perspective.

An essential component of Exploring the Special Needs and Potential Role of Nursing Homes in Surge Capacity for Bioterrorism and Other Public Health Emergencies (Phillips, 2003) was a GIS-based analysis of key variables and geopolitical boundaries together with hospital and nursing home facility locations in all 50 states and the District of Columbia. The map series is presented in atlas format in order to stimulate local/regional planning discussions.

As Hurricane Katrina swept the Gulf Coast and left a path of tragedy in 2005, relief efforts required visual displays and daily report updates on the status of healthcare facilities in the impacted areas. Health services researchers from RTI International were able to support HHS Secretary Mike Leavitt's Command Center as part of the CIDS by repurposing GIS files used in the AHRQ-funded study. It was necessary to expand (for hospitals and nursing homes) and create (for community health centers and shelters) data layers related to healthcare facility locations in the midst of the recovery chaos. Both static and updated, dynamic maps were created to monitor operational status and relative location of shelters, community health centers, hospitals, and nursing homes in relation to the flooded areas to support decision makers in their recovery and relief efforts as part of the CIDS reporting effort.

CIDS reports were initially generated on a daily basis, and every other day and then weekly toward the end of the event period. Inputs came from several agency and field sources that were updated real time and integrated with static data layers to reflect the most recent data available. The data required some reformatting, manipulation, and conversion to new file formats for these purposes. The following data files and corresponding maps were received/produced each time.

- Operational status of healthcare facilities by state
- Operational status of individual hospitals
- Operational status of individual emergency departments
- Staffing and needs at Federal Medical Shelters (FMS).

The map layouts were saved in ArcGIS mxd files and were reused for each day's maps. Only the underlying data were changed. Maps were provided together with a set of charts to support monitoring activities and decision making. A brief synopsis was created by the GIS analyst that summarized the

key findings and/or changes within the updated maps. This work required that a GIS staff member be available 7 days a week. In order to speed the CIDS report generation and spread the work around, a team of trained GIS staff members was assembled.

Lessons Learned

How data elements are defined, the source of the data, the specific questions asked, and how this information is then displayed all influence the findings. Disparities in the quality, data field standards, comprehensiveness, and timeliness of existing GIS systems maintained at local, state, and federal levels were reported in a 2003 survey by Public Technology, Inc. (ESRI Homeland Security Team, 2005). The ability to merge such data is, thus, compromised even when data sharing agreements are in place. GIS databases are typically populated with estimates and projections from census data, which may not have been accurate or are outdated; further, outdated and/or repurposed structure location information may be used. There are lags of varying duration for any major secondary dataset. In the Hurricane Katrina response example, we used year-old American Hospital Association (AHA) data to spatially locate hospital facilities in the impacted area; the problem is that not all hospitals participate in the AHA Annual Survey (i.e., the source of this information) such that we were missing key facilities in our database and had to fill in these data under extreme duress. Identifying key data needs and data sharing agreements among agency/organizational stakeholders in advance (i.e., HRSA, SAMSA, CMS, and other government agencies as well as state hospital associations, state nursing home associations, American Red Cross, etc.) would have sped the reporting process and minimized confusion and spotty reporting during critical periods in recovery and relief efforts.

Further, a significant problem with GIS is that the data layers are not always based on standardized data sets. In other words, data available on health needs prior to the disaster may be based on counties or ZIP codes, whereas population data may be based on census tracks. The definitions, unless specifically addressed, may not match the definitions used during the rapid needs assessment. We know that some data will be provided from the field on a real-time basis and need to be integrated. Standards for data submission with a unique identifier should be stored in the system. To ensure that facilities are properly located to begin with, facilities (including temporary shelters) should be asked to identify their full address (i.e., street address, city, state, ZIP code, and county name) together with the nearest major crossroads. This will enhance proper geocoding so that the data can be linked back to the GIS.

Lastly, untrained GIS users may not understand the implications of color or symbol choice, spatial relationships, spatial statistics, and display options

that are important for effective use of map displays. Anselin (2006) warns that "… care is needed in the range of activities involved in spatial data analysis, from the collection of data and the use of software to the interpretation of results and their application (p. S3)." Trained GIS analysts as part of a team that includes domain experts (i.e., public health, healthcare, emergency response, etc.) allows for guiding how relevant questions are framed so that the best possible information can be provided.

These lessons learned are not necessarily new information; however, reported in this way they serve as a guide for improvements in readiness. We draw on our collective experience to make recommendations that will enhance the application of GIS for future disaster planning, response, and recovery efforts.

Recommendations

The utilization of GIS to map health needs and critical infrastructure in disaster situations is a good example of the difficulties as well as the necessities of definitions for the data elements. For effective GIS support, our experience underscores the need to ensure that:

1. A minimum dataset is specified
2. Standards for required data elements and associated field specification are provided
3. Databases are updated and maintained on a regular basis
4. Mutual data sharing and reporting agreements are in place to support enterprise database development via database integration
5. Trained staff is available to support GIS-based analyses and the production of informational displays

These measures will ensure that geographic data usable for civil defense in the case of emergency response to terrorism, manmade disaster, and/or natural disaster are available to support planning and decision making.

Meeting future needs for flexible, dynamic access to spatial data for the creation of situation reports and maps is recommended. A web-based solution would offer more effective, efficient, widespread (more people could easily generate the maps they need), and timely graphical displays to support preparedness planning, relief, and response. A functional GIS system with a CIDS-specific enterprise database would include a web-map server to provide interactive maps to standard web browsers and a map publisher technology to make it easy for the development and printing of high-quality dynamic maps. A mapping system that provides an easy-to-use interface, the ability to produce high quality maps, and the ability to access dynamically changing

data could then be implemented in several ways depending on the specific needs and existing technology. Such a GIS that supports both web-based query and display of maps in a web browser and supports the production of high-quality printed maps is both ideal and possible.

Lastly, proactive consensus building and expert/experience-based input should be solicited with regard to how best to provide feedback to sites, feedback to participating agencies/organizations, and expanded reporting capabilities. This process should focus on knowledge gathering and produce actionable items and tools to support future relief/recovery efforts by the Secretary's Office of the U.S. Department of Health and Human Services. An example action might be to preapprove data gathering forms and establish interagency and organization agreements for data sharing.

References

Anselin, L. (2006). How not to lie with spatial statistics, *Am. J. Prevent. Med.*, 30 (2S), S3–S4.

Auf der Heide, E. (1989). *Disaster Response: Principles of Preparation and Coordination*, C.V. Mosby Publishing, St. Louis, MO.

Blanchard, B. (1985) American civil defense 1945–1984; The evolution of programs and policies. Monograph Series (2) 2. Nation Emergency Center, Emitsburg, M.D.

Brewer, C.A. (1994). Color use guidelines for mapping and visualization, in *Visualization in Modern Cartography*, MacEachren, A.M. and Taylor, D.R.F., Eds., Pergamon Press, Oxford, pp. 123–147.

Boykin, L. (November 8, 1951) Office Memorandum: National civil defense plan, retrieved from the National Archives.

CDC (2003) Mass casualties/community study: Rapid community needs assessment using modified cluster sampling methods. May 16, 2003, www.bt.cdc.gov/masscasualties/research/community.asp

CDC (2006). Public health response to hurricanes Katrina and Rita — Louisiana, 2005, *MMWR*, 55 (02), 29–30, http://www.cdc.gov/numwr/preview/mmwrhtml/ mm5502a1.htm?s_cid=mm5502a1_e (accessed January 19, 2006).

Cowen, D.J. (1990). GIS versus CAD versus DBMS: what are the differences? *Introductory Readings in Geographic Information Systems*, Peuquet, D.J. and Marble, D.F., Eds., Taylor & Francis, London, pp. 52–61.

ESRI Homeland Security Team (2005). *GIS for Homeland Security,* ESRI Press, Redlands, CA.

Federal Emergency Management Agency (1999). Incident Command System: Independent Study Course, www.fema.gov (retrieved January 9, 2002).

Government Accounting Office (2001). Bioterrorism: Federal Research and Preparedness Activities, GAO Publication No. GAO-01-915, U.S. Government Printing Office, Washington, D.C.

Homeland Security Act (2002). H.R. 5005, 107th Cong.

Homeland Security Presidential Directive 5 White House (2003). http://www.whitehouse.gov/news/releases/2003/02/print/20030228-9.html (accessed November 29, 2003).

Infante, M.S. (Ed.) (1982). *Crisis Theory: A Framework for Nursing Practice.* Reston Publishing Company, Reston, VA.

Joseph, A.E. and Phillips, D.R. (1984). *Accessibility and Utilization, Geographical Perspectives on Health Care Delivery*, Harper & Row, New York.

Malilay, J., Flanders, W.D., Brogan, D. A modified cluster-sampling method for post-disaster rapid assessment of needs. Bull World Health Organ. 74 (4), 399–405, 1996.

Meade, M.S., Florin, J.W., and Gesler, W.M. (1988). *Medical Geography*, The Guilford Press, New York.

National Response Plan, December 2004. (PDF) www.iir.com/global/fusioncenter/NRPbaseplan.pdf

Phillips, S. *AHRQ IDSRN* Contract # 290-00-0018, Task 11, 2003.

Ricketts, T.C., Savitz, L.A., Gesler, W.M., and Osborne, D.N. (Eds.) (1994). *Geographic Methods for Health Services Research*, University Press of America, Lanham, MD.

Tennessee Emergency Management Agency (2002). The History of Civil Defense and Emergency Management in Tennessee, http://www.tnema.org/Archives/EMHistory/TNCDHist1.htm (accessed November 27, 2002).

Twigg, L. (1990). Health-based geographical information systems: their potential examined in the light of existing data sources, *Soc. Sci. Med.*, 30 (1), 143–155.

Waring, S., Zakos-Feliberti, A., Wood, R., Stone, M., Padgett, P., Arafat, R. The utility of geographic information systems (GIS) in rapid epidemiological assessments following weather-related disasters. *International Journal of Hygiene and Environmental Health*. 208, (1–2), April 8, 2005, 109–116.

Waugh, W. (2000). *Living with Hazards Dealing with Disasters: An Introduction to Emergency Management*, M.E. Sharpe, New York.

An Introduction to the Concept and Management of Risk

10

JAMES O. MATSCHULAT

Contents

> I have seen something else under the sun:
>
> The race is not only to the swift
> Or the battle to the strong
> Nor does food come to the wise
> Or wealth to the brilliant
> Or favor to the learned;
> But time and chance happen to them all
>
> **Ecclesiastes 9:11**[1]

Everyone is challenged by the vagaries of time and chance, so we are all risk managers. To help gain a better understanding of these universal dimensions of life, this chapter provides a basic introduction to the concept and the management of risk. As national security professionals, it is important to be familiar with risks of all types and with effective strategies for managing risk. This topic is particularly relevant today because we appear to be entering an age of increasing risk and uncertainty. Hardly a day passes without the emergence of some new threat or catastrophe at the center of our daily flow of news. But, do we really face as dark a future as the news reports imply or are they "false alarms?"

From avian flu to global warming, from reports of melting ice caps to threats of terrorism, we are awash in cautionary views. Does this mean that the level of risk we face really is rising? After all, alarmist "yellow journalism" has a storied history. Consider the following:

> Rival New York newspaper owners William Randolph Hearst and Joseph Pulitzer are reputed to have started the practice of using blatant exaggeration and hyperbole to sell newspapers in a media war in the 1890s. Hearst, some historians claim, even played a role in helping to instigate the Spanish-American War by running a story that blamed the Cuban government, without evidence, for the sinking of the ship Maine in Havana Harbor in 1898.[2]

On the other hand, we still face all of the native risks humanity has faced over time: earthquakes, floods, fire, hurricanes, tornadoes, volcanic eruptions, and the like as well as terror, war, and famine. And, in addition, it seems that science is increasing the list of threats both directly by creating new pathogens, poisons, and weapons and indirectly by exposing humanity to unknown effects from risky experiments. Even more ominously, science is exposing humanity to the threat of bioerror and unintended consequences from experiments with new forms of life. So, perhaps, we really are in an age of increasing risk and uncertainty. And if so, how should our situation be interpreted and appropriately managed?

Since the beginning of human time, people have coped with risk. As survivors, we have a long heritage of success as we have struggled over the

ages with the unknown, uncertain dangers present in living from day to day. Everything we attempt takes place in an uncertain future — a future we cannot know. Once more, as we make choices that will play out in that unknowable future, we face a dual uncertainty. Not only do we not know what lies ahead, we also do not know how we will feel about the future we envisioned when it arrives. So, it is part of normal human experience to guess, choose, plan, hope, regret, and rejoice, all in a fog of uncertainty in anticipation and in reaction to streams of seemingly random events.

To cope, we invent myths, engage in trial and error activities, and think about and reflect on the patterns we encounter. We then adopt behaviors and approaches that appear successful and celebrate them as proven successes, at least until they fail. By accumulating knowledge in this way, we learn about the world around us and importantly, the risks we confront. The scientific method has served as an effective way to accumulate human experience and advance our understanding of why things are as they appear to be. Conceptual frameworks infused with discovery are extremely useful for creating meaning out of the way we experience the world around us. Frameworks or paradigms help us move in a factual way from myth toward meaning and permit purposeful interventions that can promote the odds of successful outcomes.

The Challenge to National Security Professionals

It is in this uncertain environment of immutable past and unknowable future, that the national security professional is challenged to establish and ensure an enduring public confidence. But, how much safety and security is needed? Who should decide? How should these questions be answered?

While we cannot be guaranteed a safe and secure existence, we expect our national security enterprise to practice effective risk management. Just as in private sector businesses, it is useful to think of "purpose" in terms of creating and retaining customers rather than simply making money, the national security enterprise should not regard safety and security as ends. They are necessary but insufficient conditions for living a free and purposeful life where scarce resources are allocated as far as practicable to productive rather than simply protective activities.

Further, at our present level of environmental knowledge and understanding we still cannot predict, let alone prevent most natural catastrophes. Also, we have not learned to prevent inflation, unemployment, many deadly diseases, war, discrimination, terrorism, and a host of other existing and emerging events that stalk a healthy, safe, and secure existence.

So, what should a conscientious national security professional do? Despite the grim realities of life, we strive to survive. Indeed, survival is our heritage and hopefully our legacy. We look to our national security corps to thoughtfully and effectively prevent loss and protect our lives and property

notwithstanding the vagaries of the threats we face from weapons of mass destruction to natural catastrophes of mass disruption. What approaches to risk management have been most helpful in the past? What lessons can we learn from great leaders? From Hammurabi "The Protector," king of ancient Babylon (c.1780 BCE) to Winston Churchill during the Battle of Britain during World War II, examples abound. But what can we learn from them that would be of use today?

The answer, despite our natural human tendency to "muddle through," can be found in the application of a rational action model for managing risk. By following a sequence of seven logical steps for recognizing and resolving risk, the national security professional can begin to effectively assess the risks to our collective health, safety, and security and begin to effectively manage them. The seven steps are:

1. Imagine
2. Describe
3. Observe
4. Measure
5. Map and Model
6. Prevent
7. Mitigate

The first five steps in the risk management sequence (RMS) are focused on recognizing risk at increasing levels of understanding. They involve knowing all we can about a risk. The last two are concerned with efficiently coping with and resolving the recognized risks. Taken as a whole, the RMS involves doing all we can about a risk. While every national security professional's tool box should include the RMS as a way of striving for deep understanding of risk and its effective management, the RMS model prescribes rational actions that are ideal, and, therefore, it is not a definitive description of the way risk management actually happens. Our limited understanding of the world around us and the human tendency to press on despite the odds inhibit the comprehensive application of the RMS. Nevertheless, application of the sequence should produce both economic and psychological benefits and, in turn, result in an increased level of public confidence in the government or organization that applies it effectively.

The catastrophic terrorist attacks on September 11, 2001 in the U.S. were widely regarded as a failure of imagination and a failure to understand the available facts and circumstances the U.S. faced. These failures resulted in an inability to prevent and protect the public and produced a significant erosion of public confidence in government effectiveness.

Similarly, the catastrophic aftermath of hurricane Katrina in August 2005 resulted from a wide-spread failure of government at all levels to sensibly

evacuate every citizen and mitigate the effects of this predictable but unpreventable event. These failures resulted in an inability to mitigate the tragic effects of the storm and also produced a significant erosion of public confidence in governmental effectiveness.

A careful application of the RMS will produce a deep understanding of risk and will help prevent unpleasant surprises, as well as provide risk managers with the opportunity for the effective allocation of resources to resolve risks of loss.

For example, private sector contemporary strategic managers in high performance organizations articulate this concept with the adage: "What you measure, you get." The idea here is that understanding a strategy at a level that permits multidimensional performance measurement augers well for successful strategic outcomes. The same is true for risk management. The better able we are to understand and actually measure, map, and model risk, the better able we will be to manage it. Thus, the keystone of effective risk management is a complete understanding of risk. But what is risk and how should it be managed?

Risk Defined as Either "Speculative" or "Pure"

It is with these questions and in this context that we begin our conversation about the concept and nature of risk. Risk has many definitions, but a useful place to start is with the Oxford English Dictionary, which defines risk as "hazard, danger; exposure to mischance or peril"[3] and expressed as a verb, "to hazard, endanger; to expose to the chance of injury or loss." The definition of risk has long been the subject of interesting debates and discussions among scholars from various disciplines, including economists, psychologists, historians, actuaries, and others. From an operational, practical, day-to-day perspective, it is adequate to simply remember that risk involves both "chance" and its counterpart, "mischance."

Of course, not every risk is bad. Risk, like beauty is in the eye of the beholder. So, there is an important psychological dimension to risk. In fact, gambling and games of chance that create risk are one of the fastest growing forms of entertainment. Unfortunately, they are also a rapidly growing source of addiction. Your eager, thrilling decent down a sheer "blue diamond" ski slope could be my worst nightmare. A shear terror! So, there are many types of risk. The most useful typology is provided by Albert Mowbray and Ralph Blanchard.[4] They identify two very different types of risk. They make a meaningful distinction between risks that present the possibility of a gain or the possibility of a loss and risks that only can result in loss or no loss. The former they term "speculative" risks. The latter are labeled "pure" risk. Pure risks are the subject of this chapter.

Building on this distinction between the two main types of risk, we can move on to a definition of pure risk. Pure risk can be most usefully defined as "chance of loss."[5] This definition, in turn, is built upon two logics or systems of inquiry or inference that can help us understand, at least to some degree, the risks in the world around us. As formal science and casual human experience accumulates facts about the dangers we face in our lives, these facts and understandings can be interpreted and put to practical use with the help of two logics or systems of inference and description. They are the logic of chance and the logic of loss.

The Logic of Chance

The logic of chance addresses the relative frequency dimension of risk. Since more things can happen than will happen, this logic provides answers or clues to help us investigate or systematically inquire about the chance that a loss will occur — and perhaps, even determine the relative frequency with which a loss may occur. The answers to these questions can be investigated with the help of *probability theory*.[6] The main idea here is that risk or the chance of loss can, in some practical operational sense, be measured and, therefore, in some practical way managed with the assistance of the theory of probability.

Probability Theory

As the logic of chance is closely aligned with the theory of probability, it is at its core about counting or estimating the likely relative frequency of events that have happened in the past and could happen again in the future. When we make a probability statement we mean that if an event is certain to happen, it has a 100% chance of occurring. If the event is impossible, we assign a zero probability to the outcome in question.

Probability can be displayed and represented on an imaginary yardstick. If the odds of the event are zero, the chances of the event happening are at the beginning of the yardstick. If we are certain that an event will occur, the event will be shown at the end of the yardstick. If the odds are even, the events chances will be shown at the middle of the yardstick and so on. The yardstick is a continuum, so possible or plausible events can be shown to lie at any point along the yardstick, depending on the odds.

Probabilities can be *objectively* derived, in accordance with the mathematical laws of probability. The counting required to derive these odds is, however, not always possible as the data may be unavailable because it is unobtainable or simply unknown. Tossing a fair die is one thing. Calculating the odds of a safe shuttle launch or a collision with a "Near Earth Object" (NEO) like an asteroid or comet is quite another matter altogether.

To see how objective probability works, imagine the odds of tossing a six with a pair of dice. The first step is to determine how many opportunities are possible. That is, what are all the available alternatives? In this case, this often very difficult step is easy. There are two chances, as each die has one six. As a cube, each die has six sides, so there are two chances out of 12 opportunities to toss at least one six, shown as 2/12 or reduced as 1/6. The odds expressed as a percentage are 16.7%. The odds of tossing two sixes with this pair of dice are 1/12 or 8.3%.

Importantly for national security professionals, probabilities can also be *conditional*. This is a situation where things work together, so the chance that one event will happen is combined with the chance of one or more other things occurring. In this case, the eventual outcome is a product of the individual probabilities. For example, the odds of two sixes on a toss of the pair of dice are the product of their individual probabilities — $1/6 \times 1/6$, equals 1/36% or 2.78% and so on. Consider the time-honored risk management adage, "Do not put all your eggs in one basket." The idea here is that two or more failures or loss events must occur before all is lost. This concept was at work during Babylonian times when camel caravans were under frequent attack by robbers. Prudent merchants split their cargoes among several caravans. Similarly, Chinese shippers put their goods on several boats to sail them down the Yangtze River rather than on just one. In this way, they spread their risk, as insurers would say. In Shakespeare's play, *The Merchant of Venice (Act 1, Scene 1)*, we can find this "spread of risk" idea celebrated as well:

> My ventures are not in one bottom trusted,
> Nor to one place; nor is my whole estate
> Upon the fortune of this present year;
> Therefore, my merchandise makes me not sad.[7]

This same "spread of risk" idea is used in the contemporary counterterrorism world. Known by a more modern name, however, this technique is referred to as defense in depth. It is achieved by deploying "rings" or "layers" of security. To illustrate the way it works, imagine that five rings of security are put into effect and if each one is thought to be 50% effective, then the overall odds of having effective security in place are the product of each of the five rings working together. To derive the overall effect, simply multiply 0.50×0.50 in five steps. The answer is 96.875%. To penetrate to the target, the attack would have to defeat each of the rings of security to succeed. The defeat of only one (50% effective) or two (75% effective) rings would, of course, be far easier. This is the approach used in the design of ancient walled cities and medieval castles. The concept was also used after September 11 at Boston's Logan International Airport as described in Stephen Flynn's important book, *America the Vulnerable*.[8] At Logan, the outer layer of defense included the fishermen in Boston Harbor. According to Flynn, they were

equipped with cell phones so they could report any out-of-pattern occurrences. Overall, Logan's defenses included many additional layers.

Finally, probabilities can also be *subjective*. These probabilities rely on an individual's opinions to determine the odds rather than the use of statistics to gather and organize data and the laws of probability to analyze and promote evaluation of the data. Because human opinions are involved, subjective risk assessments can have a significant psychological dimension. Risk is usually measured objectively when possible, but we also can assign subjective values to risk and work with them too, either alone or in combination with objectively derived probabilities. This opens our inquiry into the concept and nature of risk to a very wide debate about the role and implications for various interpretations of risk and its measures. This interesting dilemma and sometimes spirited if not sparky debate will not be resolved here.

National security professionals use modeling methods to profile terrorism events to identify leading indicators that could reveal suspected terrorists. These methods involve the application of data mining methods and other techniques in search of telling patterns of behavior that could lead to the prevention of an attack. Similarly, insurers routinely model their expected losses using the laws of probability and statistics, notwithstanding all of their real and imaginary imperfections, to set business development, underwriting, and reinsurance purchasing guidelines. Financial models employing statistics and probability statements are also used by state insurance regulators, financial rating agencies, investment bankers, and others to verify within a reasonable level of confidence that property/casualty insurers are able to deliver on the "promises to pay" that they sell. The models used by insurers are far better today than before they were put to a real world test following hurricane Andrew, which was a category four hurricane that cost over $26 billion and ruined a dozen small insurance companies in August 1992.

Andrew was America's costliest storm until Katrina came ashore in August 2005. Katrina's costs are still being counted, but the total exceeds $100 billion, so far. Deaths from Katrina exceed 1000, the most from a hurricane, since 1928. The effort to evacuate New Orleans appears to have been slower and less effective than it should have been.

The frequency of hurricanes enables insurers to build predictive models of them. The terrorism database is somewhat thinner, yet it is useful. This is true even when loss events seem too infrequent to pattern and accurately predict. For example, insurance risk assessment models are being used by insurers and security professionals to predict terrorism attacks. "…companies like Risk Management Solutions (www.rms.com), with its Terrorism Risk Model, and Air Worldwide (www.air-worldwide.com), with its Terrorism Loss estimation model, have adapted modeling for natural disasters to create models for terrorist activity."[9] Insurers use their hurricane models to "price the odds" of a storm in a given area, develop premiums, and in turn sell

insurance, but not too much that they become dangerously exposed to more losses than they have premiums with which to pay the losses. When counting and mathematical models are not practical or possible, subjective probability statements can be estimated and used. Of course, some estimates are likely to be far better than others. The quality of an estimate will depend on, among other things, the familiarity, expertise, accuracy of risk perception, and risk aversion and communication abilities of the people providing the estimate of the odds. As we will discuss later, a number of useful methods have been developed to help cope with a lack of factual information when experience is limited or even unavailable altogether. Harnessing the theory of probability and putting it to work in the service of risk management tasks is quite useful. Since more losses can happen than will happen, probability theory can help the risk manager and national security professional focus attention and allocate resources effectively.

Hazard and Vulnerability

The second dimension of the logic of chance involves calibration of the *vulnerabilities* or level of *hazard* influencing a risk. This assessment complements the concept of probability. It explores the notion of susceptibility to loss. More specifically, hazard is defined as any condition or situation that increases the chance of a loss by a peril or a threat. Hazards or vulnerabilities work to increase the odds of a loss occurring. Consider the City of New Orleans. Building a major Gulf Coast city 8 feet below sea level increased the chance that a hurricane would cause major flooding, in addition to the major wind damage expected from a hurricane. The hazardous location, in this case, was made worse by the existence of inadequate levees, sea walls, and pumps. The lack of an effective, comprehensive evacuation plan, in turn, left the people of New Orleans more vulnerable to the ravages of hurricane Katrina. Pumping oil and gas out of the ground added to the hazard level as well because this usually beneficial and economic activity had caused the city to sink even further below sea level. It is difficult to strike a reasonable balance between the benefits to some with the costs and risks to others. The natural physical buffer to the wind and water brought by the hurricane had also been eroded, developed, and otherwise consumed over time. The end result was, of course, a very vulnerable city and a population desperately in need of risk management attention. In this way, a major New Orleans hurricane became an anticipated, expected, but mismanaged disaster.

The Logic of Loss

The logic of loss informs and provides some insight into the diminution of value that is likely to result should a loss occur. It is concerned with the severity of the risk just as the logic of chance is concerned with the frequency

of risk. When losses are described, discussed, and distributed, they are often described in dollar terms or monetized. This can ease comparisons, promote conversation, facilitate risk management, and serve as a catalyst for sound policy development. Buildings have restoration, reconstruction, or repair values. Personal property and earnings have replacement values. Even life itself is often monetized. State Worker's Compensation Laws, juries deciding wrongful death cases, life insurance agents, and government accountants attempting to estimate the benefits and costs of regulation are all concerned with determining the "value" of a life. Of course, we all die, but the financial risk to our dependents occurs if we die before our time by accident or wrongfully. The loss dimension of risk is, in theory and in fact, useful information for the risk manager or someone else concerned with assessment of the significance of risk and, consequently, its management.

The questions prompted by the logic of loss include: How big could a loss be? How many fatalities and injuries? How much property loss and disruption of economic activity? To work toward answers to these questions, the logic of loss examines the impact of loss across three dimensions: (1) the cause of loss, (2) the extent of loss, and (3) the consequences of the loss.

Cause of Loss

The *cause* of a loss is referred to as a threat or peril. Threats and perils can be either *proximate* or *remote*. Causes include the familiar catastrophe natural disaster *perils*, such as windstorm, flood, famine, earthquake, volcanic eruption, asteroid collision, viruses, bacteria, and the like. We seek to be safe from these accidental perils. These natural perils or causes of loss are complemented by a long list of manmade *threats*, such as war, insurgency, terrorism, riot, and the many other agents of death, injury destruction, and economic disruption and discontinuity. We seek to be secure from these manmade threats. And threats are everywhere. They exist in nature, in the laboratory, and in the minds of terrorists. As their causes differ, so do the risk management remedies we plan and apply to them. Awareness, prevention, and protection strategies must reflect these differences. Recovery and reparation actions are less threat specific, but can be related. For example, an earthquake resistant office building may be relatively resistant to a terrorist bomb as well. Yet, understanding the inner workings of the hurricanes may only contribute minimally to our understanding of tornadoes. But, response, recovery, and reparations strategies may be applicable to both. Similarly, the same actions may prove useful following a biological, chemical, or nuclear attack, as they would be following the outbreak of a pandemic, SARS outbreak or some other large-scale health emergency.

The more familiar threats and perils are joined today, by a growing list of new threats that are frequently the by-product of our technological

progress. Robotics, nanotechnology, and transgenic experimentation hold unknown but, perhaps, significant promise of future benefits. Just think of the wonderful, life-enhancing benefits that could flow from an understanding of the genetics of cancer and Alzheimer's disease. These same laboratory experiments, however, could also represent significant possibilities for unknown, yet to be discovered losses. In this way, scientific inquiry can become an unwitting partner in the creation of agents of death and destruction. The ceaseless and sometimes careless march of scientific inquiry and experimentation would benefit from closer attention to risk. Unintended consequences seem too prevalent and too regular to ignore the probability of their existence with most new discoveries. Today's new scientific breakthrough could also become a new agent of death and destruction, either because it falls into the hands of a psychopath or because of unintended, unknown consequences at the time it was discovered or deployed. Asbestos, DDT, nuclear energy, dioxin, and thalidomide are but a few on a long list of very unfortunate examples. Scientific innovation sometimes bears twins, one good and the other evil.

To illustrate, asbestos is a good fire prevention material. Unfortunately, however, prolonged exposure to asbestos fibers can cause asbestosis, a breathing disease. These toxic fibers can scar lung tissue and create major breathing problems and possibly cancer and painful death. We now regulate and manage this risk after learning another hard lesson. Asbestosis victims and the families of victims are seeking billions in compensation for injury and death. Progress often comes at a high price. In fact, bioerror may be the biggest threat confronting humanity today. Especially, since entrepreneurs are experimenting with genes in unregulated bioengineering laboratories across the globe. Creating new life forms can have dire consequences, as it may not be possible to reverse an accidentally chosen errant course.

Less proximate, perhaps, are the dangers represented or thought to be represented by the ever-increasing release of manmade "green house gases" into the Earth's atmosphere. Carbon dioxide emissions from the burning of fossil fuels are thought by many to be contributing to a general and alarming rate of warming of the planet, particularly in the Earth's coldest regions. "There is more carbon dioxide in the atmosphere today than at any point during the last 650,000 years, says a major new study that let scientists peer back in time at 'greenhouse gases' that can help fuel global warming."[10] Catastrophic consequences are, of course, predicted. The truth of the matter, however, is elusive as the Earth naturally experiences warming and cooling cycles. Cassandras (a prophetess from Greek mythology famous for making important, but regularly ignored warnings of doom) predict the worst, while critical thinkers demand unshakable facts. Unfortunately, "certainties" in life are rare — death and taxes are two that rarely raise a debate. Much else is hypothesis. For example, consider Nobel Laureate, Kenneth Arrow on this topic: "[O]ur

knowledge of the way things work, in society or in nature, comes trailing clouds of vagueness. Vast ills have followed a belief in certainty."[11]

Of course, the less proximate the loss causes, the more debate about the existence of any risk at all. When facts are few, human minds are prone to wishful thinking and default to a favorite habit of simply muddling through. Furthermore, we are energized far more by the immediate than the remote. In fact, as far as risk is concerned, for most humans, out of sight is very much the same as out of mind. Psychologists report that this phenomenon is the consequence of one of our many natural biases or thinking errors. Consider the attitude of teenaged children toward risky behavior. Many teens act as though they are invincible. The opposite can also be true. If a loss occurred recently, we tend to think another similar loss will be likely soon. This is called the "availability bias" and few are immune to it and the many other biases that plague the normal human mind.

Another natural human perception problem is our tendency to regard low probability events as impossible. For example, nuclear power is a source of clean, relatively cheap, fuel. It is, however, efficient, only if you maintain a short-term outlook. Utility plants powered with nuclear fuel produce quantities of spent fuel that can be used to make terrible weapons. And unless scientists create a solution, these used fuel rods remain a source of lethal radiation for tens of thousands of years.

Extent of Loss

Joining "cause" in the logic of loss is the notion of *extent*. This dimension of loss addresses the question of the impact or size of the loss in question. How big? How wide spread? How long lasting? These are the relevant questions addressed by this dimension of the logic of loss.

These fundamental questions can be pursued along three lines of measurement that provide a loss with its dimension. The concepts involved include: (1) the magnitude of the loss, (2) the scope of the loss, and (3) the duration of the loss. For a loss occasioned by any cause, the usual first questions are aimed at learning its *magnitude*. Is the loss large enough to care about? The magnitude of a loss is often monetized. It can also be explained in terms of lives lost or injuries. When people are involved, the extent of a loss is frequently described in terms of the number of "casualties" caused by the loss.

The *scope* or "reach" of a loss is defined in terms of space or time. Geographic terms are used to define the reach of a loss or potential loss such as "global," "regional," or "local." In the case of disease, the term "epidemic" is used to describe a disease of very large scope or "pandemic" to refer to a disease with worldwide impact.

The last dimension of the extent of a loss refers to the *duration* of the loss event itself. Is its impact felt immediately or is it experienced over a

prolonged period of time as in the case of a continuous or repeated exposure to conditions or circumstances? According to research done by Paul Slovic, president of decision research and professor of psychology at the University of Oregon, we tend to fear immediate threats far more than those that take longer to emerge. Consider two large risks with two differing durations. Even very large earthquakes last only a few seconds. Asbestosis, the lung scarring disease causes breathing problems, heart failure, and the cancer mesothelioma. These problems become evident over a long period of time — 10 years or more, as a result of a continuous and repeated exposure to airborne asbestos fibers. Consequently, asbestosis represents a special threat to workers who are required to handle products containing the dangerous mineral fiber, asbestos. The risk of asbestosis was not initially known. Its discovery occurred over a period of many years. Hence, losses of both very short and very long duration can be measured in the billions of dollars of lost asset value and in terms of many casualties.

Consequences of Loss

The third of the three dimensions of the logic of loss addresses the *consequences* of a loss. Postloss, following an event causing casualties, injuries, damage, disruption, or destruction, the relevant questions will center on why the loss matters. Who cares about it and why? How much money and effort will be required to restore normal operating conditions or maintain the continuity of operations? How many casualties were incurred and what must be done to compensate for their deaths and injuries? What public or private property was damaged or destroyed that will have to be repaired or replaced? What environmental damage has been inflicted on air and water quality? What disruption to power, fuel, and food supplies has resulted from the loss? In short, what *tangible* and/or *intangible* assets have lost value, post-loss? Tangible assets are physical things, such as databases and networks. Intangible assets are more abstract things of value, such as reputation and relationships. Both can lose value, post-loss, and cause a diminution of operational capability and, hence, diminish business system and organizational effectiveness.

Risk is most usefully defined as "the chance of loss." The extent of the risk, its degree, can be defined and in some useful way described and informed by a thoughtful examination of two logics: the *logic of chance* and the *logic of loss*. These logics address the two principle dimensions of risk and define the significance of a risk. They provide some insight into the two most basic questions facing risk managers: "What are the odds of a loss occurring?" and "How large could the loss be?" Insurers refer to these dimensions as the frequency and severity of loss and use the averages of these statistics to calculate the premiums they charge their policyholders. In effect, insurers set their prices this way by "pricing the odds."

Risk Management

The management of risk, in a normative sense, involves two fundamental activities: *Risk recognition* and *risk resolution*. These activities are sequential. The idea is that, first a risk needs to be as thoroughly recognized and understood as well as human psychology, time, and science will allow, before it is likely that the risk will be effectively resolved. Risks need to be thoughtfully recognized before they are resolved, just as problems need to be carefully defined before they can be solved. The term *risk management* refers to purposeful intervention to eliminate or mitigate the chance of loss. The objective of risk management is to preserve the pre-loss value of tangible (office building) and intangible (organizational reputation) assets. These assets are usually the foundation of an organizations "value proposition" or more plainly, they are the reasons why an organization has customers, constituents, and stakeholders, whether they are citizens expecting safe streets in the public sector or stockholders seeking competitive returns on their investments in the private sector.

The term *risk management* was first used eons after it was first practiced. Early documentation of civic responsibility for managing risk can be found in the Code of Hammurabi written in stone by the Babylonian King of the same name almost 4000 years ago. This code was developed, in part, because bandits and robbers were attacking caravans that served as important sources of commerce to the Babylonians. To provide assurance that commercial ventures, if attacked, would not be in vain, the Code provided indemnity by the civic authority responsible for maintaining order in the area where the loss took place. The Code is engraved in a block of black diorite, (a granite-like rock). It was found in 1901 in Susa, near the ancient Persian city of Persepolis, (now Iran) by French archeologist, Jacques de Morgan. The monument preserves 44 columns with some 3600 lines. Several interesting "insurance" provisions can be identified in the Code. The pertinent sections are as follows:

> (23) If the highwayman has not been caught, the man that has been robbed shall state on oath what he has lost and the city or district governor in whose territory or district the robbery took place shall restore to him what he has lost.
>
> (24) If a life (has been lost), the city or district governor shall pay one mina of silver to the deceased's relatives.
>
> (25) If a fire has broken out in a man's house and one who has come to put it out has coveted the property of the householder and appropriated any of it, that man shall be cast into the self-same fire.

> (45) If a man has let his field to a farmer and has received his rent for the field but afterward the field has been flooded by rain, or a storm has carried off the crop, the loss shall be the farmer's.
>
> (48) If a man has incurred a debt and a storm has flooded his field or carried away the crop, or the corn has not grown because of drought, in that year he shall not pay his creditor. Further, he shall post-date his bond and shall not pay interest for that year.
>
> (117) If a man owes a debt, and he has given his wife, his son, or his daughter (as hostage) for the money, or has handed someone over to work it off, the hostage shall do the work of the creditor's house, but in the fourth year he shall set them free.
>
> (125) If a man has given anything whatever on deposit, and where he has made his deposit, something of his has been lost together with something belonging to the owner of the house, either by housebreaking or a rebellion, the owner of the house who is in default shall make good all that has been given him on deposit, which he has lost, and shall return it to the owner of the goods.[12]

Today, civic rules are legislated for a very wide variety of risks. They vary, somewhat in style, and degree of intervention, depending on the culture involved. For example, Europeans tend to promulgate regulations, whereas Americans tend to look for ways to compensate victims, after a loss, often through the courts. Americans in general have an aversion to regulations. New Hampshire even has a motto that captures and celebrates this idea — "Live Free or Die." Notwithstanding the American preference for a relatively smaller government role in risk management, a number of the more prominent federal laws that aim to reduce risk quickly come to mind. A partial list follows:

- The National Traffic and Motor Vehicle Act
- The National Highway Safety Act
- The Federal Coal Mine Health and Safety Act
- The Federal Occupational Safety and Health Act
- The Federal Consumer Product Safety Act
- The Clean Air Act
- The Federal Securities Investor Protection Act

The concept of risk management first entered the corporate world in 1916 as one of Henri Fayol's six fundamental responsibilities of management. He referred to the practice of risk management as a cluster of "Security Activities" meaning the need to protect the property and persons of the

organization.[13] His list of a manager's responsibilities included the responsibility for ensuring the continuity of the enterprise in the face of the many dangers that would disrupt or end it.

The modern practice of the management of pure risk can be tracked back to a 1956 *Harvard Business Review* article written by Russell B. Gallagher, "Risk Management: A New Phase of Cost Control."[14] At the time he wrote this article, Gallagher was the "insurance buyer" for the Philco Corporation in Philadelphia. His interest in risk management arose from a strong logic. He reasoned that by paying close attention to the risks that drove the corporation's insurance premiums, insurance costs could be controlled and, hence, Philco's profits increased. By being proactive in the identification and reduction of risk, insurance costs could be avoided, as insurance premiums tend to roughly reflect loss costs for most large policyholders. Subsequently, the "transfer" of certain pure risks to insurers was no longer the only strategy used by insurance buyers. Risk that could be controlled did not have to be transferred and become part of an insurance premium. Increasingly, managers began to think about pure risks as a management problem that could be solved without the exclusive reliance on costly insurance. Of course, managers who were unable to find an insurer willing to accept their risks had risk management activities forced on them along with the need to make some provisions for paying reconstruction and restoration costs. Very large companies, initially oil companies, formed their own "captive" insurance companies to more formally finance their risks internally. Thus, the acceptance of the financial consequences of a loss also incented a strong interest in early forms of risk management.

The Risk Management Sequence

As introduced and briefly discussed earlier, the management of risk can be thought of as a sequence of seven logical steps, each involving a set of prescribed activities aimed at preserving the strategic, operational, and financial continuity of an enterprise. These steps can be seen as a necessary sequence — a RMS because they follow a rational progression from the initial envisioning of a risk to its eventual mitigation. The steps are:

1. Phase I. Risk recognition
   (a) Step (1) *Imagine* the risk
   (b) Step (2) *Describe* the risk
   (c) Step (3) *Observe* the risk
   (d) Step (4) *Measure* the risk
   (e) Step (5) *Map and Model* the risk

2. Phase II. Risk resolution
   (a) Step (6) Loss *Prevention*
   (b) Step (7) Loss *Mitigation*

The main benefit from following the RMS is an effective use of risk management resources. By carefully understanding the risks faced along with their various dimensions, those with responsibility for managing risk in their role as either the risk manager, public policymaker or national security professional can achieve a useful position from which to craft an effective risk disrupting intervention that could result in the preservation of life and the continuity of the enterprise. The logic of the RMS is that useful, effective intervention, and hopefully mitigation of the risk will occur best for risks that can be managed through the entire RMS. Unfortunately, today many risks cannot make it all the way through the RMS. This is true because we simply do not have the scientific knowledge or we have not decided to allocate the time or resources necessary to master the many mechanisms that drive the destructive nature of even the most common and ancient risks. The vast voids in our knowledge are evident at each step of the sequence.

Risk is Reactive

As we encounter and manage risk within the highly interactive ecology that comprises our world, risk itself tends to react to the management attention we invest in it. That is, risk changes or enters into a state of change as we attempt to manage it. Hence, like most things in our dynamic world, risk has a reactive, almost organic, reflexive nature. This nature resists conformance with rigid, imposed rules. Hence, the application of the math of chance or any particular framework or sequence of steps such as the RMS can be helpful, but far from a perfect method for managing risk. Perhaps, at best, the RMS can be thought of as an iterative process. As we learn more about a risk, we can move back up the RMS and restart our decent, with more information, knowledge, understanding, and, ideally, risk management effectiveness.

To illustrate the reflexive nature of risk, consider what happens when someone purchases an insurance policy to "transfer" the financial obligations imposed by a pure risk. The moment a policy is issued the nature of the risk changes for both the insured and the insurer. In fact, the existence of the policy creates a new risk. After a property owner is issued an insurance policy, the property owner is probably less worried about the perils that threaten the property compared to the period before the owner was insured for those perils. Why? The piece of mind and freedom from financial worry insurers provide relieve the owner of at least some degree of concern. This relief could quite possibly result in reduced care and attention or even neglect of the

exposed values at risk. This relaxation of care can result in what insurers refer to as a "moral" hazard. It is in this sense that risk can be reactive to its environment and the care and attention that is allocated to it. The federal flood insurance program provides an example of the abuse that insurance can cause. Even though less than one half of hurricane Katrina's victims had this coverage, the program is now bankrupt — financially and conceptually. When insurance is working well it is a pooling process in which the premiums of the many pay the losses of the few. But for the peril of flood, only people in serious danger of regular flooding buy coverage — paying a few hundred dollars for hundreds of thousands of dollars of coverage, so the flood insurance pool is too small to pay the losses incurred. Given the omnipresent interest of real estate interests and the reluctance of coastal communities to restrict building in flood prone areas, the U.S. Treasury will probably continue to subsidize and, therefore, incent construction and reconstruction on flood-prone land. Of course, if flood insurance made good economic sense, the private sector would be providing it.

Risk like many other things in our world is ever changing, adapting, and conforming to external conditions and exogenous developments. For example, iron bridges can rust and become unsafe. They could also become too low. Should global warming result in melting of the ice caps; the bridges we now have may prove too low to allow traffic on or beneath them. Bridges like most other instrumentalities of transportation only exist to carry traffic for a finite period. They will fail at some point. The question we have about this threatened failure brings us straight back to our two logics for more information. The logic of chance will help us understand more about *when* it might fail and the logic of loss will help us understand *why* we should care.

So, how can the mercurial, organic, reactive presence of risk be effectively managed? What can we possibly impose on it to take its measure and attempt to tame its fury?

Applying the RMS

The RMS is a useful start, because it enables us to gain some understanding about where we stand with the risks we face as it identifies and clarifies the frontiers where we need to go to more effectively cope with the risks we are aware that we face. As with any useful framework, it should help us derive, organize, and extract meaning from our experience. This meaning, in turn, should enable us to cope with the dangerous, uncertain world we share with countless pure risks. As we encounter risks and strive to cope with them, we are extrinsically incented as responsible citizens and intrinsically as rational

beings to better mitigate the losses and loss potentials involved with living. Only a true fatalist would fail to intervene in any way. But, risk management is based on the optimistic assumption that the future matters and that if we think and act intelligently, we can make a positive difference — that we can usefully interfere with the natural course and change the inertial model to achieve better results. A bullish assumption, perhaps, but we have many examples of success to point to as models. They serve us as sources of encouragement.

For example, Raymond Baldwin, who was Connecticut's governor at the time of the 1938 Great Atlantic Hurricane, later reported to me that New Englanders had no warning of the approach of the terrible storm. So, there was no preparation. There was no evacuation. No need to think about safe destinations and post-storm meeting places. The prevailing view was that a thundershower was coming, not the devastating killer storm that actually raced up the East Coast and roared ashore. In sharp contrast, we have many hours, if not days of advanced notice these days, so evacuation is usually possible for people in a great storms path. Today, hurricanes along the East Coast of North America do not take the population by surprise.

More broadly, the possible benefits from the application of the RMS can be illustrated by considering a series of questions drawn from it:

- Could we have anticipated the loss or did we experience a failure of imagination?
- Can we describe the risk in ways that invite a conversation with people who may have private information that could possibly be useful?
- Have we been witness to phenomena that we did not connect with something significant?
- Are measurement methods or other forms of telemetry within reach, which could be used to save lives or reduce loss to property?
- How exactly does a natural event like a hurricane steer? If we knew, we might be able to narrow the "cone of confidence" about where, when, and with what force a massive storm might make landfall. What must we know to predict earthquakes, a collision with an asteroid, or the side effects of nanotechnology?

These and other similar questions prompted by the RMS can be helpful in pursuing the most effective ways for first acquiring an understanding of risk, and then crafting possible risk interventions that would move us toward the actual management and effective mitigation of the risks involved.

The purpose of the next sections of this chapter is to look at each step of the RMS more closely.

Risk Recognition

Step (1): *Imagine* the Risk

Many of life's troubles, it seems, begin with a failure to think critically and creatively and employ ethical reasoning. Too often, we fail to examine the underlying assertions and assumptions when we are trying to decide what to do. Effective risk management requires this careful thinking. Unfortunately, to many of us, careful thinking seems like too much work. Somehow it seems more acceptable to just carry on, take things for granted, make beneficial, action enabling assumptions, and simply hope for the best. But extreme optimism is not a viable risk management strategy, especially, for those responsible for the welfare of others or their valuable property.

Consider for a moment the use of pharmaceutical drugs. Can you imagine what they might be doing to both individual users and our society as a whole? Particularly, the kinds of psychotropic drugs that are used to modify behavior—Ritalin for schoolchildren diagnosed with attention deficit disorder (ADD), somehow, by some "expert" and tranquilizers for "stressed" adults. Are those who prescribe these chemicals and those who ingest them in the process of redefining what it means to be "human?" If by taking these drugs we are causing behavior to become more "normal," whose definition of "normal" is being used? Would Pablo Picasso, Martin Luther King, Thomas Edison, and Albert Einstein pass the test, or through our alchemy are we irreversibly altering behavior to conform to some conventional protocol? What is the quality of the science that supports the prescription of so many of these drugs to so many? If we are to manage risk effectively, we need to examine our actions with foresight and sensitivity to the things that could go awry. In his recent book, *Think*, Michael Le Gault, observes that "about 10 to 12% of all boys between the ages of 6 and 14 in the U.S. have been diagnosed as having ADD. Fifty-six percent of children diagnosed with ADD have used ritalin at one time or another. But who is doing the diagnosing?"[15] The use of a powerful drug by so many children would, one would hope, be based on some reasonable scientific support. But, there appears to be very little, if any of this support.

> The deeper one digs into the ADD-ritalin proliferation, the stronger the distinctive aroma of greenish ink on a crisp paper hinting of an unholy professional–political boondoggle. Many critics of ADD, and the entire learning disability industry as a whole, believe psychiatrists have used drug-based therapy to provide their profession equal footing, both professionally and remuneratively, with traditional medicine. The pharmaceuticals used to treat the growing number of mental and psychological

> disorders are themselves the basis of a multibillion-dollar industry. Even schools get a piece of the action, with many school districts collecting extra funds called "bounties" for each student diagnosed with a specific learning disability.[16]

The threat of terrorism in the U.S. requires less imagination, following the September 11, 2001 tragedy. We learned from *The 9/11 Commission Report* that, "… the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities and management."[17] Citizens expect their government to protect them from the ravages of all manner of risk. We expect that effective safety, security, and public health services will be provided by our government. That is the purpose of government. Indeed, we organize and support government to provide citizens with reasonable assurance that our lives and liberty will not be unduly stressed by risk. Notwithstanding the threats from natural catastrophes, terrorism, enemy attack, pandemic, or the economic threats of unemployment or inflation, we rely on our political leaders for protection. This requires imaginative, effective leadership. We want our leaders to be constantly searching for threats to our well being: "What of a serious nature might go wrong and what, practically should we do about it?"

We can look to history for answers or at least clues and follow a trial and error process. We tend to think that if a loss has occurred and we can recall it, it will happen again so we should take some steps to prepare for the emergency and the aftermath. But timing can blur our memories. In fact, our memories can be our biggest impediment to intelligent and effective risk management.

Consider for a moment, the risk of a collision between the Earth and an NEO. Historically, these events have proven very catastrophic to the Earth's inhabitants. In fact, these collisions have been so massive that they have changed the shape of the Earth itself. Fortunately, large collisions with NEOs have not been frequent. They have been so infrequent, in fact, that several current authors writing on the subject of our over wrought fears about risk suggest an NEO collision is too remote to worry about. For example, "Asteroid mania has certainly made us more aware of the dangers posed by near-Earth objects. However, it glosses over the only firm conclusion scientists can give us. There will be no Earth–asteroid collisions in this century, which is as far in the future as scientists can predict asteroid trajectories with any accuracy."[18]

And again:

> Life today for citizens of the developed world is far safer, easier, and healthier than for any other people in history. Modern medicine has all but wiped out many diseases that once were common killers. Science and technology have given us countless devices that protect our bodies from injury, secure our property, and warn

> us of impending disaster. And modern intelligence gathering can pinpoint threats to our domestic security as they arise. So why is an epidemic of fear sweeping America?[19]

According to this view, we live in an artificially created and cultivated culture of fear — a world where the slightest inconvenience is exaggerated, largely by the professional media, into predictions of impending doom, as a way to make money.

However, history would suggest that risk management is a good idea. For example, projects like NASA's Near Earth Object Program makes good sense, notwithstanding how remote the chance is of a collision with an NEO. If you can imagine for a moment, geological time rather than our own immediate frame of reference, during the 4.5 billion-year history of the Earth, the only abrupt mass extinctions of life on Earth were caused by asteroid collisions and massive volcanic eruptions. And, according to Sir Martin Rees, England's Astronomer Royal and Royal Society Professor at Cambridge University in his fascinating, if not thoroughly frightening book, *Our Final Hour*, they will happen again.

> About sixty-five million years ago Earth was hit by an object about ten kilometers across. The resultant impact released as much energy as a million H-bombs; it triggered mountain-shattering earthquakes around the world, and colossal tidal waves; it threw enough debris into the upper atmosphere to block out the Sun for more than a year. This is believed to have been the event that wiped out the dinosaurs. Earth still bears its scar: this momentous impact scoured out the Chicxulub crater in the Gulf of Mexico; nearly two hundred meters across… The Chicxulub impact … may have been the most recent event of this magnitude. Two other similarly vast craters, one in Woodleigh, Australia, and another at Manicouagan, near Quebec, in Canada, could be the aftermaths of comparable impacts 200 to 250 million years ago. Perhaps one of these caused the greatest extinctions of all, at the Permian/Triassic transition 250 million years ago.[20]

According to Rees, NEOs about 50 meters across hit the Earth once per century. The risk, given the apparent frequency, is low.

> We do not know whether a large, dangerous NEO "with our name on it" is destined to hit in the coming century. However, we know enough about how many asteroids there are on Earth-crossing orbits to be able to quantify the probability. The risk isn't large enough to keep anyone awake at night, but it isn't completely negligible either … in the next fifty years … there is about one chance in ten

> thousand that an asteroid half a kilometer across will crash into the North Atlantic, causing giant tsunamis (tidal waves) that would destroy the North American and European seaboard … The probability that we will end our lives (along with many millions of others) in such an event is about the same as the average person's risk of dying in an air crash — somewhat higher, indeed, if we live near a coast, where we are vulnerable to smaller tsunami.[21]

To add additional perspective to these numbers, according to the National Safety Council, the most recently available odds of dying in a transportation accident are 1/6000 in a given year, 1/228 over a lifetime.[22] However, given the severity involved, and the ability to determine, plot, and monitor the orbits of the NEOs, it is wise that someone at NASA is thinking about managing this risk, since a collision with even a modest-sized NEO could cause in Rees's words, "… millions of fatalities."

Given that we could have warning of an impact with an NEO, it would certainly seem worthwhile to invest a few millions to help ensure evacuation, of say, costal areas that would be at risk from a tsunami. Of course, at some point we might have the ability to deflect and alter the orbit of an oncoming NEO in time to avoid the collision altogether. But, this strategy will not be available to us if we have not been paying any attention to both our planetary history and the NEOs around us. Are NEOs a false alarm? Ignoring potentially catastrophic, low probability events is a very dangerous life style.

Certainly, in the aftermath of hurricane Katrina, it is easy to conclude that the ability to predict a calamitous event can be somewhat overrated. Nevertheless, the hurricane peril is a good example of how risk management practices can be effective. According to R.A. Scotti, in his book *Sudden Sea*, the great New England Atlantic Hurricane of 1938, which caused about 600 deaths and massive destruction throughout New England, packed very high winds, but we do not know how high as the instruments meant to clock the storm along the coast were destroyed. Wind gusts were measured at 186 miles per hour, with sustained gusts of 121 mph, 70 miles inland from the storms eye at Blue Hill Observatory in Milton, MA. Seismographs intended to measure the impact of earthquakes were set off as the storm made landfall on Long Island. Sea salt coated the windows in Montpellier, VT, 120 miles inland. It was a big, dangerous storm, and it struck without any warning. "It was the most destructive natural disaster in U.S. history; worse than the San Francisco earthquake, the Chicago fire or any Mississippi flood."[23]

In sharp contrast, before Hurricane Katrina came ashore, the residents of the area had several days notice of the storms approach and, remarkably, approximately 80% of the residents were evacuated. The point is that with notice, most people who can, will choose survival and evacuate, no matter how tempting the hurricane parties.

Unfortunately, some resist evacuation and assume the consequences. Some perhaps are left behind, unable to leave and are not offered help. This sadly, was apparently the case in New Orleans, where citizens and prisoners unfortunately were left behind to fend as best they could while the world watched the disaster unfold.

While hurricanes are no longer surprises for most, earthquakes, tornados, tsunamis, and many other perils still are. This situation suggests the need for more pervasive and more thoughtful, perhaps generic or multiperil "all risk" preparations. Since we know we are exposed to many threats and perils, but often cannot predict when they will happen, it is best to be prepared for the major emergencies we can reasonably anticipate.

Perhaps, not as dramatic as a hurricane, but highly arresting nonetheless, is the sudden loss of electrical power over a wide area. Such an event occurred in August 2003. The August 14 blackout, the largest in U.S. history, put some 50 million people in the dark across eight states and parts of Canada. Without electrical power nothing much works for very long. In this sense, our electrical grid, a network of some 3500 independently operated but automatically connected power generating organizations, represents along with food, air, and water, an essential infrastructure.

The power grid, as our power-generating network is known, is very fragile. The risk of power failure is managed by the power providers. Unfortunately, this risk appears significantly under managed, although some hopeful efforts are apparently underway that could alter this surprisingly precarious situation.[24]

The massive power failure on August 14, 2003 was caused by the failure of a small Ohio utility to trim trees along its easements. When overloaded wires sagged and touched the untrimmed trees, trees that should have been trimmed or eliminated, the power system for northeastern North America shut down. Because the power providers are linked together via the Northeast grid, the initially small, localized failure put the entire Northeast in the dark. Of course, it costs money to trim and eliminate trees and keep power right of ways well maintained. But, in the absence of standards, controls, audits, and an accountability structure to apply meaningful sanctions, profit-focused, short-term thinking can and often does overrule prudence. In our increasingly networked world, the benefits, costs, and risks of connectivity need to be given careful consideration.

Another significant risk in the hands of independent entrepreneurs exists in the world's biotechnology laboratories. Perhaps, less easily imagined than electrical wires sagging into neglected trees, but equally unmanaged are the experiments now underway and those soon to begin in the world's biological laboratories. The risk of "bioerror" becomes increasingly worrisome as scientific inquiry penetrates the mysteries of life itself. Imagine if you will, a new airborne virus or bacteria, accidentally resistant to treatment, much as the genetically modified organisms (GMO) grasses and weeds have become while

scientists were working to create a new disease-resistant corn, soybeans, and other important cash crops. Pollen blows with the wind, so when these new products are planted in open fields, there is no practical way to contain it. But, what is the risk? Who will be held responsible? And isn't life changing all the time anyway? After all, change is life's natural course. The problem is that we are implementing what once was natural selection and evolutionary processes on our own, haphazardly, with no real idea what in the world we are doing. And there is no control or accountability regime to oversee or effect any reasonable control. But, how should scientific advancements be regulated and monitored? Should the "precautionary principle" ("better safe than sorry," "look before you leap," etc.) be required somehow? In what forum should the risks that are the consequence of new life forms be discussed? Who should be included in this conversation? What types of experiments pose the worst risks?

Sir Martin Rees, in his book, *Our Final Hour*, comments on this problem from a scientist's perspective. "Restraint is obviously justified if the experiments themselves pose a risk, for instance, by creating dangerous pathogens that might escape, or by generating extreme concentrations of energy."[25]

For over 30 years, scientists have been discussing the need to exercise some caution with respect to experimentation with new life forms. In 1975, scientists reacted to laboratory manipulations of life made possible by the technique of recombinant DNA. The "Asilomar Conference," a gathering of scientists called together by Paul Berg of Stanford University, produced the Asilomar Moratorium aimed at defining a level of caution and self-restraint concerning certain types of experiments.

Of particular concern are the financial incentives available to bioengineers and their sponsors along with the intellectual property laws that together incent, permit, and protect secrecy in the lab. These practices and laws would seem to collide with the need to adopt an "open source" approach and hold open conversations about the costs, benefits, and risks to society from science that experiments with life's basic building blocks. It would be wise to invite a strong contingent of informed citizens to the table to help ensure a diversity of independent and decentralized perspectives in a conversation about how the risks arising from experiments at the genetic level should be managed.

Bioengineering, especially gene modification represents substantial intervention with the "natural" flow of evolution. Recombinant DNA technology allows scientists to blur the boundaries between species. The current biotechnology, nanotechnology, and robotics developments may be the equivalent of the discovery of fission and fusion. If so, do we run the serious risk of encountering unintended outcomes and unexpected consequences? For example: How should biobenefits be balanced with the risks of bioerror? What do we do about newly created life form rejects? Will the corporate coffers at Novartis, Monsanto, DuPont, Pioneer Hi-Bred, and Dekalb help

us respond and recover from any mistakes they make while experimenting with new forms of plant life? How are the overall costs, benefits, and risks from experiments with life being weighed, and by whom?

The risk to humanity that can be imagined from experimentation with new life forms is chilling. Especially, given the prospect for unintended consequences and the absence of any meaningful regulation over what scientists may be doing. Is it sensible for the world's laboratories to use emerging biological capabilities to pursue profits in an essentially unfettered environment? How should informed public opinion be reflected in the conversation the Asilomar conference initiated? What oversight is or should be in place? What biological tests should be required? What criteria should be met to ensure some reasonable level of security? Should some procedures or materials only be handled or conducted in supervised government labs? Is this a global rather than a national issue? Will the miracles of science really be able to fix any problems created?

Random trial and error with new, possibly toxic life forms is probably a very bad idea. Biotech products are most certainly not like any other product and, hence, should be handled with extraordinary care. Many millions of lives could well hang in the balance. Sir Martin Rees is skeptical, "… by the year 2020 an instance of bioerror or bioterror will have killed a million people."[26]

Another perspective on bioerror is offered by Claire Hope Cummings, a lawyer and environmental journalist:

> There have been only about 10 studies done on human health and GMOs, and half of them indicate reasons for concern, including malformed organs, tumors, and early death in rats.[27]

To further illustrate the potential risk of bioerror, consider the development of "super weeds," herbicide-tolerant plants that are a result of GMO contamination.

> The Union of Concerned Scientists recently reported that the seeds of conventional crops — traditional varieties of corn, soybeans, and canola — are now "pervasively contaminated with low levels of DNA originating from engineered varieties of these crops." One laboratory found transgenic DNA in 83% of the corn, soy, and canola varieties tested.[28]

Again, as with the power-grid, the biotech industry has no watchdog, no accountability structure, and no risk manager. As mentioned, some of this absence of oversight can be explained by a difference in culture. In Europe, where the alarm about GMOs is far greater than it is in the U.S., caution and

regulation are the preferred approach. In America, in line with our preferred practice of compensating victims and suing the guilty, we look to the courts to redress wrongs. Of course, scientists can most probably imagine that they will be able to "fix" any problems that may arise. According to this line of thinking, the biofarmer will be able to apply a biofix should any harm be done. No doubt the biofix will be sold by the same vendor that sold the biofarmer the toxic product initially.

But can GMO pollen be kept on the farm and away from neighboring fields? It is not hard to envision a GMO "Bhopal" (the 1984 gas leak from a Union Carbide plant in India that killed approximately 3800 people and injured many more). We could experience this type of disaster far closer to home — in Indiana and not in some remote part of India. GMO contamination of our food supply strikes a similar profile to other types of pollution, such as air and water, for example. But can it be cleaned up as easily or at all?

The problem, of course, is that we do not know. Transgenic life forms behave in unpredictable ways as do nanosize materials, the very small reductions of existing materials, along with their counterparts, the artificially created "Buckyballs" and Nanotubes. All three are the products of the emerging nanotechnology industry. Nanomaterials are so small — 1 billionth of a meter (one millimeter equals a million nanometers) — that they can easily enter our bodies. "Nanoparticles are too small to be visible to the naked eye; so small, in fact, that one would have to split a human hair 80,000 times before it reached a width of 1 nanometre."[29] Will nanotechnology produce some new form of cancer or other disease? We now have transgenic food crops, trees, fish, and insects. The list is no doubt growing. Just how should these risks be managed?

Exacerbating the problem of this risk is that the technology, like most emerging science with market potential, is ungoverned and it is in the hands of profitseekers who are shielded from precautionary oversight by patents, intellectual property laws, and regulations. Licensing regulations and the threat of legal liability provide protection and promote secrecy that potentially hides information needed to measure and map, model and monitor, and if necessary manage the risks being created knowingly and unknowingly as a by-product of the strategies employed by financially driven business interests.

So, while we imagine how the altered state of living things can provide real value to potential customers, we also need some form of responsible oversight and informed public opinion to help ensure that experimentation at the most basic level of life on Earth does not harm or even extinguish the life it aims to benefit.

We need to add an explicit risk management dimension to our scientific methods so we do not devolve into scientific madness. Certainly, entrepreneurial molecular biology is an expected, even welcomed outcome development. Without risk there is rarely any reward. And who would want to slow

the development of cures for the world's dread diseases? So, a strategy without any risk is not an option. However, before patents are granted to creators of new or modified life forms, effective safeguards should be firmly in place. Is unfettered experimentation with genes, machines, and nanomaterials in the public's best interest? Who is doing the ethical reasoning? Can we imagine the risks involved and at what cost do we fail to do so?

> We are in danger of being severed from our own ancestral lines and diverted into another world altogether, the physical and social dimensions of which are still unknown and yet to be described.[30]

To effectively recognize risk, we need to imagine how a loss might emerge from past, present, or planned activities. This will require an uncommon level of critical, creative thinking, and ethical reasoning. Risk and reward are two sides of the same coin. But, risk to whom? How is cost to be defined and over what period of time? Who should be part of this conversation?

Step (2): *Describe* the Risk

The second step in the RMS involves the description of the risk or potential risk. Transferring the risk from the imagination to language creates meaning, as its fuller dimensions emerge from the conscious and subconscious mind. It also enables conversation and creates a record and documentation for others to see and react to, perhaps, stimulating critical appraisal and greater learning. The expectation is for a conversation so more can be learned about the risk and its potential significance. In this way, we will create a deeper understanding of the risk. Of course, first efforts can create new myths as well, given an absence of durable facts and a deep understanding of the risk.

By describing what might go wrong, how a loss might occur, the risk manager can seek confirmation that loss is likely and intervention possibly desirable. Critical thinkers can also begin to gain insights from others as alternative visions flow from the conversations.

Often, in the early stages of invention and discovery, the potential for loss is apparently not evident, thought to exist, or in any meaningful way understood. Perhaps, persuaded by the benefits that seem both significant and easily within reach, the utility at hand eclipses possible uncertain future perils.

The usual human, cognitive dissonance of bias, particularly, the "overconfidence" bias, the tendency to be more confident than correct, seems to pervade the discussion of risk.[31] In these moments, myths are born and sustained not only by overconfidence, but also by the "confirmation" bias, the tendency to search for and only acknowledge finding the things we are seeking in the first place. Thus, the search for facts dissolves into self-fulfilling prophecy.

Recently, new language has emerged as we learn of new risks, such as West Nile virus, SARS, mad cow disease, chronic wasting disease, and bird flu [A (H5N1)], but our vocabulary, and, therefore, our ability to thoughtfully discuss these diseases is rudimentary. We have not yet developed a very deep understanding of these risks, so we can only refer to them with little more than their labels and the sound bites that are used to announce them on the evening news programs or by news magazines. Until we build at least a basic vocabulary, we will be unable to frame the research questions we will need to answer in order to deepen our understanding and move on through the RMS to containment and, hopefully, cure.

To revisit the earlier example, GMOs like viruses are a form of life, capable of reproduction and mutation — living pollution, in a sense. How can we best describe the implications of these new life forms on our planet's existing species of plant, animal, and insect life as the newly created forms of life combine and recombine randomly in the wild? If the public remains uninformed about the risks as well as the benefits involved, there can be little or no discourse in the public domain about what is in society's best interests. Of course, the organizations that create GMOs will need to meaningfully add "general health and welfare" to their mission statements and strategic value propositions to enter the conversation. Unless and until the Federal Drug Administration or U.S. Department of Agriculture, or World Health Organization (WHO) demands a full description of the risks, as a precondition to doing business, we are likely to experience more myth than morality in the management of GMO risk.

An example of a very useful and effective worldwide conversation about risk is revealed in the story of the rapid discovery of the SARS virus. In February 2003, the world began to hear reports about the emergence of a mysterious respiratory disease in China. Four months earlier, 305 people were reported to have succumbed to a disease that killed five of them. By the time that The Chinese Ministry of Health had finally reported the outbreak to the World Health Organization (WHO), additional reported cases were reported in Hong Kong. The WHO then issued a worldwide SARS warning and travelers to Southeast Asia were dutifully warned. The new disease was flu-like, but it did not appear to be flu. It was, however, extremely contagious, suggesting the need for quarantine. The immediate question to be addressed was what is the source of this new disease? What was quite remarkable, and suggests a useful model, as the world faces increasing numbers of new germs, given our increasingly peripatetic nature, was the global conversation and subsequent collaboration that ensued among the world's laboratories. As described by James Surowiecki in his book, *The Wisdom of Crowds*, within several weeks, 11 research laboratories in 10 countries began the hunt for the cause of SARS. Termed a "collaborative muliticenter research project," the researchers shared

hypotheses, data, findings, and conclusions during daily discussions. Surowiecki's account of this remarkable and perhaps path-breaking story follows:

> Every day the labs took part in daily teleconferences, where they shared their work, discussed avenues for future investigation, and debated current results. On a WHO web site, the labs posted electron-microscope photographs of viruses isolated from SARS victims … Because of the way the collaboration functioned, different labs were able to work at the same time on the same samples, multiplying their speed and effectiveness. By March 21, scientists at Hong Kong University had already isolated a virus that seemed like a likely candidate. That same day, scientists at the Centers for Disease Control in the United States separately isolated a virus that, under the electron microscope, looked like what's called a coronavirus … In early April, monkeys in The Netherlands laboratory came down with full-blown cases of SARS. By April 16, a mere month after their collaboration had begun, the labs were confident enough to announce that the coronavirus did, in fact cause SARS … Ultimately, no one person discovered the cause of SARS … The scope and speed of the SARS research effort made it unique. But in one sense the successful collaboration between the labs was simply an exemplary case of the way modern science gets done … Why do scientists collaborate? ... Collaboration allows scientists to incorporate many different kinds of knowledge, and to do so in an active way (rather than simply learning the information from a book) … Small groups do face tremendous challenges in solving problems and making decisions, and they can waste a great deal of time dividing up the labor, discussing results, and debating conclusions. But those potential costs are clearly, for most scientists, outweighed by the benefits … Scientists who collaborate with each other are more productive … Technology is now making global collaboration not just possible but easy and productive.[32]

Nanotechnology and robotics present similar challenges to risk managers. As scientists seek to explore and exploit these emerging and potentially profitable areas, little is known about what these exciting but potentially lethal technologies, in fact, are capable of doing across our planet. Will nanotechnology be the next asbestosis or worse? Will biotechnology create herbicide resistant weeds or antiviral resistant viruses? Will humanity's last invention be a machine that can think?

We often lack the vocabulary necessary to reasonably describe the risks inherent in scientific innovations. This gap creates difficulties for precautionary thinking. How can risk management keep pace with scientific discovery?

Exploitation appears more rewarding, short term. And then there is the problem of assigning a value to an avoided loss. Do you think this suggests that the scientific method itself may benefit from a sharper focus on risk? Perhaps, the implications of new discoveries should be assessed so humanity is equipped to cope with the possible negative dimensions of an innovation. Stated as an issue, should, for example, nanomaterials or genetically modified products be released into the markets of the world without any oversight or testing of the effects on humans and our environment?

The way that the SARS mystery was solved provides a good example of purposeful, effective dialog among scientists worldwide. Yet, even more familiar perils present problems. As stated earlier, we can predict hurricanes with some precision; yet, we cannot predict where a storm will make landfall. We can describe in some detail how hurricanes work, but we still cannot describe with any precision the hurricane steering mechanism. Thus, we cannot be clear about where they will come ashore. Forecasters simply describe their estimates as falling within a "cone of confidence." Temperatures and wind velocities within the hurricane itself appear to play a significant role, but, of course, more research is required before a more definitive description of how a hurricane actually works can be provided. Given the absence of complete knowledge and given that hurricanes present a climatic mystery, there is an effort to round up the usual suspects, such as "global warming." But, is global warming occurring and does it play a role? If so, is its impact significant? Consider:

> The gold standard of scare stories right now is, of course, global warming, with every sticky summer heat bout or period of mild winter weather initiating a new round of Earth-as-sauna articles and op-eds, quickly erasing the memory of the previous "summer that never was" or this spring's snow storms and ice dams … Many, if not most, of these stories have some factual basis. Often, however, the tone of the headline or the mere positioning of the story on the front page inflates its importance or danger … In real life, the life blood of the global fear trade is the media, which either actively publicize fearful notions or do so inadvertently by their unwillingness or inability to question, fact-check, and qualify. Recession panic, Y2K, global warming, the fears themselves acquire the status of conventional wisdom or self-propagating ideas …[33]

Notwithstanding the possible overstatement of risk in the popular media, within memory, large disasters have occurred without warning and each one enhances our ability to describe risk by raising awareness, creating new vocabulary, causing conversation, and hopefully triggering precautionary measures. In contrast, in 1938, our ability to announce the arrival of a

hurricane, describe its intensity, and understand its origins was considerably underdeveloped.

The Great New England Hurricane of 1938 arrived completely unannounced on the 21st of September, and consequently offered no possibility for evacuation, preparation, or opportunity for protection. According to R.A. Scotti, in his book *Sudden Sea*, the same had been true for a very large storm more than 100 years earlier in September of 1815 suggesting little hurricane risk management progress had been made during that period.

The 1938 storm was a very fast moving storm. It raced up the Atlantic coast at a now estimated mile a minute. "According to the National Oceanic and Atmospheric Administration, it was one of the 10 'storms of the century' and the most violent and destructive natural disaster in New England history."[34] And further:

> Although the sea had been running high and small-craft warnings were in effect, as late as midafternoon there would be no alert that the storm was prowling the coast. Rampaging through seven states in seven hours, it would rip up the famous boardwalk in Atlantic City; flood the Connecticut River Valley and turn downtown Providence into a seventeen foot lake.[35]

With little or no warning there would be no possibility of protecting people or property. Warning can help plans for evacuation and, hopefully, reduce the loss of life and injuries that would otherwise be experienced. Today, with our far better understanding of hurricanes, and equipped with advanced surveillance, and communications systems, we should lose few lives, if any. Our properties and systems should also be adequately protected, to limit to an irreducible minimum, post-loss consequences. Injuries should also be minimal, compared to when tropical storms were less well understood and unannounced in advance of their arrival. Countering, perhaps, even offsetting these benefits is the very large increase in the number of people and properties exposed to loss along the coasts today. With population and property values rising along our coasts, vulnerability to loss has significantly increased since 1938, notwithstanding our enhanced ability to describe the hurricane threat.

Thus, while we can better describe and announce the arrival of a hurricane today, we have more value at risk, so the consequences for property loss are greater. And while some recent research has been done on the construction of hurricane resistant structures by the Institute for Business and Home Safety and the University of Georgia,[36] most coastline structures are highly susceptible to damage by the wind and water a hurricane brings ashore along our coasts. Also, science has yet to learn how to effectively reduce the intensity of a hurricane. Many attempts at weather modification,

including a discontinued military project called "Stormfury," which involved the seeding of hurricanes with silver iodide crystals, have been attempted, but they have not enjoyed much success.[37]

Economic loss is often difficult to calculate in advance or estimate, especially given the many connections and interconnections within our increasingly networked society. Modern economic ecologies are exceptionally complex. As always, pre-loss planners are plagued as well by the usual human biases. Too often, low probability events, those events with which we, by definition have little experience, are regarded as so unlikely as not to deserve any serious attention. This casual thinking is perhaps natural, given wise preparations are likely to be quite difficult and require allocation of scarce resources.

But, the reality is that if a loss event is possible, it is probable. When loss potential involves significant casualties, the destruction of valuable property, or the potential for major disruption, then it demands management attention. But, unfortunately, human nature, being what it is, rarely receives it. Combined with a lack of imagination, our inability to accurately describe risk inhibits our ability to effectively manage it.

Step (3): *Observe* the Risk

Most everyone, if not everyone who witnessed the terrible attacks on September 11 or saw, shortly thereafter, the fear on the faces of those threatened with anthrax or possibly observed the desperation and destruction of hurricane Katrina, cannot easily erase those memories.

Psychologists tell us that what we witness can transform us at some level. We never are quite the same following an exceptionally vivid and perhaps frightening experience. Even though terrorist attacks similar to September 11 had been the subject of many motion picture films prior to the actual attacks on the World Trade Center, the Pentagon, and whatever the target of the airliner that was so bravely countered by the passengers over Pennsylvania, we are riveted by the real thing.

Movies such as: "Executive Decision" (1996) where a plane becomes a weapon; "The Peacemaker" (1997), where the stars deal with a nuclear threat; "The Siege" (1998), involving a terrorist attack in New York City; "True Lies" (1994), depicting detonation of an air-to-air missile to take-out "jihadists," provide not only the imaginative ideas and descriptions of the possible damage terrorists might do, they also produce vivid and persistent images, but they do not motivate much effective action.[38]

The fertile Hollywood imaginations and innovative image producing technologies they use work together to create unforgettable, as well as terrifying movie-going experiences. The thrills they create stimulate and entertain. The images Hollywood creates for us to observe as entertainment might possibly serve to prepare us to manage the risks portrayed, by making them

more "real." Some of us learn best by hearing information, some by seeing images, and some by reading. While all three work together, we each have a preference. The images themselves should help us begin to cope with a dramatized situation, particularly if we are able to think about it, reflect on it, and perhaps discuss our experience with others. For example, Phil Alder Robinson, director of the film, "The Sum of All Fears" (2002), about the detonation of a small nuclear device in a Baltimore sports stadium states, "The film is really about the response to terrorism."[39]

Not surprisingly, Hollywood screenwriters have been tapped, following September 11, by the Department of Defense. The Los Angeles-based Institute for Creative Technologies, a virtual reality military training group was reportedly solicited and agreed "…to assemble a team of screenwriters, directors, and producers to dream up terrorist scenarios for the post 9/11 world."[40]

The benefit of lively imaginations and the disciplines required to create a realistic film combine to offer counterterrorism risk managers a diverse and, therefore, highly valuable if not novel perspective. Of course, screenwriters, unlike risk managers are not required to be more than convincingly creative. Risk in the real world has greater consequences. As decision theorists remind us, however, an abundant flow of diverse, independent, decentralized input is the best route to a wise decision.[41]

The highly creative and talented minds in the film business offer a rich reservoir of ideas for imagining terrorism and many other sources of loss. Their work may help us turn imagined loss events into events we can describe, observe, and hopefully manage effectively.

Even though the events we observe in the movie theater are not "real," they work their way into our conscious and unconscious memories and are available to us. According to psychological research, if an event easily comes to mind, we tend to assume it is common.[42] The opposite is also true. If a "one-in-a-hundred" year catastrophe event is on our risk management list of worrisome perils, we are unlikely to hold an image of this event in our memories. Since we are unlikely to have ever encountered such an event we will probably resist making plans to deal with it. Yet, the risk management imperative urges us to plan for it effectively, even though a loss is extremely improbable.

Because major catastrophes are so rare, they are infrequently described, observed, and experienced, so we tend to underestimate them in several ways. First, we conclude we have better things to do than worry about losses that might be caused by a highly unlikely event. Simply infused with a sense of urgency, and perhaps some hubris, we often choose to ignore low probability events altogether. The opportunity to do something apparently more useful is too tempting to pass up. Second, out-of-sight risks tend to be out of mind as well. But, should the remote risk appear, allegations of negligence and criticism for lack of foresight will flourish.

Insurers, profit-seeking professional risk takers know that highly unlikely events occur. Insurance can be ignored for the more frequent, more predictable losses that can be added to an annual budget and treated like a normal business expense. Small, predictable losses do not require insurance. Large surprises are another matter, however. But how large is large? Losses from the perspective of the insured may not be large to the insurer because insurers pool the premiums of the many to pay the losses of the few. At least that is the theory. Of course, if there were no losses, there would be no premiums and that would be a sad day for insurers, who make a good living functioning as the "condors of commerce." Thus, insurers need to describe infrequently experienced risks to customers in ways that will motivate a sustained sale.

Public policymakers are similarly confronted with the challenging task of convincing a frightened or tax-weary public of the need to react wisely to risk.

For example, nuclear power can appear to be an appealing alternative to power produced by fossil fuels. Why not rely exclusively on nuclear power? It would appear to offer a way to simplify our international relationship strategies. Nuclear power appears to offer a quiet, clean, efficient, relatively inexpensive, non-Middle Eastern source of energy, assuming you can ignore the problem of what to do with the spent fuel and the probability of a very nasty accident.

Again, because the failure of these highly reliable systems is so rare, managers of these facilities think that because they have done a great deal to prevent an accident from occurring, one will not occur. They come to view themselves as highly effective if not invincible risk managers and could underestimate the risks involved.

The largest nuclear accident to date occurred at Chernobyl, near Kiev in the Ukraine, on April 26, 1986. The accidental explosion inside the Soviet reactor set off a fire that burned for 10 days and immediately killed about 6000 people. Today the deaths from the Chernobyl accident continue, as a direct result of the excessive exposure the victims had to radiation. Thyroid cancer is a latent, proximate problem, but places far removed from the Ukraine also have lingering radiation problems. Recently, the British government reported that soil from 355 farms in Wales, 11 in Scotland, and 9 in England are still contaminated with radiation from the Chernobyl accident 20 years earlier. Chernobyl is 1500 miles from Britain. Sheep from these farms have to graze away from these contaminated areas because the grass is so radioactive that the sheep become contaminated too. "Every time we move a sheep or lamb off our land it has got to be scanned," Welsh farmer Edwin Nobel told the London *Independent*. "The experience has made me very opposed to nuclear power."[43]

Graham Allison, a well-respected political scientist, wrote a provocative book in 2004 on what he sees as our greatest risk — nuclear terrorism.

Commenting on the accident in Chernobyl, he observes that the extent of the event is both far reaching and continuing.

> The resulting radiation forced the evacuation and resettlement of over 350,000 people and caused an estimated $300 billion of economic damage, and is likely to lead ultimately to tens of thousands of excess cancer deaths among those exposed to the fallout.[44]

The worst nuclear accident, so far, in the U.S. occurred on March 28, 1979 at the Three Mile Island (TMI) power plant in Pennsylvania. This arresting event put a chill on the expansion of nuclear power in the U.S. No one was immediately killed as a result of this event, but it caught the attention and imagination of the nation. It was universally observed as a vivid reminder of the mysterious and deadly dangers represented by the technology that destroyed the Japanese cities of Hiroshima and Nagasaki in 1945. Atom smashing releases a large amount of energy randomly. It also creates dangerous pollution that lasts for eons.

The faster we can recall an event and the more vivid that recollection, the more we expect that it will reoccur. Psychologists refer to this thinking trap as the "availability heuristic." It is set off when we reach conclusions based largely on information in our memories. But, unfortunately, it turns out that our memories are often very poor. They are limited in terms of their scope of experience and in their fidelity to the facts. Following the Chernobyl and TMI accidents, and the ready availability of these memories, we now have a more favorable view of coal-fired, steam-generating power plants. Yet, coal can present its own side effects in terms of its impact on the environment. It seems, at the moment, there is no perfect solution for meeting our energy needs. The recollection of these observed and experienced events will significantly complicate any future initiative to expand the use of nuclear power, as will the problems of waste or spent fuel disposal and the potential use of a power program for the inadvertent or intentional production of nuclear weapons. New answers are needed to effectively manage the risks inherent in the generation of nuclear power.

Less well observed and documented, at this point, but nevertheless still top-of-mind with some, is the risk of global warming. Is human activity, especially the burning of fossil fuels increasing global temperatures to our long-term detriment or are we simply observing the effects of a long-term, natural change in the planets temperature cycle?

Many fear the effects of global warming as our planet appears to heat up. Actually, we can observe some of the early clues that global warming is occurring in environmental changes all around us. Plants flower sooner, migration times change, diseases spread, amphibians disappear, coastlines

erode, and exotic species appear, apparently as carbon dioxide levels rise. Meanwhile, mercury levels climb, wildfires increase, hillsides liquefy, oceans warm, ice shelves collapse, glaciers shrink, sea levels rise, droughts linger, and seasonal changes vary unexpectedly.

These and other "geo-signs" and "eco-signs" are available to the observant eye. They are signs from the Earth that our planet is entering a warmer period. "Globally, temperatures are up 1 degree Fahrenheit over the past century, but some of the coldest, most remote spots have warmed much more … The changes are happening largely out of sight. But they shouldn't be out of mind because they are omens …"[45]

There is a lively debate about the question of global warming, both about its existence and what, if anything, should be done about it, assuming anything can be done at this point.

> Climate fluctuates naturally between warm and cool periods. But the 20th century has seen the greatest warming in at least a 1000 years, and natural forces can't account for it all. The rise in CO_2 and other heat-trapping gases in the atmosphere has contributed; both greenhouse gases and temperature are expected to continue rising. The Arctic is warming several times faster than most of the planet; ice there is melting on land and sea. The release of fresh water into the oceans could change the course of currents that play a vital role in climate. Runoff from glaciers on land is already contributing to a global rise in sea level. In the next century some coast lines could migrate miles inland, displacing tens of millions of people. Siberia and northern Canada could experience a warmer climate. Other regions could suffer more frequent and severe droughts. Taking steps now to rein in greenhouse gas emissions could limit these impacts. Lonnie Thompson of Ohio State University, (has collected) ice cores from Peru's Quelccaya ice cap, which is retreating 40 times faster today than in the 1960s. Thompson's freezer may soon contain the sole remains of tropical glaciers from around the world, including the famed snows of Mount Kilimanjaro, which could vanish in 15 years. "What glaciers are telling us," says Thompson, "is that it's warmer now than it has been in the last 2000 years over the vast areas of the planet.[46]

Imagination, combined with the ability to observe, can create powerful impressions and memories. But is the risk real? When it comes to our perception of risk, we tend to react intuitively. Psychologists can help us understand why we tend to routinely misestimate risk. Why do we, for example, spend hundreds of billions of dollars on prevention and protection, create a new presidential cabinet-level bureaucracy and challenge the limits of every

citizen's liberties following the fatality of 2880 souls on September 11, when many more (about 45000) people die on our roadways each year? Why do we fear for our security more than for our safety and health? It appears that we plainly fear unexpected attacks of violence far more than accidents that threaten our safety every day. When it comes to the risk of injury or death, we tend to care how it happens. But, why is this the case?

According to psychological research, the answer may lie in part in our past. Our memories and unconscious minds are survivors of a risk-riddled past. For example, we appear to be programmed for fear of high and confined places, so we tend to fear flying, which offers both. While some of us hunt with firearms, ski down precipitous slopes, smoke cigarettes, pilot small planes, climb sheer cliffs, and ride motorcycles for fun, others would see these pursuits as highly risky and avoid them. The more familiar we are, the more skilled we are, the more we feel in control of the hazards involved, and, therefore, the less risk we perceive. And, in fact, in some cases, the risk is likely to be less for the more capable practitioner. We fear what we cannot control or appear to control. We also may be more willing to assume risk we voluntarily undertake. The fault, if any, will be ours when we assume the risks willingly. We appear to calculate a rough cost/benefit analysis hoping to balance the joy from the thrills with the risks that result.

Paul Slovic, president of decision research and professor of psychology at the University of Oregon,[47] has researched questions of risk perception extensively. He has developed a useful framework for describing how and perhaps why rational people observe similar risks very differently. The fact that we do view risks differently is particularly useful in the operation of risk markets. Buyers and sellers of futures contracts, for example, need to see the risks involved in the transaction differently if they are to do business together. This is the basis of speculative risk. Similarly, risk to a property owner is whether or not a loss occurs. This is pure risk. Risk to the insurer of that same property is whether or not the pool of premiums collected from this and many similar property owners will be sufficient to pay the few losses incurred on the overall book of business and provide a small profit. This is speculative risk. Thus, the act of insuring a risk, converts it from pure to speculative. Consequently, insurers do not worry about any one loss. Their focus is on the aggregate book of business. Indeed, as an insurance adage notes, if there were no losses, there would be no premiums and that would be a bad day for insurers. Conversely, the property owner is primarily worried about avoiding loss to the owned property. The different perspectives meet in the marketplace and achieve a reasonable balance among the costs, benefits, and risks involved for both parties to the transaction when they agree to the risk transfer price or premium the insurer charges and the property owner agrees to pay.

Slovic developed a model that describes nine different characteristics of risk perception. It provides a useful framework for thinking about why we

tend to perceive similar risks differently. Slovic's nine pairs of risk perception characteristics include:

1. Voluntary–involuntary
2. Delayed–immediate
3. Known to be exposed–not known to be exposed
4. Known to science–not known to science
5. Controllable–not controllable
6. Old–new
7. Chronic–catastrophic
8. Common–dread
9. Certainly not fatal–certainly fatal

Without question, we perceive and consequently act differently when confronted with risks we think are more accurately described by the left side of Slovic's list. For example, most people fear immediate losses far more than losses that have a delayed impact. Teenagers, for example, tend to feel invincible. The future seems so far away. They have observed little of our world during these early years, compared to how we feel and what we learn as the decades pass. Hence, fast driving, substance abuse, smoking, and other risky pursuits are part, perhaps, of living and learning. Experiencing what life has to offer, without the learned, measured, skeptical, cautious, precautionary response that is the product of accumulated experience is to live a dangerous and, probably, unnecessarily short life. To paraphrase test pilot Chuck "The Right Stuff" Yeager, "There are old pilots and there are bold pilots, but there are no old, bold pilots."

The risks we tend to highly fear are the vivid risks we can best remember. The images of the plane crashes from September 11 are not difficult to bring into sharp focus in our minds eye. The news media played the film over and over and over again, imprinting the horrible images in our minds. Hence, at the moment, we have a major fear of terrorism. This fear has triggered a massive allocation of national attention and resources to terrorism prevention and, therefore, vastly improved our attention to national security protection.

But what about more ordinary perils? They are out of sight so they are also, for the most part, out of mind. For example, flu kills about 36,000 people annually, in the U.S.,[48] but we do not as a nation take much notice of these deaths. Similarly, because we spend countless hours safely on the road, the 45,000 or so people who die on the U.S. roadways each year are, for most just "statistics," not vivid, observed images or part of our accumulated personal experience. As largely unobserved events, these tragic deaths, like the damage to the environment by greenhouse gases, are not in the foreground of our view, so we tend to treat these risks as if they were nonexistent. The result is

that these risks remain, largely unmanaged or managed as a low-level national priority, given our country's current, predominant worldview.

If we can imagine a risk, describe it, and observe it, perhaps we might be able to measure it. Meaningful measurement would not only provide some way of prioritizing the allocation of assets, but also suggest ways to pace risk management progress.

Step (4): *Measurement*

The fourth step in the RMS focuses on the role of numbers in the assessment and management of risk. Both of the fundamental logics that define risk (the logic of chance and the logic of loss) depend heavily on the ability to quantify some relevant aspect of risk. The purpose of risk quantification is to determine and to describe the truth of risk.

Measures size the risk and are a dimensional representation or reflection, however, remote and inexact, of risk. Risk measures are for the most part intangible abstractions; shadows of reality. Notwithstanding their elusive, ephemeral, and enigmatic nature, measures are useful because they enable and empower inquiry and inference, which is the purpose of the two fundamental logics of risk. Numbers and their tendency toward precision promote a deeper level of understanding than would otherwise most likely be achieved. Risk measures enable us to imagine, describe, and observe risk in a more orderly way than would be possible without them.

Measures are of several types: internal and external, quantitative and qualitative, financial and nonfinancial, short term and long term, and so on. An important point to keep in mind in any discussion of numbers is that they are often based on broad assumptions so they are not so important for what they say, but for their acceptance. James G. March, a noted professor of international management, political science, and sociology at Stamford University, makes this point in the following way: "The validity of a number may be less important than its acceptance, and decision makers may be willing to forego insisting on either technical correctness or immediate political advantage in order to sustain social agreement."[49]

The measures that have been used to measure and communicate levels of risk are closely tied to a particular threat or peril. For example, in the U.S., we are alerted to the level of terror threat by a color code. Yellow, the color at the moment, stands for a significant risk of terrorist attack. According to The Department of Homeland Security, "The country remains at an elevated risk, Code Yellow for terrorist attack."[50] The colors used by The Department of Homeland Security range from green for low risk to red signifying severe risk.

Earthquakes are measured using the Richter scale. This approach was developed by Charles Richter of the California Institute of Technology in 1935 as a quantitative, mathematical approach for comparing earthquakes.

This measure compares earthquakes based on their magnitude. According to the U.S. Geological Service, "The magnitude of an earthquake is determined from the logarithm of the amplitude of waves recorded by seismographs. Earthquakes assigned a value of 2.0 or lower on the Richter scale are termed 'micro-quakes' and are not usually felt. Quakes causing major damage score at 8.0 or higher on this unlimited scale."[51] The Richter scale is an example of a quantitative scale as it is based on careful measurements.

A different, qualitative scale is also used to measure earthquakes. This measure is called the *Modified Mercalli Intensity Scale*, developed in 1931 by Harry Wood and Frank Neumann. The scale uses 12 increasing levels of intensity that range from imperceptible shaking to catastrophic destruction. The levels are designated by Roman numerals. The Mercalli Scale does not have a mathematical basis; instead, its rankings are based on observations of damage intensity. The Mercalli rankings range from not felt to total damage with objects tossed into the air.

A system similar to the Richter Scale is used to measure hurricanes. Hurricane intensity is measured with the *Saffir-Simpson Scale*. It ranks hurricanes on a scale from Category 1 (74 mph) to Category 5 (156 mph or higher). Category 1 storms cause minimal damage and have storm surges from 3 to 5 feet. Category 5 storms cause catastrophic damage and bring storm surges 19 feet and higher. Hurricane Camille (1969) and Andrew (1992) were Category 5 storms, as was Katrina (2005), the day before it made landfall in Louisiana.

Hurricane is the name assigned to strong tropical cyclones that occur in the North Atlantic Ocean as well as several other oceans. Cyclones exist in many parts of the world, but these large windstorms have different names, depending on the region in which they occur. The names vary as follows:

- "*Hurricane*" (the North Atlantic Ocean, the Northeast Pacific Ocean east of the dateline, or the South Pacific Ocean east of 160E)
- "*Typhoon*" (the Northwest Pacific Ocean west of the dateline)
- "*Severe tropical storm*" (the Southwest Pacific Ocean west of 160E or Southeast Indian Ocean east of 90E)
- "*Severe cyclonic storm*" (the North Indian Ocean)
- "*Tropical cyclone*" (the Southwest Indian Ocean)[52]

Storms are given names once their wind speeds exceed 39 mph. If they reach or exceed 74 mph, they are then referred to as one of the types listed above. The names are specific to the particular region in which they reach the defined intensity.

Tornados are another very troublesome windstorm and they are often associated with hurricanes. These violent storms are characterized by one or more large, black, twisting, noisy, and ground-touching clouds. Tornados are caused when warm air and cool air collide, forcing the warm air to rise very

rapidly. When this happens, they become unpredictable. Tornado wind speeds can exceed 300 mph, so they are very dangerous and extraordinarily destructive.

Tornado intensity is measured on the *Fujita-Pearson Scale*. This scale ranges from F-0: 40 to 72 mph, "Minimal Damage" (chimney damage, tree branches broken) to F-5: 261 to 318 mph, "Incredible damage" (homes lifted off foundations and carried considerable distances, autos tossed as far as 100 meters). These storms are usually very fast moving, localized, unpredictable, and incredibly destructive, so there is no highly reliable way, at this time, to measure their magnitude and intensity. In 1971, a meteorologist named Theodore Fujita developed the Fujita Scale to assist with the rough measurement and comparison of these ferocious storms. Like the Mercalli hurricane scale, the Fujita Scale is a qualitative measure based on visual impressions of the damage caused and not on scientific measurement.[53]

Even asteroid threats and threats from other NEOs have a scale for measuring their consequences. The *Torino Scale* and the more refined *Palermo Scale* are currently used for this purpose. The Torino Scale was developed in 1999, at a workshop in that Italian city. The scale uses the now familiar numbering system along with colors to designate the threat levels predicted. The scale is based on a complicated formula that takes into account the trajectory of the NEO and the path of the Earth. It addresses the likelihood of a collision with the Earth. The scale ranges from zero for "Events having no likely consequences for us here on Earth" to 10 for collisions capable of causing a global climatic catastrophe. Torino ratings of 8 or above indicate "Certain Collisions." The color white means "No Hazard;" green, "Normal;" yellow, "Meriting attention by astronomers;" orange, "Threatening;" and the color red, is used for categories 8, 9, and 10, implying "Certain Collisions" with the Earth.[54]

Flood ratings, annual rainfall, snow accumulations, credit and insurance scores, unemployment levels, inflation and other measures are frequently used for imagining, discussing, observing, and measuring levels of risk. Measures are the language of risk. They are useful for pursuing, understanding, and deriving the likely meaning of a particular risk. The measurement systems for calibrating risk and the measures themselves are constantly being improved. For example, ground-penetrating radar (GPR) is now being used by the USGS to quickly determine flood level discharges in unstable stream channels. This information can help promote downstream evacuation, when threatening conditions arise. With GPR, measurements are not only fast, but no instruments need be installed in the stream channel, as GPR antennae can be attached to bridges and across a waterway making measurement and early warning feasible and effective.[55]

Volcanoes, another important and ancient natural peril, like earthquakes, tornados, and most floods, give little warning about when they will erupt. Scientists have discovered that volcanoes do show at least three signs of

increasing activity that an eruption is likely to occur. They monitor these signs using a variety of techniques. The approaches used are focused on detecting and measuring the movement of magma beneath the volcano. "Rising magma typically will (1) trigger swarms of earthquakes and other types of seismic events, (2) cause swelling or subsidence of a volcano's summit or flanks, and (3) lead to the release of volcanic gases from the ground and vents. By monitoring these phenomena, scientists are sometimes able to anticipate events like explosive eruptions and lahars."[56] A lahar is a mudflow or landslide that flows down the sides of a volcano.

Volcano monitoring techniques include: remote sensing from satellites, ground deformation measurements, geophysical measurements, hydrology, gas emission testing, and seismic measures. Currently there are four volcano observatories. They are located in: Fairbanks, AK; on the island of Hawaii; Vancouver, WA; and in Menlo Park, CA.[57] These observatories work with universities and other organizations for the purpose of monitoring and reducing the volcano risk. The aim, as with each of the major natural threats, is to avoid being caught by surprise so evacuation and other emergency preparations can be activated.

Risk information vacuums fill rapidly. Without quantitative information, myths are often created to explain risk. Myths, as near truths, can actually be useful for initiating the explanation of the apparently inexplicable. When we simply do not know, we imagine, speak, and think we see explanations for mysterious events. We use our big brains to invent reasons, causes, correlations, values, and, often colorful, entertaining implications and inferences. By articulating what might be happening, myths can put the scientific method in motion and start the process of unraveling what, in fact, is happening, leading perhaps to deeper levels of understanding. Separating the wheat from the chaff is the research task, in the search for the truth of risk. But, myth can also inhibit progress.

Interestingly, myth has played an important inhibiting role in the pace of development of the math of chance. Surprisingly, the ancient Greeks did not discover, develop, and deploy probability theory — the core concept underlying the logic of chance. They appear well disposed to have done so, however, if they wished. They were enthralled with numbers, logic, geometry, proofs, and by far favored facts over feelings. So why did they avoid exploration of the concept of probability? Their powerful belief in the mythological origins of the universe and humanity played a major role. Also, they held a rather fatalistic worldview. Since fatalists think of nature as essentially capricious, they do not bother with making plans or estimating the chance of future failure or success.[58] Human fates and fortunes were written in the stars and were in the hands of indifferent gods.

As beliefs tend to drive behaviors and behaviors produce results, the pace of risk management progress would have been more brisk had the ancient Greeks

taken a greater interest in probability theory and statistics — more motivated toward measurement and less bound to mythological belief.[59] The ancient Greek world was ruled by capricious, tricky, self-centered gods who did not maintain a very strong and sustained concern for humans. Thus, there was little if any incentive for the Greeks who held this fatalistic worldview to predict the future. Humans were allowed choices by the gods, but often chose poorly.

Conceptually, these ancient thinkers were very close to discovering the theory of probability. In fact, Socrates defined the word "eikos," which means plausible or probable, as "likeness to truth."[60] Their conceptual proximity, however, did not yield much real insight and consequent progress in the measurement of risk.

It was not until thousands of years passed during the "Age of Enlightenment" that the search for knowledge about many things, including the future, was ignited. By the 17th century, the time had come for humans to think more carefully and explore the world around them with more active curiosity. During this period, people were increasingly less inclined to believe in myths or in the infallibility of the church in Rome. It was a time of robust critical and creative thinking and ethical reasoning — a time when humans were well disposed to take matters, any matter into their own hands.

In the 1600s, people in general (and mathematicians were no exception) became fascinated with gambling and the speculative risks these games produced. This was a fertile intellectual era. It was in this environment that the math of chance was born.

As Peter Bernstein relates in his excellent history of risk, *Against the Gods,* Thomas Gataker, a Puritan minister, signaled the beginning of the era, in 1619, when he published, *Of the Nature and Use of Lots*, arguing in harmony with the tenor of his times, that natural law, not divine law determined outcomes of gambling games. Along with many other areas of thought, the math of chance made sweeping advances during the Age of Enlightenment. The unbridled search for knowledge, truth, and perfection, at this point in human history laid the foundations for the Declaration of Independence of the 13 colonies from Britain as well as the U.S. Constitution and countless other advancements.

The origin of the math of chance in the 17th century was based on discoveries made by a number of the period's thought-leaders including: Galileo (1564–1642), Pascal (1623–1662), Fermat (1601–1665), and deMoivre (1667–1754). The basic theory of probability came about as the result of an effective collaboration between Chevalier de Mere, a gambler, and Blaise Pascal who was, among other things a mathematician.

In 1654, de Mere was seeking an answer to how the pot from an unfinished game of *balla*, a popular gambling game at the time, should be divided between the two players, when one of the players was ahead. The problem was not a new one. It had been posed 200 years earlier by a monk named

Luca Paccioli and was unsolved. de Mere challenged Pascal for a solution. Pascal, in turn, enlisted the assistance of his friend, Pierre de Fermat. Together, they then developed, as their correspondence revealed, a solution to the distribution of the partially finished game and, as they did, they developed the basic rules of probability theory.

The significance of this development is that it was now demonstrably possible to look sensibly and systematically by means of reason and logic into the uncertain future and draw conclusions with assurance about what was likely to happen. "Their solution to Paccioli's puzzle meant that people for the first time could make decisions and forecast the future with the help of numbers."[61]

Probability theory is the keystone of risk management. Risk management decisions must be made in the present in preparation for an uncertain and unknowable future. More losses can happen in the future than will happen. Many losses are possible, but some are more probable than others. As we cannot know the future and we need to make decisions now about that uncertain future, the theory of probability can be a useful aid for determining what we might do now so we are reasonably prepared to cope with nature and the world's evils.

Probability enables us to bring structure to the organization of past events and using the rules that Fermat and Pascal gave us, apply logic to make reasoned statements about the future.

> A probability is a quantitative measure of the likelihood of a given event. If we are sure that an event will occur, we assign it a one hundred percent probability. If we are sure an event will not occur, we assign it a probability of zero percent.[62]

Of course, decision makers have been getting risk wrong for as long as decisions have been made. Notwithstanding this history and because the future is not exactly like the past and cannot with absolute certainty be predicted, some theorists, referred to as "subjectivists," have argued that probability does not exist. This "all or nothing" argument asserts that because risk and its main measures that are based on probability theory are both so reflexive and so subjective, they inherit all the vagaries of human perception and mental imperfection. Therefore, the concepts of risk and probability are of little or no operational or practical use. Consider one argument representative of this view:

> **PROBABILITY DOES NOT EXIST**
>
> The abandonment of superstitious beliefs about the existence of Phlogiston, the Cosmic Ether, Absolute Space and Time, … or Fairies and Witches, was an essential step along the road to scientific

> thinking. Probability too, if regarded as something endowed with some kind of objective existence, is no less a misleading misconception, an illusory attempt to exteriorize or materialize our true probabilistic beliefs.[63]

Building on the notion that probabilities are so uncertain and so subjective that they are little more than mental fiction, a simple state of mind, and therefore unknowable in any useful, objective sense, subjectivists reason that it is impossible to define risk in any meaningful way. This reasoned absence of any useful operational benefit leads the subjectivist to the conclusion that there is no such thing as "true risk."[64]

Risk then, as we nominally know and use the term *danger, hazard, exposure to mischance or peril*, becomes, in the subjectivists argument, unknowable, unmeasurable in a precise way, and, hence, nonexistent. But, we do not need precise measurement to find the concept of risk and probability measures useful. Consider this view. "Risk … embodies the concepts of probability and magnitude found in the quantified 'scientific' definitions of risk, but does not insist that they be precisely knowable. If one retreats from the unattainable aspiration of precise quantification, one may find, I believe, some useful aids for navigating the sea of uncertainty."[65]

As sailors do not need to understand all there is to know about sea breezes to sail a winning race, risk managers can usefully apply measurement concepts to risk assessment and management, absent exacting computation.

The engineering discipline of systems safety provides an example. At the dawn of the space age in the 1960s, most aviation technologies were developed using "trial and error" approaches — a "fly it and fix it" approach. Given the high cost of the space rockets and intercontinental ballistic missiles (ICBMs), engineers needed a more economical and practical approach to identifying and solving spaceflight problems and testing new ideas.

At the core of the systems safety approach is simulation. A hypothetical diagram of the system to be tested is drawn or developed that includes system component failure probability data. Various analyses are carried out, including "fault tree analysis," "failure mode and effect analysis," and others. These data-intensive simulations are intended to provide systems designers with significant understanding of the overall systems reliability at the component and subsystem level. Their purpose is to simulate a flight statistically, so the rocket can be designed to fly safely or at the very least "fail safely." The objective is to use these simulations to identify and quantify the possible failures and seek ways to avoid or eliminate them without extensive, expensive testing.

For example, if we knew the probability of failure of an "O" ring used to seal sections of a rocket booster at certain temperatures, we might calculate the chance of launch failure. *Challenger* space shuttle engineers at NASA did

these calculations and system failure estimates. Launch at temperatures below 54 F was "…not in the direction of goodness." But sadly, management judgments, in this case, overrode engineering discipline, dooming the *Challenger* and its crew when the launch at near freezing temperatures was authorized. As this sad episode illustrates, more than measures are needed to reach a wise risk management decision.

Examination of the decision making around the reentry of the *Columbia* Shuttle in January 2003 suggests a similar disregard for measured input from NASA engineers. The engineers in this case were asked to carry out a "crater analysis" to determine the likely impact of the 1.67 pound piece of foam that struck the leading edge of the Shuttle's left wing at takeoff. However, after their analysis and evaluations were concluded, they could not assure Linda Ham, the Mission Management Team leader, that critical damage had not occurred. Why? "… the Crater algorithm they were using had been designed to measure the impact of pieces of debris hundreds of times smaller than the one that hit the Columbia, so there was no way to be sure that its results were accurate. The engineers focused on how uncertain their analysis was, but NASA management focused instead on their conclusion."[66] Finding the right tool for measuring risk can present a significant challenge and ultimately present a formidable obstacle for reducing risks of loss.

Often, precise estimates cannot be calculated, but reasonable approximations of system failures can be determined. In the end, of course, human judgment is an absolute necessity for the accurate assessment of risk. The assimilation of the nonquantifiable variables is an essential complement to the variables that lend themselves to quantification. Both must be blended and weighed to reach a smart decision.

The skills required to apply system safety techniques, along with the data needed to determine the failure rates of the millions of components that comprise space shuttles, present the systems safety engineer with an extreme if not entirely overwhelming challenge. But, thankfully, useful techniques exist to help fill information gaps and improve the quality of challenging estimation problems.

For example, when measures are entirely elusive, risks can often be assessed using the Delphi Method.[67] First conceived in 1944 by RAND and then refined into a workable method in the 1950s and 1960s, the method involves polling anonymous panels of knowledgeable, informed experts. It gathers the opinions from these experts as a way of securing the best possible estimate from a diverse group of independent, decentralized sources. The main use of this approach is for gathering information needed to guide judgments when the facts required are few or do not exist. The Delphi method systematically gathers the diverse opinions through a series of rounds, often three, as the panels respond to a structured questionnaire or survey. Between rounds, the panels are given the aggregate responses of the group as feedback.

The rounds can continue until the opinions converge on an alternative that appears as the best solution to the problem. The consensus of the group is selected as the "best" answer available. As ever, errors will occur, since no one can know the future. But the Delphi method can be a useful decision aid when statistical data is unavailable, given the novelty of the situation being examined.

Another useful approach for making decisions under conditions of uncertainty is found in the application of Bayes' Theorem. This approach, first articulated by an Anglican minister, Thomas Bayes, in 1761, mixes new information about an event with existing information to refine initial expectations. It provides a mathematical way of supplementing intuition about the odds of an event or scenario with actual information. Bayes' Theorem proved useful to the navy in its search for the U.S. *Scorpion,* a submarine that sank in May 1965 and was inexplicably lost in the North Atlantic. By creating and selecting a series of scenarios and enlisting a panel of independent experts, the lost submarine was located 220 yards from where the group thought it would be. Interestingly, no one member of the group picked the spot, but the group as a whole was quite accurate. According to an account of this episode described in James Surowiecki's book, *The Wisdom of Crowds:*

> What's astonishing about this story is that the evidence that the group was relying on in this case amounted to almost nothing. It was really just tiny scraps of data. No one knew why the submarine sank, no one had any idea how fast it was traveling or how steeply it fell to the ocean floor. And yet even though no one in the group knew any of these things, the group as a whole knew them all.[68]

Risk management decisions are almost always made in a murky mist of uncertainty. When actually attempting to measure risk, it is sobering and perhaps therapeutic to revisit several cautionary comments made when probability theory was being created. In an exchange of correspondence, as described by Peter Bernstein in *Against The Gods,* Gottfried von Leibniz's wrote to his friend Jacob Bernoulli, a Swiss mathematician and member of a famous family of mathematicians. Bernoulli had observed that since we can know the odds or chance of tossing a five rather than a three with a pair of dice, we should also be able to know the chance that a man of 20 will outlive a man of 60. "Might we not, he asks, find the answer to this question by examining a large number of pairs of men of each age?"[69]

Leibniz's answer is worth remembering. "[N]ature has established patterns originating in the return of events, but only for the most part."[70]

The logic of chance is like a triptych, with three mirrors: one reflecting, however, dimly the past, another the brief present, while the other peers into

the fog of a dreamlike, unknowable future. We can use probability theory to learn something about the future, but we can only learn in part.

Step (5): *Mapping and Modeling*

The aim of the fifth step in the RMS is an attempt to deepen our understanding of a risk by applying what we have learned about risk so far to construct a map and model of how a risk is created and how it causes loss. This can be done by mapping and, when possible, modeling the risk. If risk can be envisioned, described, observed, and measured, we should be able to develop a map or perhaps even a model of how the risk causes loss under a variety of critical conditions.

The purpose of this fifth step in the RMS is to display the relationships between risk characteristics. Our purpose is to identify and gain a workable understanding of any cause and effect relationships that may emerge. Correlations between one risk element and another may be revealed. We are looking for greater clarity about how a risk emerges, behaves, and causes loss. Benefits will emerge, once we have gained some understanding of a risk to the point where we are able to take its measure. We should then be able to draw at least a one-dimensional representation or map of the risk. We may also be able to learn enough to draw or diagram a multiple dimensional representation or dynamic model of the risk as well. The aim is to make connections between cause and effect and between the origin of a risk and its impact.

Drawings, flow charts, matrices, Venn diagrams, logic trees, and other visual representations of the risk can be helpful analytical aids to risk management problem solvers and decision makers. It is often elucidating to visualize a complex problem as an important step toward solving it. Maps and dynamic, multidimensional models can also be useful communication and teaching aids. When we can understand a risk well enough to map and model it, we should be able to monitor it and perhaps manage and possibly mitigate it. In this way, risk prediction and loss prevention and mitigation will save lives and preserve the utility of tangible and intangible assets.

To systematically assess risk, data and some sense of context to work with as inputs are required to map and model the potential loss. Timing is important as well. For example, early maps of the World show North America as a shape with only a vague relationship to how we now know it to be. Geologists inform us that long ago, there was just one continent — Pangaea, a supercontinent that combined all the Earth's continents. This was before life on Earth began to diversify, before the Triassic Period, before the NEO created the Chicxulub crater.

As explorers began to visit North America, the details became clearer and could be reflected on increasingly accurate maps. Today, with the help of satellites that offer a highly accurate view of Earth, very detailed topographical map books have been created. Also, for less than $150, we can purchase mapping software that uses the Global Positioning System, a network of satellites that send signals to Earth, enabling precise location. All this capability can be made very portable using a wireless Bluetooth-equipped laptop computer or even smaller devices, such as a personal data assistant or even a mobile telephone.

Integration of measuring, mapping, and modeling capabilities represents considerable progress. It is propelled by our inexorable scientific curiosity and enabled by scientific innovation. Similar patterns of progress can be evident in the management of risk as well. Recall again that in 1938, we had absolutely no warning of the killer hurricane's approach. Today, with days of prior notice, technology has substantially enhanced our capacity to predict advancing threats from many natural perils.

Long before it struck, hurricane Katrina was identified as a low-pressure area off the coast of Africa.[71] Its track was then mapped for 11 days as it made its way eastward across the southern Atlantic. On August 23, 2005, the National Weather Service gave the low-pressure disturbance a name: Tropical Depression #12. Warm ocean waters over 82 degrees and winds fed the growing storm. Winds exceeded 35 mph. Forward speed was 7 mph. Satellites and specialized aircraft mapped its every move. One hundred and thirty-five miles east of the Florida coast, Tropical Depression #12 earned a new name as her wind speeds exceeded 45 mph. She was now to be known as "Katrina." With winds extending outward for 70 miles, Katrina was becoming a storm worth watching.

On August 25, Florida's southeast coast and west coast received notice of a "hurricane watch." At 5:00 p.m., (EDT), sustained winds reached 75 mph, extending for 15 miles. Katrina now was classified as a Category 1 hurricane. The storm then reached the Florida coast on August 25 with winds clocked at 80 mph. The storm surge was up to 4 feet. As a Category 1 storm, no real damage was expected.

Weakening over Florida, Katrina entered the unusually warm waters of the Gulf of Mexico. Recharging its winds over the warm Gulf waters, Katrina headed toward Louisiana and Mississippi. The Gulf's warm waters elevated Katrina to a Category 5 storm with winds up to 175 mph.

On Sunday, August 28, the storm was now 1000 miles across and indications were it would produce a 28-foot storm surge, or wall of water, as it came ashore, creating not only a threat of wind damage but of substantial flooding and pollution as well, given all the petroleum and chemical facilities in its path. Katrina was now on a direct path toward New Orleans — a very

vulnerable city, but one that had not experienced a hurricane in 40 years. The mayor of New Orleans then ordered the first-ever evacuation of the city. Katrina made landfall about 7:00 a.m., (EDT), on the 29th as a 135 mph Category 4 hurricane, heading straight north and then weakening over Mississippi to a tropical storm. Katrina and the subsequent flooding caused about 1300 fatalities and billions of dollars of damage. Estimates at this time exceed $100 billion, but the eventual costs and consequences are certain to be higher.

Unlike the 1938 hurricane 67 years earlier, Katrina's every move was closely tracked — observed, measured, mapped, and modeled. Unfortunately, the response to this well-announced hurricane and the easily anticipated threat it represented was ineffective for far too many. Poor judgment can easily trump good information in the absence of sound risk management and result in avoidable death and destruction.

Hurricanes also threaten other U.S. cities and coastal areas. "According to longtime NOAA meteorologist Joseph Golden, the five places in the U.S. at greatest risk for calamitous hurricanes are: Tampa Bay, FL; Mobile, AL; Houston, TX; New York City and Long Island, NY; and Miami, FL. More than 23 million Americans live in areas where a hurricane catastrophe is not an 'if' but a 'when.'"[72] Additional areas in the U.S. threatened by catastrophic risk include: earthquake-threatened areas in the San Andreas Fault in California and the New Madrid Fault zones in southern Illinois, as well as "tornado alley" in Oklahoma. Terrorism could hit just about anywhere, as could bio-error and impact with an NEO.

Building a "dynamic map" or model requires an ever deeper understanding of risk so the risk, hopefully, can be managed. This concept applies to all perils and threats. For example, just as counterterrorism professionals build "threat models" to help plan, prepare, prevent, and protect population centers and our critically valuable infrastructure from terror threats, insurers build windstorm models to help ensure the availability of sufficient funds following a large hurricane or other insured natural disaster. These models also assist clear and convincing communication with citizens, the Congress, regulatory agencies, financial rating agencies, investors, and other stakeholders.

Modeling, by representing many simultaneous and sequential variables, helps simulate how loss frequency and severity occurs. Using real data, from prior events or inputting plausible but not experienced loss dimensions, planners and risk managers can better prepare to cope with actual, serious emergencies.

Maps are useful for tracking storms and informing builders, for example, about the location of fault lines where earthquakes could occur. However, maps stop short of simulating how the various conditions that could cause a loss arise and how loss prevention actions might assist.

For example, the floodwalls designed to contain Lake Pontchartrain failed during Hurricane Katrina. Countless gallons of water flooded over 80% of New Orleans, a city with areas over 8 feet below sea level.

> From Louisiana to Florida more than 90,000 square miles were declared a disaster area … Roughly eighty percent of the city's 450,000 residents fled before the storm hit. Those left behind lacked the resources needed to leave, or defiantly opted to stay. Thousands may have died making Katrina one of the deadliest U.S. natural disasters on record.[73]

Modeling Katrina using satellite data reveals that the storm increased from a Category 1 on August 25 to a Category 5 within 3 days over the warm Gulf waters. It drew energy from the exceptionally warm water currents flowing from the southern Caribbean Sea.

> A map of water temperatures 230 feet below the surface, modeled using satellite data, shows a long Loop Current sent deep warm water toward New Orleans. As Katrina passed over it on August 28, what had been a weak Category one storm 2 days earlier surged to the top of the scale – Category five.[74]

The loop current flows from the Caribbean through the Gulf of Mexico and then eastward toward and then past the west coast of Florida. In 2005, this current flow extended, possibly as a result of global warming, farther north and coincidently coincided with Katrina's path. "It was just sitting for more than 12 hours over the Loop Current," says oceanographer Isaac Ginis, "This was one of the key factors in the intensification." And again, "By August 25," says hurricane forecaster Chris Landsea, "it was apparent that all the right ingredients were in place" Scientists predict that the ocean warming we have been experiencing since 1995 is a troubling omen. In fact, Atlantic storms are increasing in frequency. Their number has doubled in the past decade compared to the prior decade, yet as discussed, questions about global warming persist.

"The change in the Atlantic is not a small signal; we expect it to stay around for a while — it could be 25 years or more — and the implications are tremendous."[75] Given human nature, especially our tendency to react rather than act with purposeful intention before it is too late, shrill Cassandra like predictions are highly unlikely to cause much alarm or preparatory action. Even when losses are predicted accurately, as in the case of New Orleans, the smart money is on business as usual. It does not require sophisticated modeling to conclude that a Gulf coastal city, 8 feet below sea level is in jeopardy of catastrophic flooding. Once again, it is very clear that poor

judgment can easily override the best risk management intentions. After a risk has been recognized as well as it can be, given the level of our scientific knowledge, what next? What can reasonably be done about a risk that is not well recognized or even one that is well understood?

Risk Resolution

Step (6): *Loss Prevention*

Risk resolution is the second phase of the two major phases of the risk management process. It begins with steps to prevent loss. These steps, in turn, are based on the knowledge of the risk acquired by following the previous five steps in the RMS. The objective of loss prevention is to take the actions required to *avoid* the chance of loss. When loss cannot be avoided, loss prevention initiatives aim to *eliminate* the chance of loss. Once a risk has been imagined, described, observed, measured, mapped, and modeled, we can probably agree that it has been thoroughly recognized or as recognized as science will permit, at this point. Using this understanding, the most efficient thing to do would be to avoid the creation of any risk. If the risk cannot be avoided, the next action will be aimed at risk elimination.

Since the purpose of risk management is to maintain the continuity of an organization's system of operation, the prevention of any disturbance to the system prior to loss is the first priority. The second priority is to minimize any casualties and post-loss reduction in the value of the system's tangible or intangible assets so the organization can continue to operate.

Tangible assets include the physical facilities, equipment, networks, databases, and other infrastructure components that contribute value to the enterprise. Intangible assets include the knowledge and skills of the organizations staff, relationships between people, access to organizational capabilities, the reputation and image that the organization holds and strives to uphold. Tangible and intangible assets are used in often unique combinations by organizations to create value for its stakeholders.

Stakeholders, the people who benefit from an organization, include employees, investors, taxpayers, donors, partners, vendors, customers, clients, directors, trustees, and other overseers. Stakeholders are the people that depend in some important way on the organization. They are the reason the organization exists and are the object of the organization's mission, values, vision, and strategy. The organizations operating pattern, in turn, is the way the organizations capabilities are combined to deliver a unique value proposition to these stakeholders. The RMS helps ensure the continuity of the organizations operating pattern.

Loss prevention, the first step in the risk resolution phase, really picked up the pace at the beginning of the Industrial Revolution and the shift to a

money economy. At that time, people migrated from small, rural, agrarian settings to work in large factories and live in large cities, in tight clusters of wooden buildings. This was an ideal setting for a variety of social ills including the ever-present threat of fire. Water supplies were sparse and fire-fighting capabilities were rudimentary, when they existed at all. Many catastrophic fires occurred at this time. These large fires and the financial environment within which they occurred stimulated the beginning of fire insurance in North America.

The start of modern property/casualty insurance can be traced directly to The Great Fire of London, which occurred on September 2, 1666, and burned for 5 days. "Nearly one-quarter of the buildings in the City of London, where wood construction predominated, were destroyed."[76] Major fires also occurred in Boston in 1630; Philadelphia in 1730; Charleston, SC in 1740; New York in 1835; Chicago on October 8, 1871, where Mrs. O'Leary's cow caused the burning of over 2000 acres; and in San Francisco, following the earthquake in 1906. The San Francisco fire burned approximately 3000 acres and destroyed over 28,000 buildings.[77]

These terribly destructive fires, in addition to initiating the creation of the property and casualty insurance industry set loss prevention in motion within the public and private sectors of society.

> Prior to the organization of fire insurance companies, there were two principle participants in fire prevention activities: governments and independent fire-fighting groups. For an example of governmental involvement after a serious fire in Boston in 1630, Governor Winthrop prohibited construction of houses with wood chimneys and thatched roofs and he appointed fire wardens to enforce the prohibition.
>
> The first independent fire-fighting groups were formed in Philadelphia under the leadership of Benjamin Franklin. In 1752, Philadelphia had at least six groups, with an aggregate membership of 225, 8 engines, 1055 buckets, and 6 ladders. At first these groups operated for the protection of their own homes; later they fought all fires in their respective areas and depended in part on financial help from property owners.[78]

Loss prevention is the primary risk resolution activity because it is more efficient to avoid the creation of pure risks or eliminate them rather than deal with them in any other possible way. The allocation of assets for the prevention of say terrorism, assuming this threat could be avoided or eliminated, is a better, more efficient use of time, attention, and assets than the application of loss mitigation initiatives would be. Simply, why treat risk that can be avoided or eliminated? If resources are spent doing some unnecessary

risk management work, we incur what economists term "opportunity costs." This phrase refers to resources that could have perhaps been spent in pursuit of some better opportunity, hence, the term *opportunity cost*. The difference between the less productive use and the more productive use of organizational resources is defined as the opportunity cost.

There are several types of loss prevention.

> The more common ones are the engineering approach, the human or personal approach, the statistical approach, the educational approach, and the enforcement approach. To prevent a loss, it is necessary to find and eliminate or reduce the cause of loss, Causes are due either to things or to persons; in other words, causes are inanimate or animate. Inanimate causes are generally attacked through engineering methods; animate causes are generally attacked through personal means … The property engineering approach involves a knowledge and use of such sciences as physics, mathematics, chemistry, electricity, and so forth; the human approach involves knowledge and use of such sciences as psychology, physiology, sociology, and anatomy.[79]

The *9/11 Commission Report* provides a good discussion of the principles underlying the concept of loss prevention in relation to terrorism and serves as a good example of loss prevention thinking. Several recommendations aimed directly at terrorism prevention are recorded in Chapter 12 of The Commission's Report. After observing that "the nation has committed enormous resources to national security and to countering terrorism." And that, "… the American homeland is the planet." The Report advises that we should:

- Attack terrorists and their organizations
- Prevent the continued growth of Islamist terrorism
- Protect against and prepare for terrorist attacks

The Report recommends, among many other things, that we "engage the struggle of ideas." Our engagement in this struggle is an example of initiatives to prevent the birth of the evils of terrorism by implementing the following recommendation:

> Recommendation: The U.S. government must define what the message is, what it stands for. We should offer an example of moral leadership in the world, committed to treat people humanely, abide by the rule of law, and be generous and caring to our neighbors. American and Muslim friends can agree on respect for human dignity and opportunity. To Muslim parents, terrorists like Bin Laden

> have nothing to offer their children but visions of violence and death. America and its friends have a crucial advantage – we can offer these parents a vision that might give their children a better future. If we heed the views of thoughtful leaders in the Arab and Muslim world, a moderate consensus can be found.[80]

Three additional ideas include: "One of the lessons of the Cold War was that short-term gains in cooperating with the most repressive and brutal governments were too often outweighed by long-term setbacks for America's stature and interests … The United States should rebuild the scholarship, exchange, and library programs that reach out to young people and offer them knowledge and hope … The U.S. government should offer to join with other nations in generously supporting a new International Youth Opportunity Fund. Funds will be spent directly for building and operating primary and secondary schools in those Muslim states that commit to sensibly investing their own money in public education."[81]

The thrust here is to direct resources toward the underlying problems of low education, poverty, and hopelessness felt by the young people in Muslim countries and increasingly by Muslims in Western countries, in the hope of avoiding terrorism. Michael Scheuer, the author of *Imperial Hubris* raises some complications with the Report's terrorism loss prevention "education strategy," however.

> America has demanded Muslim educational authorities alter their curricula to teach a brand of Islam more in keeping with modernity and, not coincidently, U.S. interests. Thus, America wants Muslims to abandon the word of God as He revealed it in the Koran – which Muslims consider perfect and unalterable – and the Prophet Mohammed's traditions and sayings for U.S. – dictated and manmade replacements. "The other thing is that no one, no matter who he is, may interfere with our learning material … ," declared Mohammed Sayyid Tantawi, the Grand Shaykh of al-Azhar University, in early 2001. "No one may interfere in our religious curricula, which we decide on the prerequisites of our shariah. No one may stick his nose in our affairs, or in the affairs of a country like Saudi Arabia …. one who can force specific curricula on us has not been born yet."[82]

Despite our best efforts to root out the underlying causes of terrorism, the risk is likely to remain for a very long time because its antecedents are very deeply rooted. Terrorists lack prosperity and the hope that things will improve without their intervention. People with little or no hope are being taught in their youth that the U.S. is their enemy and the enemy of their

religion — that Americans "occupy" their holy lands with our armies and that we prop-up for our own purposes their repressive leaders so we can exploit their natural resources. It will take more than a "smart bomb" to turn this situation into a more positive environment for the U.S. Some risks, like terrorism cannot be prevented. Consider the following comment about the threat of radical Islamist terrorism from a counterterrorism expert.

> That threat is not something that we can defeat with arrests and detentions alone. We must work with our Islamic friends to create an alternative to the popular terrorist perversion of Islam. It is not something that we can do in a year or even a decade. We cannot be lulled into thinking we are succeeding because we have dealt with "the majority of the known al Qaeda leaders," or because there has been no major attack for some time. Their recruitment goes on, aided by our invasion and occupation of Iraq. Time is slipping by in which the new, follow-on al Qaedas are gaining strength in scores of countries. Time is passing, but our vulnerabilities to attacks at home remain.[83]

Thus, the efforts to reduce the chance of loss should start with a series of simultaneous activities. The strategy or game plan should start with imaginative, thoughtful ways of avoiding the risk altogether followed by steps to eliminate the chance that a loss will occur. For the risk of lung cancer, not smoking is an example of the former; stopping is an example of the latter. The chance that a loss will occur still remains, in most cases, however. For example second-hand smoke could present a health hazard to a nonsmoker. So could other environmental and perhaps genetic factors. In the risk manager's world, precautionary vigilance is a perennial necessity.

Step (7): *Loss Mitigation*

Loss mitigation is the final step in the RMS. If a risk cannot be completely prevented, its impact must be acknowledged and managed as effectively as possible. This involves three basic actions: (1) response, (2) recovery, and (3) reparations.

Response

The response to the presence of risk can take several forms. *Protection* from loss is a natural first step. As mentioned earlier, many security strategies start by seeking ways to diversify the exposure or the reliance on any one or even just two layers of protection, while at the same time preserving, as much as possible, the effectiveness of the business system or operating pattern the risk management interventions were intended to protect.

Concerning the threat of terrorism, The 9/11 Commission Report addresses these concerns in a number of ways. In Chapter 12, Section 4, "Protect Against and Prepare for Terrorist Attacks." Recommendations include:

> Targeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorists travel intelligence, operations and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility … The U.S. border security system should be integrated into a larger network of screening points … to intercept individuals who pose catastrophic threats … The Department of Homeland Security, properly supported by Congress, should complete, as quickly as possible, a biometric entry–exit screening system … Hard choices must be made in allocating limited resources. The U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort …[84]

As stated in The 9/11 Commission Report, "No single security measure is foolproof." Given the obvious lack of security at Boston's Logan International Airport on September 11, it is natural to assume that the Massachusetts Port Authority is placing new emphasis on loss prevention now. As reported by Stephen Flynn, in his thought provoking book, *America the Vulnerable*,

> At Logan International, security has become everyone's business, from Craig Coy, the CEO of the Massachusetts Port Authority, on down. Each day at 8:30 A.M., representatives from 40 different agencies, airlines and service providers gather to attend a daily security briefing.[85]

Not surprisingly, the security professionals at Logan use the now familiar "defense in depth" and "layers of security" idea as the foundation for their security strategy.

> With a "never again" sense of mission, The Logan Airport community essentially has taken a no-holds barred look at how to rewrite the book on airport security without breaking the bank or generating terminal gridlock.

> They began by recognizing that there are inherent limits to focusing primarily on passenger and baggage screening. What security officials needed were opportunities to intercept the bad guys before they got to the screening stations. They also had to close off the other ways in which terrorists might gain access to the airplanes, such as penetrating the perimeter of the airfield or mixing among the thousands of employees who have access to the aircraft. The result has been an innovative effort to build a series of concentric rings, each of which can help to elevate the probability of detection and interception of a terrorist threat. Collectively, these measures provide a powerful deterrent.[86]

This is the time-honored "don't put all of your eggs in one basket" spread of risk concept at work, supplemented with the idea that it is best not to "… throw the baby out with the bath water." Protection against loss takes many forms. Fire detection systems help warn and trigger the immediate use of fire extinguishers or perhaps the spontaneous and automatic release of a fire retardant chemical or water to put out the fire, as the occupants head for the fire-stairway exits, in accord with their training, following their "floor fire wardens" sporting their red baseball caps and avoiding the dangers of elevators.

Risk response planning requires actual in-the-field training and highly realistic simulation exercises to be effective. First responders and the emergency managers and commanders they follow are trained and drilled to ensure that the least loss of life and destruction of property ensue. The three "TOPOFF" (top officials) exercises conducted to date were aimed at ensuring that antiterrorism responders and their leaders are as prepared as they can be to mitigate whatever loss or damage has been caused in an attack.

The 2005 TOPOFF exercise was a full-scale test of readiness in Connecticut, New Jersey, the U.K., and Canada. The terrorist scenario portrayed a biological and chemical attack. It was planned by experts with the aim of stressing and testing first response capabilities. The best way to know if plans will work and where they are weakest is to test them and that is what TOPOFF was all about.

In general, the TOPOFF exercises were aimed at determining "readiness." They were mandated by Congress in the wake of September 11. The goal is to be fully prepared for the next attack or major emergency with, among other things, interoperable communications capabilities and a unified command structure connecting the first responders and creating a cohesive emergency response team. TOPOFF was meant to address some of the major failings evident during the September 11 attacks. The exercises are built upon the familiar "not if, but when" logic.

According to The 9/11 Commission Report:

> The lesson of 9/11 for civilians and first responders can be stated simply: in the new age of terror, they – we – are the primary targets. The losses America suffered that day demonstrated both the gravity of the terrorist threat and the commensurate need to prepare ourselves to meet it.
>
> The first responders of today live in a world transformed by the attacks on 9/11. Because no one believes that every conceivable form of attack can be prevented, civilians and first responders will again find themselves on the front lines. We must plan for that eventuality. A rededication to preparedness is perhaps the best way to honor the memories of those we lost that day.[87]

Witnesses to the hours, days, and months following hurricanes Katrina and Rita in the summer of 2005 can report, no doubt, that while we are making some important progress, we have a very long way to go in the area of post-loss response.

Recovery

A main aim of risk management is maintenance of an organization's effectiveness, notwithstanding the presence of a large number of existing and emerging pure risks. If that proves impossible, the RMS then focuses attention on the rapid recovery from loss, so *recovery* is the second loss mitigation step. The purpose of this initiative is the maintenance of system continuity. The faster repairs and replacements are made, post-loss, the better. In the private sector, the insurance business system is designed to meet this goal. In general it works well. Adjusters are usually quick to respond and quick to pay what is owed.

The public sector often supplements insurers' efforts to help with post-loss recovery. After areas are declared "National Disaster Areas," the Small Business Administration and the Department of Homeland Security's Federal Emergency Management Agency work with regional and local authorities to help restore pre-loss operability of damaged infrastructure and personal and commercial properties through a plethora of grants and loans.

Often these payments are not nearly as carefully made by the public agencies involved, than by private insurers. In general, public agencies have not developed the business systems needed to accurately assess loss and damage and determine repair and replacement costs. Thus, post-loss fraud is prevalent. The payments following Katrina produced many millions of fraudulent payments, according to the Government Accountability Office. In fact, the government has established a special task force, involving the Justice Department and the Federal Trade Commission to combat the rampant fraud following Katrina.[88]

Reparations

Following loss, major efforts are usually made to provide funds or *reparations* for repair and replacement of damaged property. Payments as compensation are also sometimes made for loss of life. State Worker's Compensation Laws schedule payments for injuries and for fatal occupational accidents. Payments vary by state. Similarly, juries decide the value of a life in wrongful death cases. Payments also vary based on a number of known and unknown variables. Income potential, age, family situation, general health at time of death, along with the nature of death should be used as significant variables in the "life value" calculation.

Our most recent experience with large-scale, public reparations occurred after the September 11 tragedy. According to Kenneth Feinberg in his book *What is Life Worth: The Unprecedented Effort to Compensate the Victims of 9/11,* the U.S. government paid a total of $7 billion for all of the 2680 eligible claims or an average payment of $1.3 million per claim. These payments were made to people from 32 states and 58 countries. They were made from the Victims Compensation Fund of 2001. This fund was created as part of the Air Transportation Safety and System Stabilization Act, passed into law on September 22, 2001. The fund was created to provide tax-free compensation to the families of those who died and were injured in the September 11 tragedy.

Given that no such payments were made following the Oklahoma City bombing or the first WTC loss where six died, we could appear to be on a new reparations path. But, as lawyers reason, "facts alter circumstances" and the Fund payments required the recipients to sign a legal release in favor of the investor-owned airlines. As the airlines were responsible for security, pre-September 11, the accumulated legal liability could have destroyed the industry, thus necessitating the payments. In Feinberg's opinion, the Victims Compensation Fund should not become a precedent. "… I think it would be a mistake for Congress or the public to take the 9/11 fund as a precedent for similar programs. Despite its success, I would not use the Fund as a model in the event of future attacks."[89]

Recovery plans and funding arrangements will be needed to help ensure a rapid return of first vital and then necessary and subsequently less critical capabilities. The restoration, repair, and replacement of critical public and private infrastructure will take priority, particularly, health and public safety, communication and transportation services along with any disruption involving air and water quality. The nation's food supply will also be a high priority. Additionally, as we realized after September 11 and hurricanes Katrina and Rita, the circumstances of the tragedy and its implications for the economy or some other important dimension of society may demand that victims and their families be paid compensation.

Summary

Risk as defined in the Oxford English Dictionary is "hazard, danger; exposure to mischance or peril." The typologies used to discuss different types of risk identify two main types: speculative risk, where there is a chance of gain, no gain, or loss, and pure risk, where there is a chance of loss or no loss only.

Pure risk is defined as "chance of loss." Pure risk is usefully informed and explored by two logics or systems of inquiry or inference: the logic of chance and the logic of loss. The management of pure risk is defined as "chance of loss."

The logic of chance is further defined by two basic measures. The first conforms closely to the theory of probability. In that theory, probabilities can be of three types: (1) objective, (2) conditional, and (3) subjective. The first two are mathematically derived. The last, subjective probabilities, are mental estimates and, therefore, uncertain and subject to the highly variable perception of the person making the estimates with all the usual biases potentially at work.

The second dimension of the logic of chance is the level of vulnerability or hazard present. Vulnerabilities and hazards are conditions that could increase the chance of a loss by a peril or threat. Perils and threats are specific causes of loss, such as fire, windstorm, terrorism, and the like. The levels of hazard could be defined by the construction materials in a building and the occupancy of the building.

The logic of loss has three dimensions: (1) cause, (2) extent, and (3) consequence. Causes of loss can be either proximate or remote. Losses are caused by threats or perils. Perils and threats are agents of death, injury, sickness, disruption, and destruction. The second dimension of loss concerns the extent of the impact of the loss. The extent or impact of a loss, in turn, has three significant components: (1) magnitude, (2) scope, and (3) duration. Impact is usually monetized or expressed in terms of lives lost or injuries incurred. The third of the three dimensions of loss are its consequences. Post-loss, following an event causing fatalities, injuries disruption, and/or destruction, important questions arise. How many casualties were incurred? What public or private property was damaged or destroyed? What environmental damage has been inflicted on our air or water? What disruption to power, fuel, and food supplies has resulted from the loss?

Once understanding of the concept and nature of the risk has been established, the next question is: How can pure risk be effectively managed?

The management of pure risk requires work in two phases; risk recognition and risk resolution. The first phase focuses on risk and the second on loss. These phases are activated by following a sequence of seven steps called the "Risk Management Sequence."

1. Phase I. Risk recognition
   (a) Step (1) *Imagine* the risk
   (b) Step (2) *Describe* the risk
   (c) Step (3) *Observe* the risk
   (d) Step (4) *Measure* the risk
   (e) Step (5) *Map and Model* the risk
2. Phase II. Risk resolution
   (a) Step (6) Loss *Prevention*
   (b) Step (7) Loss *Mitigation*

Many perils cannot flow smoothly or completely all the way through the RMS because we lack the necessary understanding of how the risk works. Hurricanes, perhaps one of the best understood perils, cannot be modeled to the point that we can, at this stage of our scientific understanding of climatology and meteorology, accurately predict landfall with a high degree of precision. But we can roughly imagine, describe, observe (fly into the eye wall), measure (forward speed, highest sustained wind speed, diameter), and map these storms quite well. Especially when compared to other natural perils, such as earthquakes, tornados, tsunamis, volcanic eruptions, wildfires, mudslides, and asteroid impacts.

Further, we are making some progress on terrorism, kidnap and ransom, and various global diseases. The control of nuclear proliferation and certain socioeconomic ills, such as inflation and unemployment, are on the risk management frontier, as are the pure risks arising from newly emerging technologies, such as nanotechnology, robotics, and genetic engineering. Bioerror would appear to be our biggest unmanaged risk, at this point.

Once risk has been recognized as well as it can be, given the state of our scientific knowledge, risk resolution can be initiated. Risk resolution initiatives usually attack either the chance that a loss could or would occur by employing prevention strategies that aim to avoid or eliminate the risk or by focusing on loss reduction through effective response, recovery, and/or reparation plans programs or actions.

Simply, effective risk management creates a safer, healthier, more secure society. Actually, risk management has much in common with a healthy life style. It is not a requirement, but it is a wise pursuit.

References

1. *The NIV Large Print Study Bible,* 10th ed., Zondervan, Grand Rapids, MI, 1995, p. 1297.
2. LeGault, M.R., *Think*, Threshold Editions, New York, 2006, p. 147.
3. *The Compact Oxford English Dictionary*, 2nd ed., Oxford University Press, New York, 2000, p. 1598.

4. Mowbray, A.H. and Blanchard, R.H., Insurance, *Its Theory and Practice in the United States*, 5th ed., McGraw-Hill, New York, 1961, pp. 6–7, cited in Vaughan, *Fundamentals of Risk and Insurance*, 9th ed., John Wiley & Sons, Hoboken, NJ, 2003, p. 7.
5. Lenz, M. Jr., The Nature of Risk, unpublished thesis, 1970, available at the St. John's School of Risk Management, Manhattan Campus Library, New York.
6. See Aczel, A.D., *Chance*, Thunder's Mouth Press, New York, 2004, for a primer on probability theory.
7. Shakespeare, W., *The Merchant of Venice*, cited in Bernstein, P.L., *Against The Gods: The Remarkable Story of Risk*, John Wiley & Sons, New York, 1996, p. 94.
8. Flynn, S.E., *America the Vulnerable*, Harper Collins, New York, 2004.
9. Yates, R., Does risk assessment work for terrorism? *Homeland Protect. Prof.* Aug. 2004, p. 42.
10. Neergaard, L., *The Day,* Friday, Nov. 25, 2005. The full report can be found at www. sciencemag.org.
11. Bernstein, *Against the Gods*, p. 7.
12. Pfeffer, I. and Klock, D., *Perspectives on Insurance*, Prentice Hall, Englewood Cliffs, NJ, 1974, pp. 5–6.
13. Fayol, H., *General and Industrial Management*, Pitman Publishing Corporation, New York, 1949, p. 4, Cited in Vaughan, *Fundamentals of Risk and Insurance*, pp. 18–19.
14. Gallagher, R.B., Risk management: a new phase of cost control, *Harvard Bus. Rev.* Sept.–Oct., 1956.
15. LeGault, *Think*, p. 89.
16. Ibid., p. 94.
17. *The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks Upon The United States*, W.W. Norton & Company, New York, 2004, p. 339.
18. LeGault, *Think*, p. 150.
19. Siegel, M., *False Alarm: The Truth About the Epidemic of Fear*, John Wiley & Sons, Hoboken, NJ, 2005, front jacket cover flap.
20. Rees, M., *Our Final Hour: A Scientist's Warning*, Basic Books, New York, 2003, p. 90.
21. Ibid., p. 92.
22. See The Odds of Dying at www.nsc.org.
23. Scotti, R.A., Sudden Sea: The Great Hurricane of 1938, Back Bay Books, New York, NY, 2003, p. 94.
24. Douglas Page, '03 blackout finally trips grid-hardening effort, Homeland Protection Professional, Jan./Feb., 2006, pp. 10–11.
25. Rees, Our *Final Hour*, p. 75.

26. Ibid., p. 74.
27. Claire Hope Cummings, Trespass, *World Watch*, 18 (1), , 2005, p. 29.
28. Ibid., p. 30.
29. Hett, A. et al., Nanotechnology: small matter, many unknowns, *Risk Perception*, Swiss Reinsurance Corporation, Zurich, 2004, p. 5, available at www.swissre. com.
30. Cummings, *Trespass*, p. 35.
31. See Meyers, D.G., *Psychology*, 7th ed., Worth Publishing, New York, 2004 chap. 28–32 for a basic introduction to thinking and intelligence.
32. Surowiecki, J., *The Wisdom of Crowds*, Doubleday, New York, 2004, pp. 158–163.
33. LeGault, *Think*, pp. 148–154.
34. Scotti, *Sudden Sea*, p. 23.
35. Ibid., p. 24.
36. See www.ibhs.org for more on the research being done to make structures more hurricane resistive.
37. See www.aoml.noaa.gov for more on weather modification history and current applications.
38. See Howe, R.F., Hollywood goes to war, *Readers Digest*, Oct. 2004, pp. 86–93 for a detailed discussion of how moviemakers anticipated the era of terror we are now experiencing.
39. Ibid., p. 92.
40. Ibid., p. 92.
41. See Surowiecki, *The Wisdom of Crowds*, for a through discussion of a normative approach to decision making and the criteria for making a wise decision.
42. Meyers, D.G., *Psychology*, 7th ed., Worth Publishing, New York, 2004, pp. 394–395.
43. Chernobyl fallout lingers, *The Week*, Mar. 24, 2006, p. 8.
44. Allison, G., *Nuclear Terrorism*, Times Books, New York, 2004, p. 7.
45. Glick, D., Montaigne, F., and Morell, V., Signs from the Earth, Appenzeller, T. and Dimick, D.R., Eds. *National Geographic*, Sept. 2004, pp. 2–75.
46. Ibid., p. 62.
47. Slovic, P., *The Perception of Risk*, Earthscan, London, 2000, pp. 80–153.
48. The Centers for Disease Control's website (www.cdc.gov) is a useful source for information on human diseases.
49. March, J.G., *A Primer on Decision Making*, The Free Press, New York, 1994, p. 18.
50. The Department of Homeland Security website (www.dhs.gov) is a useful source for safety and security information.
51. The U.S. Geological Society (www.usgs.gov) is a useful source for measures of Earth perils.

52. Hurricane information is available at the National Oceanographic & Atmospheric Association (www.aoml.noaa.gov) and at the National Hurricane Center website, (www.nhc.noaa.gov).
53. Tornado measurement information can be found on the Federal Emergency Management Agency's website (www.fema.gov) and at a website offered by Jim Cornish (www.cdli.ca).
54. Information on the measurement of asteroid threats and impacts can be found at the National Aeronautics and Space Administration website (www.nasa.gov.) and at www.space.com.
55. See www.usgs.gov. for information about monitoring floods and volcanoes.
56. Ibid., see http://volcanoes.usgs.gov/Products/Warn/warn.html.
57. Ibid., www.usgs.gov.
58. See Adams, J., *Risk*, Routledge, London, 2004, pp. 33–38, for a discussion of risk, world views and culture theory.
59. See Bernstein, *Against the Gods*, for a lucid and comprehensive discussion of the impact of myth on the math of chance.
60. Ibid., p. 16. Also, refer to pp. 1–192, for a clear history of the math of chance.
61. Ibid., p. 3.
62. Aczel, *Chance,* p. 1.
63. Holton, G.A., Defining risk, *Financ. Anal. J.*, 60(6), 19, 2004.
64. Ibid., p. 24.
65. Adams, *Risk,* p. 27.
66. Surowiecki, *The Wisdom of Crowds*, pp. 173–191.
67. See www.iit.edu for a basic description of the Delphi Method and its history.
68. Surowiecki, *The Wisdom of Crowds,* p. xx–xxi.
69. Bernstein, *Against The Gods,* p. 118.
70. Ibid., p. 118.
71. See Katrina, *National Geographic*, Special Ed., Dec. 26, 2005, pp. 1–102; van Heerden, I., *CNN Reports: Katrina-State of Emergency*, Andrews McMeel Publishing, Kansas City, MO, 2005, pp. 1–176; *The Editors of Time, Hurricane Katrina: The Storm That Changed America*, Time Inc. Home Entertainment, New York, 2005, pp. vi-121, for detailed descriptions, photographs, and maps of Hurricane Katrina. The facts on these pages were taken from these sources.
72. Katrina, *National Geographic*, Special Ed., p. 102, the National Oceanic and Atmospheric Administration (NOAA), is a scientific and environmental arm of the U.S. Department of Commerce. Among other services, NOAA warns of dangerous weather. See www.noaa.gov.
73. Ibid., pp. 13–14.
74. Ibid., p. 38.
75. Ibid., p. 35.

76. Pfeffer and Klock, *Perspectives on Insurance,* p. 18.
77. Ibid., p. 31, 47.
78. Deneberg, H.S., Eilers, R.D., Malone, J.J., and Zelten, R.A., *Risk and Insurance*, Prentice-Hall, Englewood Cliffs, NJ, 1974, pp. 82–83.
79. Ibid., p. 92.
80. The 9/11 Commission Report, p. 376.
81. Ibid., p. 378.
82. Anonymous, *Imperial Hubris*, Brassey's, Inc., Washington, D.C., 2004, p. 11.
83. Clarke, R.A., *Against All Enemies*, Free Press, New York, 2004, p. 289.
84. The 9/11 Commission Report, p. 385–392.
85. Flynn, S., *America the Vulnerable*, HarperCollins, New York, 2004, p. 70.
86. Ibid., p. 71.
87. The 9/11 Commission Report, p. 323.
88. See www.fbi.gov./katrina.htm for a brief description of the Katrina Fraud Task Force.
89. Feinberg, K.R., *What is Life Worth*?, Public Affairs, New York, 2005, p. 178.

The Structure of National Security Decisions

11

JAMES O. MATSCHULAT

Contents

The fact that we were able to talk, debate, argue, disagree, and then debate some more was essential in choosing our ultimate course.[1]
Robert F. Kennedy
Thirteen Days: A Memoir of the Cuban Missile Crisis

Introduction

Selection of a course of action is often more spontaneous than studied, more sporadic than systematic, and more hurried and haphazard than carefully considered. That decisions are made imperfectly based on individual bias and incomplete and imperfect information is reasonably well documented. What is less well known is why this is so, and what might be done to help the national security enterprise significantly improve the odds of making a sound decision. This would be particularly useful when making a national security decision because of the unusual significance of these decisions in terms of their consequences for life and liberty.

The vexing nature of national security decisions is exacerbated by the time and political pressures that comprise the context of these decisions. In retrospect, it is frequently far easier to discern the correct course after the fact and from afar, as we will see, than it appears to be at the time of decision. Time, good judgment, and wise counsel, thoughtfully given and judiciously taken are scarce commodities.

National security decisions have been analyzed and evaluated by political scientists, decision theorists, psychologists, and students of management and organizational behavior. Careful and creative thought has been given to how these decisions should happen and how in fact they have happened. These normative and descriptive accounts of history provide a rich learning laboratory notable for its diversity of opinion, imperatives, and models.

In general, when human minds turn to the question of how decisions should be made, some form of logic is invoked and a structured approach attempted. Yet, when decision makers are observed, the logics and benefits of structure are, at best, only partially evident. The optimistic belief that "to be forearmed is to be forewarned" persists in the face of considerable evidence to the contrary.

By far, the most common portrayal of decision making is one that interprets action as rational choice. The idea is as old as thought about human behavior. Its durability attests not only to its usefulness, but also to its consistency with human aspirations.

The purpose of this chapter is to encourage the national security decision maker to think about and explicitly decide how to decide. What decision-making method achieves the best fit with the problem to be solved or the issue to be resolved? We explore this terrain together in another attempt to

harvest the hard lessons learned from prior decisions with the hope that the history of unfortunate decisions will not, for the most part repeat.

The sections that follow, intend to impart a working knowledge of the most prominent features of decision theory, with particular emphasis on small group, face-to-face decisions made under conditions of risk and uncertainty. This brief review is followed by a summary of how an organization, under ideal circumstances, should approach decision making to increase the odds of a sound decision along with a few thoughts for decision group, thought leaders. The chapter then concludes with a discussion of the implications and influence human intuition, organization structure, and U.S. history and culture have had on several national security decisions concerning adventures in Cuba.

An Introduction to Decision Theory

The essence of decision is choice. And choice is about doing something or deciding not to do something — acting or choosing it would be wiser not to act. So, deciding is finally about making up your mind and doing something, even if that something is deciding to do nothing.

Deciding well is about making smart choices, choices that are arrived at deliberately, usually in one of two major ways. James March, a preeminent management scholar describes how decisions happen, "Support for decisiveness in decisions in actions normally comes from one of three different sources: hopes for consequence, pursuit of identity, or arbitrary willfulness."[2] We will concentrate in this chapter on the first two of March's observations. According to March, decisions are normally made either following a logic of consequence in which the decider is driven to realize a preference or by a logic of appropriateness, which is a function of the decider's role and the rules attached to that role. And, of course, decisions are made by people in organizations and are, therefore, plagued by all the biases and cultural administrative viruses present in our minds and within organizations. March identifies four issues around which the theory of decision-making segments.

> The first issue is whether decisions are to be viewed as choice-based or rule-based. Do decision makers pursue a logic of consequence, making choices among alternatives by evaluating their consequences in terms of prior preferences? Or do they pursue a logic of appropriateness, fulfilling identities or roles by recognizing situations and following rules that match appropriate behavior to the situations they encounter?
>
> The second issue is whether decision making is typified more by clarity and consistency or by ambiguity and inconsistency. Are

> decisions occasions in which individuals and institutions achieve coherence and reduce equivocality? Or are they occasions in which inconsistency and ambiguity are exhibited, exploited, and expanded?
>
> The third issue is whether decision making is an instrumental activity or an interpretive activity. Are decisions to be understood primarily in terms of the way they fit into the problem solving, adaptive calculus? Or are they to be understood primarily in terms of the way they fit into efforts to establish individual and social meaning?
>
> The fourth issue is whether outcomes of decision processes are seen as primarily attributable to the actions of autonomous actors or to the systematic properties of an interacting ecology. Is it possible to describe decisions as resulting from the intentions, identities, and interests of independent actors? Or is it necessary to emphasize the ways in which individual actors, organizations, and societies fit together?[3]

Many decision methods advocate or simply assume some form of rational, logical, or scientific approach based on facts and feelings. As the story is told, the rational decision maker arrives at a sound conclusion after thoughtfully selecting among a number of options, following careful application of critical, creative, and ethical reasoning skills. The alternative selected is then celebrated as a considered judgment about what course of action or conclusion is best, given the circumstances confronted or envisioned at the time the decision is arrived at.

This normative or ideal description of a decision process is often more fiction than fact. Decisions, for a variety of reasons, do not usually happen in this way. Many day-to-day decisions do not allow time or require the effort to engage in elaborate problem structuring and extensive consultation, deliberation, and documentation. Ideally, the decision method selected should fit the type of decision being made. Some decisions are snap decisions and some require collaboration — situations where "two or more heads are better than one." Decisions made in critical, life-threatening circumstances need to be made very quickly, on an almost intuitive basis and so, they require preparation, training, and extraordinarily good judgment. These snap judgments are apparently a combination of intuition and training. They are the type of decisions made by first responders, emergency room physicians, and soldiers and sailors under fire to name a few examples. The training received incorporates the lessons learned, rules, cultural norms, and general history appropriate to the occupation or position the person making the decision holds. Good actuaries like good accountants, good corrections officers, and good intelligence analysts make decisions in ways appropriate to their positions and roles in the organization. This is March's logic of appropriateness

in action. The better the training, the better the student, the better the decision or so the theory goes.

Of course, conformity with existing rules and roles may not produce desired current or future outcomes. Cultural norms and notions of appropriate behavior are often highly dynamic. As lawyers reason, "facts alter circumstances." Airport security is nothing like it was pre-September 11, 2001. Neither is our sense of security and well being. Rules, roles, and preferences need to be continually refreshed. But can they be reactive or refreshed fast enough to remain relevant to the decision makers circumstances?

Application of highly rational decision models employing the logic of consequence presents a similar, but somewhat more vexing problem. A large family of rational action models purports to guide the decision maker from awareness that the inertial course will not suffice to a new, more promising course of action based on careful consideration of an often creative array of attractive, thoughtfully analyzed and evaluated alternatives, implemented with resources and timely discipline. (A collection of these models is available in Appendix A at the end of this chapter.)

Each of these rational action models shares a common core. They first begin with a clear definition of the problem, which hopefully ties in some meaningful way to a relevant strategic, operational, or financial context followed by a survey of the options. The best options are then subjected to analysis and evaluation hopefully against the criteria made explicit in the first problem definition step. Next follows a ranking process that results in the selection of the most attractive option. Implementation planning and action steps follow, possibly joined by an accountability review of the process followed and the success produced.

Rational action decision models are typically based on a series of implicit assumptions about the ability of the decision makers to identify all the relevant alternatives and about just what the desirable outcome would be. But how can post facto decision analysts identify these assumptions and determine who defined and imposed or employed them and in what ways? Often, the criteria for defining the profile of desirable results are unstated, assumed, or implicit and, therefore, unchallenged and untested. This is unfortunate, for it is within an explicit, relevant context that decisions create intelligence and have meaning. As time and circumstances change, these assumptions may become obsolete. So, how is it possible for the criteria to become well understood and subjected to thoughtful, constructive challenge by critical thinkers? Absent this transparency and testing, it is not surprising, therefore, that the decision results are also likely to be unsatisfactory, even if the desired future state could be defined with any precision, which it usually cannot. Simply, since we cannot know the future, there can be no such thing as a sure thing. All strategic, operational, and financial plans are hypothetical. In fact, most decisions are made under conditions of *risk* where

the probabilities of a successful outcome are reasonably determinable but not absolutely predictive or *uncertainty* where they are neither. So decision making even within a well-defined context is a dicey business.

Therefore, if decisions should be made rationally, either in conformance with defined rules or in accord with logical models, but are not, how should decisions happen?

Structured Decision Making

Whether snap or considered, intuitive or explicit, singular or deliberative, decisions that are structured are best. Structured decisions are revealed and documented decisions that follow an explicit process of some kind, whether made by an individual or a group. Structured decisions do not just happen somehow. They are decisions where the facts and feelings they are based on and the ways the facts and feelings are used are explicitly and clearly documented in an accessible way.

Structured decisions exhibit two major benefits. First, structured decisions can be revisited. Decisions, especially important ones are often very complex, involving a large number of factors, actors, and frequently conflicting organizational and political considerations. Also, if time permits, a decision can be left to stew for a few days. This can be a good thing if, over this time, our reflections draw on our unconscious minds and allow us to become aware of ideas and considerations that we did not think of immediately. If, however, this reflective opportunity is wasted, as appears to have been the case in the disastrous Bay of Pigs invasion we will discuss later, trouble can ensue. Consider this exchange between first, Arthur Schlesinger, Jr., an advisor to JFK, and then President Kennedy, who finally and ominously approved the ill-fated invasion: "What do you think about this dammed invasion?" He (Schlesinger) said wryly, "I (President Kennedy) think about it as little as possible."[4]

So, important decisions are like a good stew. They involve many ingredients and tend to get better over a few days as the spices and primary ingredients blend. Of course, left too long, the decision like a stew will get old and spoil. Time is a critical dimension to both the stew cook and the decision maker. Moreover, decisions usually have a season. They need to be anticipated and properly prepared for. Both too much time and too little time can present a serious constraint and reduce decision quality — the ability of the decision to make the intended difference. These realities can test even the best memories. To cope, decision makers have evolved a number of mapping and modeling approaches. These maps and models are useful because they make the problem explicit and visual. These steps make the problem more tangible and help us conceive the cause and effect relationships

that may be at work permitting deeper understanding of what may be happening and what might be done to solve the problem, close the gap, stop the loss, or whatever is at risk of not turning out the way we prefer. Making the components of a decision and their interrelationships clear is the nature of a structured decision. This diagramming or mapping of a decision process is called "decomposing and externalizing" a problem by Richards Heuer, Jr., in his book *The Psychology of Intelligence Analysis.*[5] Heuer and others cite an interesting early example of how a problem with many variables might be very simply structured to take pressure off the memory, a scarce resource in even the very best human mind. The approach begins by reducing the problem fundamentals to writing and revisiting it over several days. This structured approach and documentation also creates at least the possibility of involving others in a meaningful way in the decision-making process. This involvement is the second benefit of a structured approach.

A simple, but very useful example of how a visual aide, in this case a "T" account of pros and cons, can assist with a decision is contained in a letter written to Joseph Priestley, a noted scientist and discoverer of oxygen, by Benjamin Franklin dated September 19, 1772. The purpose of the letter was to respond to Priestley's question concerning a potential move to a new position shortly after he had recently accepted another position. Thus, the question was personal.

> Dear Sir,
>
> In the affair of so much importance to you, wherein you ask my advice, I cannot, for want of sufficient premises advise you what to determine, but I will tell you how.
>
> When those difficult cases occur, they are difficult, chiefly because we have them under consideration, all the reasons pro and con are not present to the mind at the same time; but sometimes some set present themselves, and at other times another, the first being out of sight. Hence, the various purposes or inclinations that alternately prevail, and the uncertainty that perplexes us.
>
> To get over this, my way is to divide half a sheet of paper by a line into two columns; writing over the one pro and over the other con. Then during three or four days consideration, I put down under the different heads short hints of the different motives, that at different times occur to me, for or against the measure.
>
> When I have thus got them all together in one view, I endeavor to estimate their weights; and where I find two, one on each side, that seem equal, I strike them both out. If I find a reason pro equal to two reasons con, I strike out the three. If I judge some reasons con, equal to some three reasons pro, I strike out the five; and if, after a day or

> two of further consideration, nothing new that is of importance occurs on either side, I come to a determination accordingly.
>
> And, though the weight of reasons cannot be taken with the precision of algebraic quantities, yet when each is thus considered, separately and comparatively, and the whole before me, I think I can judge better, and am less liable to make a rash step, and in fact have found great advantage from this kind of equation, in what may be called moral or prudent algebra.
>
> Wishing sincerely that you may determine for the best, I am ever, my dear friend, yours affectionately.
>
> **B. Franklin**[6]

Another somewhat more current example of Franklin's "balance sheet" of pros and cons approach is offered by Arthur Schlesinger in his account of the Bay of Pigs decision, which we will discuss in more detail later. According to Schlesinger, Secretary of State Dean Rusk was weighing advice from his staff and Schlesinger whether or not he should recommend to President Kennedy that the invasion of the Bay of Pigs not proceed.

> Rusk … said, "Maybe we've been oversold on the fact that we can't say no to this"… Finally he said he had for some time been wanting to draw a balance sheet on the project, that he planned to do it over the weekend and would talk to the president on Monday … I don't know whether Rusk ever drew his balance sheet …[7]

The second benefit of a structured decision is the ability to communicate clearly the factors and feelings that informed the decision. Communication can be used to invite others to contribute to the decision, review it for appropriateness, or understand it so it can be effectively implemented. Often two heads are far better than one. In general, where practicable, decisions reached collaboratively are best, although not all groups are wise. As Friedrich Nietzsche observed, "Madness is the exception in individuals, but the rule in groups."[8] It is not difficult to recall market crashes, stories of rampaging mobs, and the insane behavior of large crowds, so groups are not alike and it is apparent that whatever the differences are, they matter a great deal when it comes to clear thinking and taking effective action. As Surowiecki reports:

> Groups work well under certain circumstances, and less well under others. Groups generally need rules to maintain order and coherence … The stories of these kinds of mistakes are negative proofs of this book's argument, underscoring the importance to good decision making of diversity and independence by demonstrating

> what happens when they're missing … An intelligent group, especially when confronted with cognition problems, does not ask its members to modify their positions in order to let the group reach a decision everyone can be happy with. Instead, it figures out how to use mechanisms-like market prices, or intelligent voting systems to aggregate and produce collective judgments that represent not what any one person in the group thinks, but rather, in some sense, what they all think.[9]

Groups can even help improve snap decisions. By harvesting the lessons learned after the fact in a collaborative setting, groups can usefully revise the rules or improve the tools used and possibly help construct lesson plans for training future snap decision makers. The goal is to improve future performance. As thinkers, decision makers, and problem solvers, we tend to do best, when we have help. Structured decisions permit this help because the key factors that drove the choice are documented along with the rules that were in play while the decision was being formed and implemented. According to James Surowiecki, in his book *The Wisdom of Crowds*, "The idea … is not that a group will always give you the right answer, but that on average it will consistently come up with a better answer than any individual could provide."[10]

Deliberative decisions involving a wide variety of inputs are often best because decisions made individually tend to reflect an individuals biases and lack of a highly diverse scope and breadth of worldly and local knowledge. But how can the biases of a normal human mind be overcome, and how can sufficient diversity be achieved in a decision making group?

The Behavior of Decision Makers

Normal human minds exhibit an array of biases and an affinity for dysfunctional group dynamics. These tendencies cause even the best and brightest of us to regularly trip into an impressive list of thinking traps. An inventory of the most commonly cited biases along with a brief description of each can be found in Appendix B. These biases and dynamics behave like sand in our decision-making gears and substantially reduce our effectiveness as decision makers. Psychologists have identified and studied these standard mental errors and group tendencies extensively. Armed with some basic understanding of these biases, national security decision makers can, perhaps, begin to approach decision tasks with an awareness that can guide the design and selection of their decision-making methods. The assumption here is not that adherence to a particular decision method would be best, but rather that decision makers should strive to achieve the best fit between the methods they choose to use and several basic decision-making principles that appear

to offer the best hope of avoiding the thinking traps. James Surowiecki builds a strong case for four of these principles. They include: diversity, independence, decentralization, and, importantly, an unbiased method for bringing these decentralized views together in a useful way. He refers to them as "conditions that characterize wise crowds."[11]

One of many examples he offers to illustrate his point is of particular interest to national security decision makers. It involves the use of markets where real money could be made to gather intelligence from just about anyone on the planet about probable terrorist or other national security actions and developments of interest. It is based on the understanding that "… everything we know about decision making suggests that the more diverse the available perspectives on a problem, the more likely it is that the final decision will be smart."[12]

Many large organizations have difficulty sharing information effectively. The U.S. intelligence community is no exception. *The 9/11 Commission Report*[13] makes this point quite clearly. So, how might the intelligence gathering community effectively apply the four characteristics Surowiecki cites? Centralizing intelligence gathering is not the path to obtaining a diversity of views. Only a brief exposure to bureaucrats and command and control thinkers and their tendency to speak in conclusions is evidence enough to persuade someone seeking a diversity of views to look elsewhere. Nor is the creation of a small group of highly intelligent people likely to get the job done. According to Surowiecki, "… everything we know about cognition suggests that a small group of people, no matter how intelligent, simply will not be smarter than the larger group."[14]

Rather than relying on one very smart person or small group to gather the widest possible range of views from within and without the intelligence community, what was done, or rather attempted, was the creation of several projects aimed at predicting the probability of future terror events or their antecedents. One project was called FutureMap, an internal intelligence community project and a second policy analysis market (PAM). PAM was intended to gather the views from people outside the formal intelligence establishment. Both FutureMap and PAM are excellent examples of sound decision-making approaches where uncertainty is very high and facts few.

The idea is to invite informed people to participate in a futures market where information, expectations, and hunches could be aggregated — a type of highstakes Delphi Method. Funding, according to Surowiecki, was provided by a portfolio manager at the Defense Advanced Research Projects Agency (DARPA).[15] This open source approach to intelligence gathering appears to have a lot to offer because it ostensibly avoids the omnipresent organizational pressures to achieve premature, often mindless consensus characteristics of lynching mobs, corporate board meetings, strategic planning retreats, faculty meetings, and other places where people gather to come

to agreement when confronted by intractable uncertainties, personal agendas, and image issues. Money, it seems is as political and bureaucratic as it is moral. It has the advantage of being bias free, if it can be obtained honestly.

The real problem is not reaching consensus, for without eventual consensus there can be no action taken and no problem solved. Rather, the problem is reaching consensus too soon based on thin facts and thinner thinking. Compromise is the enemy of sound decision making. It is like an injection of Novocain to our frail critical thinking skills. Hearing, understanding, appreciating, and reflecting on differences are essential to sound decision making. Sparky meetings are inevitable as they are essential if decision makers are to avoid diluting the groups IQ by rounding off the sharp edges of arguments in an attempt to achieve, often feigned harmony among the decision-making group members. It takes courage to give sustained voice to our convictions and speak truth to power at decisive moments. If we listen to that voice that only we can hear in our heads, we as members of effective decision-making groups must self-censor the self-critical voice urging us to silence; the self-deluding voice urging us to feed our egos and give voice to the truth that must be spoken and sustained for the greater good.

While FutureMap survives in some form, PAM was dead on arrival. It was deemed incorrect by several political leaders who felt it immoral to allow people to profit monetarily by accurately predicting loss events. Surowiecki states, "If PAM would actually have made America's national security stronger, it would have been morally wrong not to use it."[16]

The application of decision theory to real world problems is difficult, as the PAM example illustrates. Congress and the will and perceptions of "We the People" are difficult realities that national security professionals, indeed all of us need to deal with daily. While markets may be excellent tools for gathering information and predicting the future in the abstract, gambling and speculating produce windfall gains that can appear ill gotten. During the debate about the fate of PAM, making money by predicting disaster was deemed unacceptable. Insurers take note. The property/casualty industry makes a handsome profit predicting, preparing for, and paying for loss, yet it has not confronted criticism because it derives profit from the adversity of others. Perhaps, the industry's contribution to overall economic well-being is more obvious and more welcome than could be seen in the deployment of PAM.

So, decision makers have a number of methods and tools at their disposal and a wide variety of approaches to follow. The best decisions will be based on three principles: a diversity of perspective, independent input, and aggregated, decentralized (local) knowledge. Conversely, when decisions are reached without these characteristics present, the decisions are most likely to be suboptimal. In fact, we can use these principles as criteria for evaluating a selection of historical national security decisions.

Decision-Making Challenges in Organizations

Decision-making groups within large organizations, particularly small, face-to-face groups have been observed by psychologists and others to drift into decision-making styles that do not reflect the three characteristics of sound decision making. Moreover, the decisions these groups make tend to result in very poor outcomes for three reasons.

First, the alternatives that poorly performing groups select are often quite risky. The course of action they recommend is often more risky than anyone in the group alone would choose. Dramatic, outlandish ideas fail to get censored. Rather, they get reinforced. Instead of thinking critically, creatively, ethically, and independently challenging underlying assumptions and assertions, the group calcifies and acts as one monolithic whole like investors during a market crash. It takes on the behavior of a monster and becomes more of a mob than a deliberative, consultative group focused on carefully weighing the pros and cons of each alternative. When diversity is not present or present but muted or silenced, the group loses its diversity, independence, and the rich vitality that can be contributed from decentralized, local, or regional input. To be good, decisions need to be federal. This requires a constancy of shared purpose among people who respect each others diverse views. Groups that approach decision making in this way treat each other with respect and demonstrate this caring by actively listening to each member to gain a full understanding and appreciation for differing views. Disagreements do not lead to disagreeable behavior. Members, for example, do not talk over one another. They speak truth as they think, observe, and feel it personally. They do not report what they sense others may feel, only what they themselves think, so they speak in the first person, from their own experience. Also, they do not react or exclaim out loud and do not talk over or interrupt one another. Equal time to speak is also carefully monitored by a leader who values diversity, so aggressive members are calmed and quiet members encouraged.

Second, the staffing of decision-making groups is often poorly thought through. An invitation to participate in a group decision has reputation value in most organizations. That is, participation may have more social meaning than consequent decision value — more symbol than substance. This same phenomenon can be seen in the distribution of information. If you are on the distribution list, have high-security clearance, can get into the database and so on, you are presumed to be of some import. Either because of who you represent or because of the position you hold or because of who you know or because of what you know, and possibly can contribute to the quality of the decision.

In addition to the real need for special, private information that can enrich a decision-making process, decision-making groups need special skills

to perform well. If we disaggregate the decision processes, we can see the need for differing skills. For example, people who are quite good at creative thinking may not also have a towering competence in analytical thinking. Presumably, if the group is employing a rational action model, like one of the models in Appendix A, the exploration for alternatives may be best carried out by someone with a flourishing creative flair. Similarly, when it comes time to realistically examine and exploit each alternative by methodically and carefully comparing and ranking each option against a set of predetermined decision criteria, a more numerate mind may do the job best. If the decisions are being made pursuant to the logic of appropriateness, than too, some consideration should be given to the fundamental skill set of the decision maker selected for that role. We can see this principle at work when we think about the people who appear most comfortable and effective in their roles. We experience accountants, actuaries, computer engineers, research analysts, and university professors differently than we do police or military officers, CEOs, and other command and control personality types. The former group tends to be very reflective, thoughtful, careful, and precise, often very willing to put off a decision. The command and control group is more inclined to decide and act with a sense of urgency — ready, aim, and fire, hopefully, in that order. So, in addition to having content experts on the team, additional staffing dimensions need to be carefully considered. When staffing decision-making groups, a blend of both creative, right brained types, as well as analytical lefties, would appear to be desirable as would both reflective and more action-oriented people.

Finally, groups need to be well led. The ability to make a balanced assessment of thoughtful alternatives and select an adequate if not highly effective course of action depends on the behavior of the decision-making group's leader. When we come together to make a decision, we enter the room with many assumptions. These assumptions include the reasons we were invited, what this experience will mean to us and our department or affinity group in the near and longer term, how we relate or should relate to the others in the group, as well as the task itself, and, of course, how we should relate to the leader, among many other things.

Group dynamics can be very complex because groups and the organizations of which they are a part are highly complex dynamic, nonlinear ecologies. They are ever changing in seemingly inexplicable ways. Once more, the people we are expected to bond and purposefully interact with will have different capabilities, perspectives, political preferences, moral development, world views, and assumptions about the state of the world and our place in it, to mention only a few of the more likely major differences. Reverend Martin Luther King and President Lyndon Johnson arguably shared a common goal, but they thought about the role and the rule of law differently. For the President, a lawmaker, the laws were to be obeyed. For Reverend

King, obeying certain laws was highly immoral and it was our duty to disobey them. Hence, the route to their common goal was very different. To achieve a reasoned and durable consensus, decision group leaders need to make sense of the differences present, maintain the independence of the group's members, while harnessing the energy in the group to the decision that needs to be made, all within the time required to take effective action. Leadership is as important as it is difficult.

Groupthink: A Leadership Challenge

A special case of organizational dysfunctional decision making called "groupthink" was identified in 1972 by Irving Janis, then a psychology professor at Yale, following investigation of a series of high-profile national security and foreign policy decisions. Janis found that the observations made during his and other investigations of several decisions seemed to fit a pattern he had previously recognized in his work with dysfunctional groups of nonsmokers and others. He conceived the theory of "groupthink" after rereading Arthur Schlesinger's account of the decision-making surrounding the Bay of Pigs invasion of Cuba, which was ineptly supported by the newly elected Kennedy administration in 1961. Janis hypothesized that many poorly functioning, small, face-to-face decision-making groups tended to come to consensus prematurely before a thoughtful, critical assessment of alternatives was made. According to Janis:

> At first I was puzzled: How could bright, shrewd men like John F. Kennedy and his advisers be taken in by the CIA's stupid, patchwork plan? I began to wonder whether some kind of psychological contagion, similar to social conformity phenomena observed in studies of small groups, had interfered with their mental alertness … the poor decision-making performance of the men at those White House meetings might be akin to the lapses in judgment of ordinary citizens who become more concerned with retaining the approval of the fellow members of their work group than with coming up with good solutions to the tasks at hand … when I reread Schlesinger's account, I was struck by some observations that earlier had escaped my notice. These observations began to fit a specific pattern of concurrence-seeking behavior that had impressed me time and again in my research on other kinds of face-to-face groups, particularly when a "we-feeling" of solidarity was running high. Additional accounts of the Bay of Pigs yielded more such observations, leading me to conclude that

> group processes had been subtly at work, preventing the members of Kennedy's team from debating the real issues posed by the CIA's plan and from carefully appraising its serious risks.[17]

Janis went on to identify eight symptoms of "groupthink" after examining a number of other presidential decisions, including FDR's failure to prepare for the attack on Pearl Harbor, President Truman's invasion of North Korea, Lyndon Johnson's travails with Vietnam, and Nixon's Watergate fiasco. About each of these Janis concluded:

> Each of these decisions was a group product, issuing from a series of meetings of a small body of government officials and advisers who constituted a cohesive group. And, in each instance, the members of the policy-making group made incredibly gross miscalculations about the practical and moral consequences of their decisions.[18]

The eight symptoms he identified are classified into three types:

1. Type I. Overestimation of the group
   (a) Illusion of invulnerability
   (b) Belief in the inherent morality of the group
2. Type II. Closed-mindedness
   (a) Collective rationalization
   (b) Stereotypes of out-groups
3. Type III. Pressures toward uniformity
   (a) Self-censorship
   (b) Illusion of unanimity
   (c) Direct pressure on dissenters
   (d) Self-appointed mindguards[19]

Taken as a whole, these eight markers suggested to Janis that the outcomes from a decision-making group where the leader has not taken explicit steps to counter them, will most likely have a very low probability of a successful outcome. Of course, success is often undefined, highly subjective, or defined after the decision has played out, so analysis of decision success is a dicey business. In general, decision group leaders need to be very sure that they are countering the apparently natural tendency for national security as well as other important decision-making groups to overestimate themselves, be closed-minded and stifle dissent and divergent views.

Effective Leadership: The "Groupthink" Antidote

Optimistically, Janis prescribed nine steps a leader should take "… as potentially useful means for partially counteracting groupthink …"[20] The nine "prescriptions" follow:

1. The leader of a policy-forming group should assign the role of critical evaluator to each member, encouraging the group to give high priority to airing objections and doubts. This practice needs to be reinforced by the leader's acceptance of criticism of his or her own judgments in order to discourage the members from soft-pedaling their disagreements.
2. The leaders in an organization's hierarchy, when assigning a policy-planning mission to a group, should be impartial instead of stating preferences and expectations at the outset. This practice requires each leader to limit his or her briefings to unbiased statements about the scope of the problem and limitations of available resources, without advocating specific proposals he or she would like to see adopted. This allows the conferees the opportunity to develop an atmosphere of open inquiry and to explore impartially a wide range of policy alternatives.
3. The organization should routinely follow the administrative practice of setting up several independent policy planning and evaluation groups to work on the same policy question, each carrying out its deliberations under a different leader.
4. Throughout the period when the feasibility and its effectiveness of policy alternatives are being surveyed, the policy-making group should from time to time divide into two or more subgroups to meet separately, under different chairpersons, and then come together to hammer out their differences.
5. Each member of the policy-making group should discuss periodically the group's deliberations with trusted associates in his or her own unit of the organization and report back their reactions.
6. One or more outside experts or qualified colleagues within the organization who are not core members of the policy-making group should be invited to each meeting on a staggered basis and should be encouraged to challenge the views of core members.
7. At every meeting devoted to evaluating policy alternatives, at least one member should be assigned the role of devil's advocate.
8. Whenever the policy issue involves relations with a rival nation or organization, a sizeable block of time (perhaps an entire session) should be spent surveying all warning signals from the rivals and constructing alternative scenarios of the rival's intentions.

9. After reaching a preliminary consensus about what seems to be the best policy alternative, the policy-making group should hold a "second chance" meeting at which the members are expected to express as vividly as they can all their residual doubts and to rethink the entire issue before making a definitive choice.[21]

Janis, as a realist, understood that most organizational decision makers would not wish to take the time to engage in such elaborate processes as his nine steps require. His hope was that resourceful, concerned decision makers would take the time and apply the skills necessary to make their important decisions well. If his advice had been followed, we could arguably have avoided several recent national security fiascoes. For it seems that "groupthink" is, unfortunately, still a problem today. Of course, Janis has his critics. His thesis assumes a causal connection, as do all rational action models, between the faithful execution of good process and good outcomes. In reality, that appears an overly broad assumption. According to Paul 't Hart, in his book *Groupthink in Government: A Study of Small Groups and Policy Failure*, "… the underlying premise of groupthink research is that there are ways in which to overcome the pitfalls of collective stupidity; the big problem is how to identify these in theory and how to mobilize these in practice."[22]

Examination of the nine steps reveals that the three basic characteristics of a sound decision-making process are firmly embedded in them. Each step strives to promote diversity and independence of the decision participants while preserving the opportunity for an abundance of decentralized input. The trick, as 't Hart observes, is to figure out how to effectively improve the performance of government decision making.

> The continued occurrence of decisional failures and policy fiascoes suggests that governments have difficulty improving their performance. Studies of government learning are generally pessimistic about the possibilities to upgrade the quality of government action and induce policy makers to avoid repeating the mistakes of the past. Not only is it difficult to implement proposed reforms and improvements. More fundamentally, each of the policy recommendations offered by prescription-oriented analysts has potential drawbacks, which may offset the benefits. There are no golden formulas for solving permanently the dilemmas of government decision quality. There is no easy way to streamline the process of organizational and interorganizational problem-sensing, information processing, and choice. There is no simple, if any, method to get individual officials to enact well-trained skills and professional and ethical norms, to escape the logic of collective action, and manage bureaucratic complexity

> to make organizational behavior more morally responsible. The best one can do is to continue to try and understand the conditions of success and failure, to rethink standards of evaluating the quality of government, and to produce policy-relevant theories to stimulate improvements.[23]

One of the keys appears to be the leader's behavior. Obsequious adherence to the real or imputed desires of the leader in a decision situation can crush critical and creative thinking and suffocate any embryonic or latent ethical reasoning.

The Role of Ethics in National Security Decisions

As we will see when we examine several national security decisions, ethics have played an interesting role in national security decision making. Certainly, ethical considerations have influenced many if not every national security decision. For example, ethical considerations did not appear to weigh heavily in the decision to put the Cuban exiles on the beach unsupported and leave them there during the Bay of Pigs fiasco. Alternatively, Robert Kennedy's insistence that the decision team come up with alternatives to a military air strike, given the odious nature of a Pearl Harbor-like sneak attack on Soviet troops and the danger to Cuban "innocents" during the subsequent Cuban Missile Crisis, drove the eventual selection of a quarantine approach that peacefully defused the crisis. Interestingly, Kennedy referred to the use of indiscriminate bombing in this situation as un-American, "… a betrayal of our heritage and our ideals …"[24] In this instance, ethical considerations prolonged the search for alternatives and saved that day and many more to come.

Ethical considerations can, however, possibly contribute to the three forces that create the "groupthink" phenomena. Since our own moral development may be at odds with that of the majority of the decision-making group of which we are a part, stresses and strains can buildup like forces along an earthquake fault inside the decision maker. For example, if we are asked to agree to the possible killing of innocents as collateral damage, we might cope with this pressure by suspending our personally felt dissent and go along with the group on the assumption that the group is good, so their decisions must also be good, too. Alternatively, we might conclude that we enjoy or find benefit from association with such an important group as we find ourselves a part of, so we do not give our ethical feelings voice in the decision-making process. We might also conclude that our doubts are unworthy of consideration by such a prestigious group of seemingly more qualified

participants. Anyway, the death of innocents is often a by-product of national security decision making. And after all, "you can't make an omelet without breaking a few eggs," a statement that serves as an example of the type of mindless put-down often heard in these situations when an attempt is made to belittle and silence a discordant voice. In this way, the divergence of our personal ethical values from that assumed to be held by the decision-making group can become an antecedent to "groupthink." The majority or perhaps a self-appointed mindguard will often work hard to fog clear foresight and mute a dissonant voice. Janis, ever the optimist, recognized this potential clash between decision makers' personal, humanitarian values and the daunting requirements for making utilitarian national security decisions. "… Improving the quality of decision making by eliminating certain sources of error that prevent a group from achieving its goals can be expected to have good social consequences for policy-making groups that have good goals, otherwise not."[25]

Analyzing and Evaluating National Security Decisions

National security decisions are by nature very important decisions because they impact the health and well being of nations. The impact these decisions can have on the course of world events causes them to become the subject of much analysis, evaluation, and debate. In most cases, the analysts, evaluators, and debaters had nothing or little to do with the initial decision, so the facts and feelings they review are not based on first-hand information and are, therefore, subject to individual bias, wrong information, and consequent misinterpretation.

Even the decision makers themselves may be hard pressed to make a full accounting of all that happened during the decisions they participated in. Consider the following statement by President Kennedy on this point. "The essence of ultimate decision remains impenetrable to the observer — often indeed, to the decider himself … There will always be the dark and tangled stretches in the decision-making process — mysterious even to those who may be most intimately involved."[26] Nevertheless, the facts we can find are the facts we have to work with. Even if we cannot be perfect in our analyses, we can at least look to see if anything can be usefully gained from reviewing the public record.

Several historically significant decisions concerning Cuba in the 1960s are of particular interest to students of national security decision making. The decision making surrounding the 1961 Bay of Pigs invasion and the 1962 Cuban Missile Crisis are the two that come to mind most easily. These

decisions were made only 15 months apart by the same administration. Six of the principal decision makers were the same in each decision. Yet, the outcomes were arguably very different. The Bay of Pigs invasion was a disaster, whereas the Cuban Missile Crisis, perhaps the most dangerous time in human history, so far, was arguably a success. What were the major differences between these two decisions? Can we spot, in our analyses, any lack of diversity, independence, and decentralization in the Bay of Pigs and the abundance of these three in the successful resolution of the Cuban Missile Crisis? Were any of Janis's nine prescriptions for decision success evident?

Judging Decision Quality

The analysis and evaluation of national security decisions can be made against the backdrop of what students of decision making have learned about how decisions happen. But to some degree these retrospective analyses are self-fulfilling. Proponents of rational action models view decision quality from the perspective of the fidelity with which a decision model was followed. Similarly, if the decision maker was acting in accord with the logic of appropriateness and, therefore, acting in concert with a chosen or assigned role, the decision is deemed a success if it was made appropriately, in tight conformity with the tenets of the assigned role or guild requirements. Hence, decision quality tends to be judged subjectively, by an assessment of the process employed with more emphasis on the form of the decision than on the decision's success or after the fact based on how the decision worked out or more ambiguously and perhaps realistically, based on what those in high authority say about or how they interpret the decision when its impact and implications are known. In this way, failures are labeled "opportunities for improvement," lies "virtual certainties," and abject ethical lapses "errors in judgment." Decision makers are also subjected to similar treatment. Depending on how things turn out, decision makers can be:

Dimension 1 bold (*foolish*)	careful (*timid*)
Dimension 2 independent (*arrogant*)	consultative (*indecisive*)
Dimension 3 fresh (*naïve*)	sophisticated (*cynical*)
Dimension 4 honest (*rude*)	sympathetic (*soft*)[27]

Of course, success and history itself are subjective, raising the question of how history happens. Who decides based on what criteria whether an event is worthy to be recorded as history or if a decision was, in fact, of historical significance?

Notwithstanding all these difficulties, we can usefully review the two Cuba decisions and extract a few lessons for national security decision making.

Bay of Pigs

The invasion of Cuba's Bay of Pigs occurred in April of 1961. As Janis describes it:

> On April 17, 1961, the brigade of about fourteen hundred Cuban exiles, aided by the United States Navy, Air Force, and the CIA, invaded the swampy coast of Cuba at the Bay of Pigs. Nothing went as planned. On the first day, not one of the four ships containing reserve ammunition and supplies arrived; the first two were sunk by a few planes in Castro's air force, and the other two promptly fled. By the second day, the brigade was completely surrounded by twenty thousand troops of Castro's well-equipped army. By the third day, about twelve hundred members of the brigade, comprising almost all who had not been killed, were captured and ignominiously led off to prison camps.
>
> In giving their full approval, President Kennedy, Dean Rusk, Robert McNamara, and other high-level policymakers in the United States government had assumed that "use of the exile brigade would make possible the toppling of Castro without actual aggression by the United States." The president's main advisers certainly did not expect such an overwhelming military disaster … None of them guessed that the abortive invasion would encourage a military rapprochement between Castro and the Soviet leaders, culminating in a deal to set up installations only ninety miles from the United States shores equipped with nuclear bombs and missiles and manned by more than five thousand Soviet troops, transforming Cuba within eighteen months into a powerful military base as a satellite of the Soviet Union. Had the president and his policy advisers imagined that this nightmarish scenario would materialize (or had they even considered such an outcome to be a calculated risk), they undoubtedly would have rejected the CIA's invasion plan.[28]

The expedition in the Bay of Pigs failed for many reasons. "The expedition was not only misconceived politically. It was also misconceived technically … The president had insisted that the political and military risks be brought into balance; given the nature of the operation, this was impossible, and someone should have said so."[29] Further, according to Schlesinger:

> What caused this disaster? … For the reality was that Fidel Castro turned out to be a far more formidable foe and in command of a far better organized regime than anyone had supposed … His

> performance was impressive … One reason Washington miscalculated Castro, of course, was a series of failures in our own intelligence … And there were tactical errors.[30]

Clearly, the fact that President Kennedy had inherited the ill-conceived Cuban invasion initiative from the Eisenhower–Nixon administration was a factor in the decisions poor quality. Inertia overcame intelligence, in this case. Also, Kennedy was riding high and failed to assert himself and take control of the government as he should have. So hubris played a role too. Finally, even though the Bay of Pigs decision has become a poster child for the "groupthink" syndrome, a group is required for it to be in operation. According to Janis, "Groupthink refers to a deterioration of mental efficiency, reality testing, and moral judgment that results from in-group pressures."[31]

An examination of the critical tactical decisions in this episode suggest that the Bay of Pigs decision defects may not have been caused by "groupthink." The initial idea of an adventure in Cuba was suggested initially and ironically, by Nixon, planned in the head of the CIA's then deputy chief of operations, and creator of the tremendously successful U-2 program, Richard Bissell, and made by Kennedy, not by a cohesive group of anesthetized critical thinkers. For more on this alternative view, consider this statement by Peter Wyden, from his book, *Bay of Pigs*:

> But too much can be made of group dynamics. The five key decisions of the Bay of Pigs were not made in a group, nor even, for the most part, in a group setting: (1) The decision to escalate the adventure from a plausibly deniable infiltration effort into an invasion was made in Bissell's head; (2) the decision to weaken the first air strike and make it "minimal" was made unilaterally by Kennedy; (3) the decision to cancel the second air strike was made by Kennedy late on a Sunday night by phone in consultation with Rusk and Bundy; (4) the decision to give the "go" order was made by Kennedy after extensive, lonely soul-searching; (5) the decision not to escalate the invasion in the face of incipient disaster — to become a "bum," not an aggressor — was made by the President, sparring fiercely with Admiral Burk; other advisers were practically silent. Inevitably, the President's personality and power shaped events more than they shaped him. The initiative and responsibility were his. He relished both. Action. That's what he had become president for. That's what the country wanted. "Vigah," as he said it, especially after the sleepiness of the Eisenhower years … As Schlesinger later wrote … His confidence in his own luck was unbounded. "Everyone around him thought he had the Midas touch and could not lose"…[32]

In any case, "groupthink" is both an interesting and useful hypothesis for investigating national security decisions.

There are many well-written and useful accounts of the Bay of Pigs disaster. Two from the period include Theodore Sorensen's *Kennedy* and Arthur Schlesinger's *A Thousand Days*. Both retell of the surprise, anguish, and regret that the president and his advisers felt following this awful episode.

> President Kennedy was stunned. As the news grew worse … he became angry and sick at heart. He realized that the plan he thought he had approved had little in common with the one he had in fact approved. "How could I have been so stupid to let them go ahead?" he asked. Sorensen wrote, "His anguish was doubly deepened by the knowledge that the rest of the world was asking the same question."[33]

According to Schlesinger's account of the president's reactions after the fiasco, the event was part of a larger context and perhaps an important learning opportunity.

> Kennedy looked exceedingly tired, but his mood was philosophical. He felt that he now knew certain soft spots in his administration, especially the CIA and Joint Chiefs. He would never be overawed by professional military advice again. "We can't win them all," he said. "And I have been close enough to disaster to realize that these things which seem world-shaking at one moment you can barely remember the next. We got a big kick in the leg and we deserved it. But maybe we'll learn something from it."[34]

Schlesinger was himself a player in the Kennedy administration, serving as a special assistant to President Kennedy and was a professor of history at Harvard. He explains his personal role in the Bay of Pigs in this way:

> In the months after the Bay of Pigs, I bitterly reproached myself for having kept so silent during those crucial discussions in the Cabinet Room, though my feelings of guilt were tempered by the knowledge that a course of objection would have accomplished little save to gain me a name as a nuisance. I can only explain my failure to do more than raise a few timid questions by reporting that one's impulse to blow the whistle on this nonsense was simply undone by the circumstances of the discussion.
>
> It is one thing for a Special Assistant to talk frankly in private to a President at his request and another for a college professor, fresh to the government, to interpose his unassisted judgment in

> open meeting against such figures as the Secretaries of State and Defense and the Joint Chiefs of Staff, each speaking with the full weight of his institution behind him. Moreover, the advocates of the adventure had a rhetorical advantage. They could strike virile poses and talk of tangible things — fire power, air strikes, landing craft and so on. To oppose the plan, one had to invoke intangibles — the moral position of the United States, the reputation of the President, the response of the United Nations, "world public opinion," and other such odious concepts.[35]

But what were the lessons learned? If we are to believe that good decisions probably are more likely to flow from good decision processes, a belief that requires a willingness to downplay a deterministic role for bureaucratic rivalries, personal politics, organizational dynamics among many other decision-shaping forces, we should be able to detect the absence of diversity, independence, and decentralized input in the Bay of Pigs decision process. For an example of a lack of independence, decentralized input consider this comment from Schlesinger: "The same men … both planned the operation and judged its chances of success … The need to know standard — i.e., that no one should be told about a project unless it becomes operationally necessary — thus, had the idiotic effect of excluding much of the expertise of government at a time when every alert newspaperman knew something was afoot."[36]

If the three characteristics of a quality decision are at work, we should also see efforts to include these then in the application of the lessons learned in the president's future decisions.

According to Schlesinger speaking of Kennedy:

> The first lesson was never to rely on the experts. He now knew that he would have to broaden the range of his advice, make greater use of generalists in whom he had personal confidence and remake every decision in his own terms … And he took a new view of the White House staff. While Bundy and I had not performed with distinction, he had not used us as he would use his White House staff later; he had not, for example, called us in for a staff discussion of Cuba, away from the inhibiting presence of the grandees in the cabinet room … In the future, he made sure he had the unfettered and confidential advice of his own people. For our part, we resolved to be less acquiescent the next time. The Bay of Pigs gave us a license for the impolite inquiry and the rude comment. In addition, Bundy was moved over from the Executive Office Building to the West Wing of the White House and given new authority as a coordinator of security affairs within the White House. He instituted regular morning meetings for his National

> Security Council staff, to which he invited other members of the White House group involved in foreign affairs … This valuable innovation provided the White House a point of information and control below the top and strengthened Bundy's services to Kennedy. All this helped the President to tighten his personal hold on the sprawling mystery of government.[37]

So, the move to include "generalists" can be interpreted as a search for greater diversity in the decision-making process. The taking of a "new view of the White House staff … away from the inhibiting presence of the grandees …" can be seen as a move toward securing independent views and the institution of more open, broadly attended regular meetings to "… provide the White House with a point of information and control below the top …" could be viewed as an effort to achieve a higher level of decentralized input in the White House decision making.

Thus, the efforts to improve decisions in the Kennedy administration, following the Bay of Pigs episode attempted to capture at least some of the benefits that can be gained from the deployment of diversity, independence, and decentralization in national security decision making. These same initiatives may help decision makers avoid the "groupthink" syndrome. The failure to sufficiently challenge underlying assumptions, and passively accept glib answers to good questions as well as failing to think creatively about an issue, can in part be attributed to an absence of these important decision characteristics.

Certainly, interpersonal relations and rivalries, real or imagined, also can be seen to play an important role. As strategists know, clever ideas are cheap, but the initiative to carry them out is quite dear. That is, ideas are a lot easier to come by than are the efforts required to execute them well. And students of high-performance management would advise that the key to effective execution is having the right people in the right positions at the right time. This is, of course, far easier said than done. But this principle too can be seen in Kennedy's Bay of Pigs recovery program when he turned to his trusted advisers and repositioned them through a reorganization initiative, so they had both more authority and were closer to him throughout the remainder of his administration. To gain a deep understanding of national security decision making, the relationships between the president and the president's advisers is essential.

As we have seen, Janis's analysis and evaluation of the Bay of Pigs and several other fiascoes led him to conceive his "groupthink" hypothesis. Schlesinger's account of the Bay of Pigs decision triggered Janis's creative, psychologist's mind with his reflections on the decision process that was employed. For example, "Our meetings were taking place in a curious atmosphere of assumed consensus."[38] Janis explored this notion of a "curious

atmosphere" and found a plausible explanation in his "groupthink" hypothesis. Perhaps, the next Cuban adventure can offer further evidence of the usefulness of the "groupthink" hypothesis.

Cuban Missile Crisis

Within 15 months of the Bay of Pigs invasion in April of 1961, the Kennedy Administration was again confronted with the need to make an important national security decision. Of course, this time, during what Robert Kennedy has referred to as the "Thirteen Days," which occurred between the U-2 spy plane's photographs of the Soviet missiles in Cuba on October 15, 1962 and the Soviet Premier's agreement to remove them on October 28, the decision process would be quite different, as the Administration had learned some hard lessons during their previous encounter in Cuba. In Schlesinger's words:

> The impact of the failure shook up the national security machinery … It was a horribly expensive lesson, but it was well learned. In later months, the President's father would tell him that, in its perverse way, the Bay of Pigs was not a misfortune but a benefit. I doubt whether the President ever fully believed this; the thought of the men of the Brigade suffering in Cuban prisons prevented easy consolation. But no one can doubt that failure in Cuba in 1961 contributed to success in Cuba in 1962.[39]

As is usually the case, the two Cuban events are related, both to each other and to larger world events. National security decisions are highly complex, both in themselves and in terms of the context within which they occur.

While we cannot be certain, it appears that the U.S.'s deployment of 15 Jupiter nuclear missiles in Turkey on the Soviet doorstep in April 1962 on the heels of the Bay of Pigs episode probably precipitated the Soviet decision to install missiles in Cuba. Further, Cuba needed a trading partner since they had lost the U.S. sugar and other markets in 1961 with the U.S. embargo and severing of diplomatic relations. In this way, economic strategies drive national security agendas. Stable, prosperous peoples are not normally warlike; nor do they typically engage in terrorism. Bellicose acts often have their antecedents firmly rooted in economic conditions and economic outlooks. For more background on the economic antecedents to the U.S./CIA-led adventures in Cuba in 1961, the reader can look into events that took place in Iran in 1953 with the overthrow of Mohammed Mossadegh and in Guatemala in 1954, when the government of Jacobo Arbenz Guzman fell. Both events resulted in the removal of governments regarded as antithetical to U.S. interests. Both countries were of economic interest to the U.S. and

both collapsed quite easily when confronted by the CIA's operational capabilities. Castro's Cuban government has proven somewhat more resilient.

This Time a Different Approach and Better Results

In response to the Soviet and Cuban governments' agreement to deploy nuclear weapons in Cuba, President Kennedy decided to force the Soviets to remove the missiles. This decision by the president at the outset of the crisis immediately became the goal. And it was not discussed or seriously challenged or debated by the president's advisers. It was simply accepted and used to drive the ensuing decision-making process. Of course, the goal could well have become the subject of deep discussion and debate because the implications brought the world to the brink of nuclear war, but it was not. It was for the most part adopted by the president's team and pursued with a far more effective decision-making process than that employed during the Bay of Pigs decision drama.

The decision-making process used during the missile crisis was designed to avoid the many mistakes encountered during the earlier Cuban crisis. The steps taken infused the process with the familiar three characteristics of sound decision making cited earlier: diversity, independence, and decentralization. These efforts also appear to have obviated the advent of "groupthink" as well.

After making the goal clear by defining what needed to be done, President Kennedy stepped back and let his team — now referred to as The Executive Committee, or "ExCom" as it became known — sort through the facts and feelings, circumstances and implications, and come to a consensus about how the goal of ridding the island of the missiles was to be achieved. The ExCom consisted of about 17 top advisers. They met regularly and in secret, without agenda and often without the president in attendance. According to Schlesinger's account of these proceedings:

> In the Executive Committee, consideration was free, intent and continuous. Discussion ranged widely, as it had to in a situation of such exceptional urgency, novelty and difficulty. When the presence of the president seemed by virtue of the solemnity of his office to have a constraining effect, preliminary meetings were held without him. Every alternative was laid on the table for examination, from living with the missiles to taking them out by surprise attack, from making the issue with Castro, to making it with Khrushchev. In effect, the members walked around the problem, inspecting it from first this angle, then from that, viewing it in a variety of perspectives. In the course of the long hours of thinking aloud, hearing new arguments, entertaining new considerations, they almost all found themselves moving from one

position to another. "If we had had to act on Wednesday in the first twenty-four hours," the president said later, "I don't think probably we would have chosen as prudently as we finally did." They had, it was estimated, about ten days before the missiles would be on the pads ready for firing. The deadline defined the strategy … On the first Tuesday morning, the choice for a moment seemed to lie between an air strike or acquiescence — the president had made clear that acquiescence was impossible. Listening to the discussion, the Attorney General … then … said aloud that the group needed more alternatives; surely there was some course in between bombing and doing nothing; suppose, for example, we were to bring pressure by placing nuclear missiles in Berlin? The talk continued and, finally, the group dispersed for further reflection … In the meantime the Pentagon undertook a technical analysis of the requirements for a successful strike … All these considerations encouraged the search for alternatives. When the Executive Committee met on Wednesday, Secretary McNamara advanced an idea that had been briefly mentioned the day before and from which he did not thereafter deviate — the conception of a naval blockade designed to stop further entry of offensive weapons into Cuba and hopefully to force the removal of the missiles already there. Here was a middle course between inaction and battle, a course which exploited our superiority in local conventional power and would permit subsequent movement either toward war or toward peace … the majority of the Executive Committee by the end of the day was tending toward a blockade … In the evening the president met with the Executive Committee … He was evidently attracted by the idea of the blockade. It avoided war, preserved flexibility and offered Khrushchev time to reconsider his actions. It could be carried out within the framework of the Organization of American States and the Rio Treaty. Since it could be extended to nonmilitary items as occasion required, it could become an instrument of steadily intensifying pressure … the blockade, by enabling us to proceed one step at a time, gave us control over the future. Kennedy accordingly directed that preparations be made to put the weapons blockade into effect on Monday morning … now, several began to re-argue the inadequacy of the blockade … Secretary McNamara, however, firmly reaffirmed his opposition to a strike and his support for the blockade. Then Robert Kennedy, speaking with quiet intensity, said that he did not believe that, with all the memory of Pearl

> Harbor and all the responsibility we would have to bear in the world afterward, the President of the United States could possibly order such an operation. For 175 years we had not been that kind of country. Sunday-morning surprise blows on small nations were not in our tradition … In retrospect most participants regarded Robert Kennedy's speech as the turning point.[40]

From review of the record provided by Schlesinger, we can see and sense the deliberative nature of the missile crisis decision process. Clearly, spirited debate and careful, wide-ranging consideration of alternatives characterized the process they followed. President Kennedy, had ruled out the option of giving in, after all, missiles on subs, in Moscow, or in Cuba would presumably be as deadly. However, the president framed the debate and, while he was directive, he was not domineering. And, of course, unlike the Bay of Pigs, he was fully engaged in the decision making from the outset to the action. By allowing agenda-less, leaderless meetings to proceed in his absence, he encouraged unfettered interaction among the wide group of involved advisers. But when it came time to reach consensus, he made sure it was achieved and effective action taken. In the end, in exchange for an explicit promise not to invade Cuba and a quiet private agreement to dismantle the soon obsolete Jupiter missiles in Turkey, Khrushchev agreed to withdraw the Soviet weapons from Cuba. Thus, in this way the world moved on to the next crisis in Berlin and beyond.

A similar account of the crisis is available in Robert Kennedy's book, *Thirteen Days*. In his account, which tracks closely with Schlesinger's, he stresses in the chapter titled "Some of the Things We Learned …" the president's insistence on including different views in the debate about what to do in response to the Soviet/Cuban nuclear cabal.

> The fact that we were able to talk, debate, argue, disagree and then debate some more was essential in choosing our ultimate course … I believe our deliberations proved conclusively how important it is that the president have the recommendations and opinions of more than one individual, of more than one department, and of more than one point of view. Opinion, even fact itself, can be best judged by conflict, by debate. There is an important element missing when there is unanimity of viewpoint. Yet that not only can happen, it frequently does when the recommendations are being brought to the President of the United States … We had virtual unanimity at the time of the Bay of Pigs. At least, if any officials in the highest ranks of government were opposed, they did not speak out.[41]

Additional Case Examples

Further examples of effective and ineffective national security decisions can be found in the work of Graham Allison's *Essence of Decision* (the Cuban Missile Crisis); 't Hart, *Groupthink in Government* (Iran-*Contra*); and Janis, *Groupthink* (North Korea, Pearl Harbor, the Vietnam War, the Marshall Plan, and Watergate). Each of these well-researched resources focuses on the relative presence or absence of effective decision making by government leaders and their advisers.

In the end, the question of how to make better national security decisions eludes a clear, succinct answer. Individuals have many natural biases and so we turn to groups to make our most important decisions on the optimistic hope that these groups will decide wisely. Yet, as we have seen, groups have problems too, unless they are well led to include diverse views, championed by independent participants who hold unconventional insights and can somehow be encouraged to share them persuasively.

Current examples of defective decisions by governments and governmental agencies are not, unfortunately, difficult to identify. For example, the highly flawed decision making around the reentry of the space shuttle *Columbia* is arguably a recent example of "groupthink."[42] The earlier *Challenger* disaster is another example from NASA of this phenomenon. The decision making on the recent *Discovery* shuttle appears far better. Both of the earlier cases illustrate how pressure was applied to silence critics of the conventional, ultimately disastrous course the mission team leader chose. Leaders need to cultivate and promote the sharing of diverse views and avoid being overly directive. Yet, decisions have to be made on the best information and judgment available and, of course, no one can be correct all the time. The future is unknowable and bad luck happens, notwithstanding the most thoughtful application of sound decision-making processes.

According to Janis, there are seven markers that decision investigators can use to help identify a defective decision making process. They are, of course, based on the optimistic assumption that good decision-making processes will lead to good governmental decision outcomes. While not intended to serve as a model for sound decision making, they provide, in the inverse, a useful topographical map for scouting out a sound decision.

> First the group's discussions are limited to a few alternative courses of action (often only two) without survey of the full range of alternatives. Second, the group does not survey the objectives to be fulfilled and the values implicated by the choice. Third, the group fails to examine the course of action initially preferred by the majority of members from the standpoint of nonobvious risks and drawbacks that had not been considered when it was originally

> evaluated. Fourth, the members neglect courses of action initially evaluated as unsatisfactory by the majority of the group. They spend little or no time discussing whether they have overlooked nonobvious gains or whether there are ways of reducing seemingly prohibitive costs that had made the alternatives seem undesirable. Fifth, the members make little or no attempt to obtain information from experts who can supply sound estimates of losses and gains to be expected from alternative courses of actions. Sixth, selective bias is shown in the way the group reacts to factual information and relevant judgments from experts, the mass media, and outside critics. The members show interest in facts and opinions that support their initial preferred policy and take up time in their meetings to discuss them, but they tend to ignore facts and opinions that do not support their initially preferred policy. Seventh, the members spend little time deliberating about how the chosen policy might be hindered by bureaucratic inertia, sabotaged by political opponents, or temporarily derailed by the common accidents that happen to the best of well-laid plans. Consequently, they fail to work out contingency plans to cope with foreseeable setbacks that could endanger the overall success of the chosen course of action.[43]

The analysis of significant, remote national security decisions has been the subject of insightful work carried out by another scholar, Graham Allison. For example, in his book, *Essence of Decision on the Cuban Missile Crisis*, he offers three models for analyzing foreign policy and military decisions. His analytical models are based on the realization that significant national security decisions are not usually made by individuals, but rather they are formed by circumstances and made by large governmental organizations. For example:

> When we are puzzled by a happening in foreign affairs, the source of our puzzlement is typically a particular *outcome*: the Soviet placement of missiles in Cuba, the movement of U.S. troops across the narrow neck of the Korean peninsula, the Japanese attack on Pearl Harbor. These occurrences raise obvious questions: *Why* did the Soviet Union place missiles in Cuba? *Why* did U.S. troops fail to stop at the narrow neck in their march up Korea? *Why* did Japan attack the American fleet at Pearl Harbor? In pursuing the answers to these questions, the serious analyst seeks to discover why one specific state of the world came about — rather than some other.

> In searching for an explanation, one typically puts himself in the place of the nation, or national government, confronting a problem of foreign affairs, and tries to figure out why he might have chosen the action in question …. In offering (or accepting) these explanations, we are assuming governmental behavior can be most satisfactorily understood by analogy with purposeful acts of individuals In many cases this is a fruitful assumption … But this simplification — like all simplifications obscures as well as reveals. In particular, it obscures the persistently neglected fact of bureaucracy: the "maker" of government policy is not one calculating decisionmaker, but is rather a conglomerate of large organizations and political actors. What this fact implies for analysts of events like the Cuban missile crisis is no simple matter: its implications concern the basic categories and assumptions with which we approach events.[44]

Allison offers several useful models for analyzing foreign and military policy decisions. His models emphasize the role that governmental preferences, large governmental bureaucracies, and political forces play in decision making at the national level.

In the end, when we undertake the task of analyzing and evaluating national security decisions, we are left with the task of finding our way through largely uncharted seas. There does not appear to be any one ideal approach for either making or subsequently analyzing national security decisions at this point. Yet, we press on, lurching and lumbering forward, hoping for at least some improvement in our governmental decision making. While humanity in the universal scheme of things may be more like "the dream of a shadow" than a Colossus bestriding the world, the human spirit is ever optimistic.

Summary

National security decisions are extremely important decisions because they affect us all. Therefore, these decisions should be made as thoughtfully as possible. We want our best critical and creative thinking skills and capabilities to be fully engaged when we are deciding about waging war and maintaining peace.

Study of prior decisions and how they have happened suggests that we make our best decisions when we are thinking carefully, critically, creatively, and ethically. That is, when we are clear about the context of the decision and understand the definition of the situation we are to resolve or problem we are to solve. The makers of national security decisions have a responsibility

to employ a rational, structured process for making decisions. Simply, problems are unlikely to be effectively solved if they are not thoroughly understood and thoughtfully defined.

Careful, critical thinking is informed skeptical thinking. It involves an unemotional systematic search for the underlying assumptions and the unshakable facts that support them. It eschews the conventional wisdom and tests the pivotal evidence presented. Critical thinkers question the premises promoted by the advocates and the experts alike. It is the thinking exhibited by mature, realistic, thoughtful, people with a well-formed sense about how the world has, does, and both should and, perhaps most likely, will work. People who think and decide in this way personify the "precautionary principle." They instinctively look before they leap. These are the people we want to enlist in our national security enterprise to drive our decision making. Especially, those decision tasks involving problem definition, evaluation, and the choice itself.

But, before we can evaluate a decision option or alternative and decide, we ideally would like to have before us a rich array of attractive alternatives to select from. The type of thinking that is best at generating an impressive display of diverse options is creative thinking. This involves the ability to see things from a different point of view and arrive at different conclusions. Among a group, a highly creative person can look at the same situation or set of facts and analyses as the rest and see things very differently. Creative people are able to imagine unique alternatives because they think very different thoughts seemingly by blending a contrary worldview with sometimes alarmingly odd ideas. In this way, novel options for solving problems are identified. The creative thinker is a guide with a very different compass and desire for adventure than most. A visit to any art museum will make the point that people experience and can see our world in quite different ways.

Ethical reasoning is also central to effective national security decision making. It is present in the decision when the decision makers clearly address the right way to behave as a key factor in a decision. These considerations are central to the concept of a "just war" and a "just way" to conduct war, treat prisoners, and impact innocents. As we have seen in the two Cuba decisions, it was noticeably absent in the Bay of Pigs decision, particularly with respect to the decision to encourage, and then leave the Cuban Brigade (freedom fighters) on the beach and standby as they were vanquished by Castro's forces. During the Cuban missile crisis, at Robert Kennedy's urging, the search for alternatives to a comprehensive bombing campaign was largely motivated by the harm such an indiscriminate choice would do to the American image and reputation. In general, if something feels wrong, it usually is. This feeling can be the result of our ethical, perhaps unconscious mind at work.

While we tend to trust decisions made explicitly in accord with a logical, sequential process, decisions made quickly, unconsciously without any recall

as to how, can be quite correct and effective, in the right setting. These "snap" decisions are, in fact, often required of first responder public safety professionals. Our minds are always working even though we may not be completely or even remotely aware of the processes involved. Thus, when the time comes to choose and act, we can be ready, assuming we have the right instincts, ingrained responses, and capabilities available. These can be acquired and learned through training and experience. Psychologists refer to this mental faculty as our "adaptive unconscious."

More usual, in the national security setting decisions are made by small, cohesive, face-to-face groups. Experience suggests that these decisions are best made by groups that exhibit three characteristics in abundance: diversity (a variety of views), independence (free from control or influence), and decentralized (local) information. Thus, leaders of decision-making groups should strive to include these decision characteristics in the decision processes they choose to employ and promote them in the behaviors they adopt. Failing to do so, can expose groups to a deleterious phenomenon called "groupthink," the tendency on the part of poorly led groups to suspend critical thinking and arrive at an often risky consensus prematurely.

National security decisions present themselves within very politically, administratively, and diplomatically complex and often, time sensitive contexts. Thus, a leisurely approach is frequently not an option, although some decisions do offer decision makers plenty of time. Months were available prior to the Bay of Pigs fiasco. The Cuban missile crisis famously allowed the ExCom 13 days to select a course of action.

In the end, national security decision-making processes are quite difficult to understand. For example, when we search for the meaning of a decision should we focus on their historical consequences, how appropriate they were for their time, or something else altogether? Much, perhaps too much, is left to our imaginations. Even when we try to investigate national security decisions our empathy will often lead us astray. Retrospective analyses are likely to reflect too darkly or too brightly on events, depending on the analyst's frame of mind at the time. Bias is an ever-present threat to clear thinking. Decisions seem to happen in inexplicable ways. Perhaps, their true meaning is buried deeply in their convoluted contexts far away from us in both space and time. As with the ancient Pharaohs in their hidden valleys and once secret tombs, we are enticed to guess the meaning of the archeologist's find and the hieroglyphic's theme. When analyzing and evaluating a national security decision to determine its meaning, we need to try to discern the influence current and historical organizational and political forces may have had on the shape of the decision structure. That is, how did the various components of the decision process and decision makers relate to one another and what impact did these relationships have on the decision? Moreover, we need to consider whether or not

a vision of consequence or a sense of appropriate behavior may have had a role in the design of the decision. Perhaps, these are things that will be forever hidden from us as we pursue our study of the history and prehistory of significant national security decisions. National security decision makers are like the traveler viewing the fork in the road in Robert Frost's poem "The Road Not Taken." The way less traveled can seem most enticing, but one choice inexorably leads to another, so our initial decisions can make all the difference in the end. Finally, national security decisions define who we are and what is to become of us.

Appendix A

A Collection of "Rational Action" Models

The following five models are offered as examples of the many sequential decision-making processes developed by students of decision making. They are drawn from a wide variety of settings to illustrate the fundamental fact that they share at their core, what James March terms the "logic of consequence."[45] That is, each of the models assumes that the decision maker is rational. They also assume that preferences can be determined and that the decision maker has the ability to both identify the best alternatives and exploit them.

The Eight Elements of Smart Choices[46]

1. Work on the right decision problem
2. Specify your objectives
3. Create imaginative alternatives
4. Understand the consequences
5. Grapple with your tradeoffs
6. Clarify your uncertainties
7. Think hard about your risk tolerance
8. Consider linked decisions

The Sequence of Steps Involved in the Decision Process[47]

1. Classifying the problem
2. Defining the problem
3. Specifying the answer to the problem
4. Deciding what is "right" rather than what is acceptable, in order to meet the boundary conditions
5. Building into the decision the action to carry it out
6. Testing the validity and effectiveness of the decision against the actual course of events

A Generic Approach to Solving Decision Problems

1. Define the problem
   (a) What is wrong?
   (b) How do we know?
   (c) What are the criteria to be used to define a successful solution?
2. Identify the issues
   (a) What could be done to solve the problem or close the gap?
   (b) What should be done?
   (c) Why?
3. Develop solution ideas or hypotheses via "brainstorming and "brain streaming."
4. Create a plan of analysis
   (a) Break the problem into segments
   (b) Draw a diagram, flow chart, map, or model
   (c) Assign the segments based on an assessment of skills and tasks
5. Evaluate findings and draw conclusions
6. Develop solution alternatives
   (a) Check facts and sources
   (b) Compare solutions to criteria in the problem definition
   (c) Quantify degrees of improvement costs and risks
   (d) Assess overall fit with the organization
   (e) Inquire if other problems may be created
7. Evaluate solution in depth along with the processes used to create it
   (a) Relevant?
   (b) Realistic?
   (c) Implementation considerations? The problem is not solved until effective corrective action is taken.

Analysis of Competing Hypotheses[48]

1. Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.
2. Make a list of significant evidence and arguments for and against each hypothesis.
3. Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence and arguments, that is, identify which items are most helpful in judging the relative likelihood of the hypotheses.
4. Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.
5. Draw tentative conclusions about the relative likelihood of each hypothesis rather than prove them.

6. Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.
7. Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.
8. Identify milestones for future observation that may indicate events are taking a different course than expected.

Action as Rational Choice[49]

1. *Goals and objectives*. National security and national interests are the principle categories in which strategic goals are conceived. Nations seek security and a range of other objectives.
2. *Options*. Various courses of action relevant to a strategic problem provide a spectrum of options.
3. *Consequences*. Enactment of each alternative course of action will produce a series of consequences. The relevant consequences constitute benefits and costs in terms of strategic goals and objectives.
4. *Choice*. Rational choice is value maximizing. The rational agent selects the alternative whose consequences rank highest in terms of his goals and objectives.

The Wise Choice Process[50]

1. What is my present situation?
2. How would I like my situation to be?
3. Do I have a choice here?
4. What are my possible choices?
5. What is the likely outcome of each possible choice?

Thresholds: Toward a Decision-Directed Life[51]

1. See the situation clearly
2. Know what you want
3. Expand the possibilities
4. Evaluate and decide
5. Act

Appendix B

Common Thinking Traps

Normal human minds exhibit a tendency to fall into a number of common "thinking traps." A few of these are briefly listed in this appendix. Biases or "thinking traps" have been studied by psychologists and other behavioral

scientists. Research in this field can be helpful to decision makers who wish to design their decision processes in an attempt to avoid them. Awareness of these traps can also, perhaps, help diagnose what may have gone wrong when unsatisfactory decisions are being analyzed and evaluated during a post-decision quality review.

1. Framing bias
   (a) The way the question is asked drives the way it is answered. You will be unlikely to solve a problem you cannot define.
   (b) A poorly framed problem is unlikely to result in a wise choice.
   (c) Why? Framing places emphasis on different objectives and the way we perceive them.
2. Confirmation bias
   (a) The tendency to decide what before why.
   (b) We tend to focus on the things we like or expect to see.
   (c) We are drawn to information that confirms our initial thinking.
3. Anchoring bias
   (a) Allow initial impressions to dominate our perspective.
   (b) Particularly prevalent when working with numbers.
4. Overconfidence bias
   (a) The tendency to be more confident than correct.
   (b) Tendency to allow or accept estimates that fall within a very narrow range.
   (c) Works with the anchor bias to seriously cloud our critical thinking ability.
5. Sunk cost bias
   (a) Unwillingness to admit a mistake by placing concern with self-esteem ahead of service of the mission.
   (b) Forgetting that decisions only influence the future: hanging onto past decisions and not letting them go.
   (c) Failing to focus sharply on the variables that affect *this* decision.

References

1. Kennedy, R.F., *Thirteen Days: A Memoir of the Cuban Missile Crisis*, W.W Norton & Company, Inc., New York, 1971, p. 89.
2. March, J., (with Chip Heath), *A Primer on Decision Making: How Decisions Happen*, The Free Press, New York, 1994, pp. viii–ix.
3. Ibid., pp. viii–ix.

4. Schlesinger, A.M., Jr., *A Thousand Days: John F. Kennedy in the White House*, Houghton Mifflin Company, Boston, 1965, p. 246.
5. Heuer, R.J., Jr., *The Psychology of Intelligence Analysis*, Government Printing Office, Pittsburgh, PA, 2003, p. 87.
6. Hammond, J., Keeney, R., and Raiffa, H., *Smart Choices*, Broadway Books, New York, 1999, pp. 84–85.
7. Schlesinger, Jr., *A Thousand Days*, p. 257.
8. Cited in James Surowiecki, *The Wisdom of Crowds*, Doubleday, New York, 2004, pp. xv–xvi.
9. Ibid., p. xix.
10. Ibid., p. 235.
11. Ibid., p. 10.
12. Ibid., p. 77.
13. The National Commission on Terrorist Attacks upon the United States, July 2004.
14. Ibid., p. 78.
15. Ibid., p. 79.
16. Ibid., p. 81.
17. Janis, *Groupthink*, p. vii.
18. Ibid., p. viii.
19. Ibid., p. 244. See Figure 10-1 on page 244 for a helpful diagram of the "groupthink" theory.
20. Ibid., p. 262.
21. Ibid., pp. 262–271.
22. 't Hart, P., *Groupthink in Government*, The Johns Hopkins University Press: Baltimore, MD, 1990, p. 1.
23. Ibid., pp. 294–295.
24. Schlesinger, Jr., *A Thousand Days*, p. 807.
25. Janis, *Groupthink*, p. 274.
26. Kennedy, J.F., "Preface" to Theodore Sorensen, *Decision-Making in the White House: The Olive Branch and the Arrows*, Columbia University Press, New York, 1963, *In* Allison, G.T., *Essence of Decision: Explaining the Cuban Missile Crisis*, Little, Brown and Company, Boston, 1971, p. vi.
27. March, *A Primer on Decision Making*, p. 186.
28. Janis, *Groupthink*, p. 15.
29. Schlesinger, *A Thousand Days*, pp. 294–295.
30. Ibid., p. 293.
31. Janis, *Groupthink*, p. 9.

32. Wyden, P., *Bay of Pigs: The Untold Story*, Simon and Schuster, New York, 1979, p. 316.
33. Ibid., p. 16.
34. Schlesinger, Jr., *A Thousand Days*, p. 290.
35. Ibid., pp. 255–256.
36. Ibid., p. 248.
37. Ibid., pp. 296–297.
38. Ibid., p. 250.
39. Ibid., p. 297.
40. Ibid., pp. 802–807.
41. Kennedy, R.F., *Thirteen Days: A Memoir of the Cuban Missile Crisis*, pp. 89–90.
42. See Surowiecki, *The Wisdom of Crowds*, pp. 171–191, for an account of the decision making surrounding reentry of the NASA space shuttle Columbia.
43. Janis, *Groupthink*, p. 10.
44. Allison, G.T., *Essence of Decision: Explaining the Cuban Missile Crisis*, Little, Brown and Company, Boston, 1971, pp. 2–3.
45. March, J. with Chip Heath, *A Primer on Decision Making: How Decisions Happen*, The Free Press, New York, 1994, pp. 2–3.
46. Hammond, J., Keeney R., and Raiffa, H., *Smart Choices: A Guide to Making Better Life Decisions*, Broadway Books, New York, 1999, pp. 6–9.
47. Drucker, P.F., The effective decision, *Harvard Business Review on Decision Making*, Harvard Business School Press, Boston, 2001, pp. 2–3.
48. Heuer, R.J., Jr., Psychology of Intelligence Analysis, U.S. Government Printing Office, Washington, D.C., 1999, pp. 95–109.
49. Allison, G., *Essence of Decision*, Little, Brown and Company, Boston, 1971, p. 33.
50. Downing, S., *On Course*, 4th Ed., Houghton, Mifflin Company: Boston, 2005, pp. 35–36.
51. Burglass, M. and Duffy, M.G., *Thresholds Teacher's Manual*, Correctional Solutions, Inc., Cambridge, MA, 1974, p. 2.

National Security Executive Orders and Legal Issues

12

ROY SHANNON

Contents

Introduction

It is axiomatic that the U.S. is a nation of laws. From our inception as a unique republican experiment over 2 centuries ago, we, as a people, have struggled to account for the dark forces of human mendacity from both our enemies and our own citizens. The weapon of choice has been our Constitution and the laws and procedural framework that flow from its precepts. Uppermost in the Founders' minds was the evil that humans can do to one another. They were acutely aware the most formidable engine for oppression was government, for they witnessed the excesses and depredations of unrestrained rule and rulers all around them in colonial America. The Founders sought something better. Freedom, though a cherished ideal throughout history, was a rarely glimpsed almost mythical creature in human societies

up to that time. A bold group of farmers, tradesmen, lawyers, landowners, merchants, ministers, and soldiers all came together to create and, more importantly, to implement the greatest mechanism yet devised for the establishment and maintenance of personal liberties. No one has improved on their efforts in the 216 years since. That work of collective genius, our Constitution, is the foundation upon which the American edifice stands. Its wisdom has guided us through all of our tribulations as a nation and all the threats to our survival, internal and external. Our nation now faces yet another trial, perhaps our greatest, with the tension between government and freedom at its core. As it has before, the Constitution is there to guide us and by remaining faithful to its principles we will survive and triumph in this epoch of international terrorism.

The notion that a strong, effective central government could exist while providing the people with the freedom to generally live as they pleased was once considered to be utopian sophistry. Our success has proved the point. The problem is that we can never rest, we can never have respite because we must be vigilant and proactive in maintaining what we have struggled to create. Because of what America represents, the age-old forces of fear, envy, repression, and intolerance must resist us. If they do not, our way of life would likely quickly spread to most of the world. The tangible menace of international terrorism is a raging conflagration that threatens to engulf the world unless definite active steps are taken to snuff it out. Feeble "Chamberlain-ism," forgotten in most of Europe with its amnesia and malaise, will only embolden an implacable enemy. Corrupting the tenets of a great faith, irrational jihadists pursue a single-minded goal aimed at nothing but the destruction of a society such as ours. The core principles of our Constitution are anathema to the creed of fatwa-fueled ideologues of jihad. The two just could not be farther apart. Because of this misdirected devotion to destruction in the name of God, our nation faces a threat to its security as great as any that we have faced in the past. Thus, national security, job one for any government, must now be the central focus of national policy. Do it we must, but we must not sacrifice our own sacred principles in the process. By remaining faithful to the Constitution in this epic battle, we will win in the end. This chapter surveys the tools at our disposal to prevail in this crucial fight and still remain loyal to the rule of law that sets us apart as a nation.

Basic Constitutional Principles and National Security

The war on terror is a war like any other, differing only in the composition of the combatants and the battlefields.[1] While it may seem counterintuitive pairing war and law, all of our "wars" or military engagements at home and

overseas have been conducted according to the law.[2] National security, of course, now includes much more than just waging war, but this is a useful place to start our survey. A basic understanding of the Constitution is essential in analyzing and comprehending this burgeoning area of the law. National security law is developing rapidly into a distinct discipline and the implications affect all citizens.[3] While courts have always ruled on cases involving what we now call national security, it is a recent development that these issues have become a focus of national attention.[4] All national security law and jurisprudence, from 1789 to the present, is rooted in the Constitution. We now briefly pause to trace its growth and development.

Constitutional Foundation

The Founders drafted the Constitution with the images of tyrannical colonial rule fresh in their minds. Excesses of totalitarian government, here an aristocratic monarchy, were well known and understood. We had just won independence and it remained to be seen if we could win the future. Also fresh were the failings of the Articles of Confederation, a looser proto-Constitution. The Founders were also acutely aware of our fledgling nation's vulnerability to attack and predation from the global European powers. They had to contend with internal dissensions. The Founders were committed to a federal system with a separation of powers with checks and balances. While easy to state, it required the best minds in America to forge into being. They ultimately succeeded, as we know. However, it is still a work in progress, and the genius of the Founders was to build a system that could adapt over time to changing demands.

The basic essential was personal liberty guaranteed for all citizens, followed by security from internal and external threats. The rights of the States were of paramount concern lest they be dominated by an all-powerful national central government. Trade, banking, and sovereignty all had to be addressed along with all the other competing forces. The only way to do it was to make everyone, in government and ordinary citizen alike, all subservient to the rule of law. Many of the Founders were deeply mistrustful of standing armies, given the excesses of British soldiers and mercenaries on these shores. Yet, they realized the necessity of armed forces and sought a way to have a credible armed defense force that would be subservient to civilian authority. The final problem was: who would wield power and how? Would power be shared or consolidated in an executive? When you consider all of the complex competing interests, it is all the more amazing the Founders succeeded in balancing them fairly in a workable system of government of, by, and for the people. After heated debates, the Founders struck the delicate balance between liberty and security.

> It is impossible to consider the degree of concord which ultimately prevailed as less than a miracle.
>
> **James Madison**[5]

The solution was federalism. The Founders' vision was to create a centralized national government of separate, limited powers while the states retained their identity and sovereignty, thus we became the *United* States. Government functions would be split into three core functions allocated to distinct, independent, and coequal branches. In a nutshell, the laws would be made by Congress (Art. I, §1), they would be executed and enforced by the executive branch (Art. II, §§ 1 & 3), and the law would be interpreted and applied by the judicial branch (Art. III). No branch would be superior to any other.

The national (or federal) government would do the things only a centralized government could do best, foremost of which was to provide for a national defense and maintain foreign relations. It just made no sense for every individual state to carry on separate relations with foreign powers or conduct military campaigns on their own, as such actions would certainly affect the rest of the country. What was needed was for the new U.S. to act uniformly in matters of defense and foreign relations. We needed to speak with one voice to the rest of the world. The best way to do this was through an executive officer, but many of the Founders were suspicious of personal authoritative leadership because it seemed too much like a monarch or dictator.

More complicated was determining the legislative process. The Continental Congress had been in existence from the beginning of the Revolutionary movement and a Congress had lumbered through the Articles of Confederation period (1781–1787) just after we won independence. Thus, the notion of a representative body was sacrosanct in the emerging political psyche. Its composition was a source of hot disagreement. Some favored a unicameral national legislature with membership based on the population of a state. Critics noted this would allow for "mob" rule and that the majority states would always have things their way. Another proposal was that representation is equal regardless of population, and this in turn led to a criticism that small states could unfairly restrict the legitimate concerns of larger states by combining to block matters important to the large states, a tyranny of the minority. The brilliant compromise struck was a bicameral legislature composed of a House of Representatives whose membership was based on proportion of population and a Senate whose membership was an equal two senators from each state. Either body could propose laws, but the proposed legislation would have to be approved by both houses. This ensured a thorough review of all laws and the lengthy process of review ensured fairness because of the intense scrutiny. Certain tasks were allocated to a particular house. For instance,

appropriations bills originate in the House of Representatives (Art. I, § 7), but the Senate can propose amendments. Another example is only the Senate may refuse or ratify treaties the U.S. makes with foreign powers (Art. II, §2), and only the Senate approves the appointment of officers and judges by the president with their "Advice and Consent" power (Art. II, §2). While the House of Representatives has the sole power to seek an impeachment of an officer or judge of the U.S. (Art. I, §2), only the Senate may try federal officials or judges following an impeachment (Art. I, §3).

The task of Congress may be summed up by its obligation to provide for the "common defense and general welfare" of the U.S. (Art. I, §8). Subsumed under its lawmaking authority, Congress has a number of specifically enumerated powers many of which are relevant to national security (Art. I, §8). The most important such power is that only Congress may declare a state of war. Congress also raises and funds the army and provides for and maintains a navy. Congress defines the rules and regulations of the armed forces including rules of engagement. This branch also has virtually unlimited power to regulate commerce both at home and internationally. Congress also determines the rules governing immigration and naturalization. Modernly, Congress determines the rules for intelligence, counter-intelligence, and criminal offenses. Under the necessary and proper clause of Article I, Section 8, Congress may make all laws necessary to carry out its constitutional mission. In appropriate cases, Congress may delegate rulemaking authority to executive agencies. In such cases, because Congress has authorized the legislation, the regulations have the force of law even though actually written by executive branch agents. Absent such direct authorization, however, the executive branch may not make law on its own. This express delegation is how federal agencies regulate activities within their sphere and often how they regulate themselves. This delegation is also the source of authority behind presidential executive orders (EO) that have the force of law.

One important caveat should be noted: While Congress may delegate *rulemaking* authority to the executive; it may not delegate its constitutionally bestowed power to *legislate*. In other words, only Congress may create a given legislative schema, but they may permit an agency, like the CIA, National Security Agency (NSA), Department of Energy, or any other to develop rules and regulations because of the agency's greater expertise in an area. Any lawmaking "power" the president does have is limited to suggesting bills to Congress. Any rules the executive agencies create are subject to review by both Congress and the courts. The basic point is that the executive branch may not make law out of whole cloth, and any rules it does appear to make is only done by and subject to Congressional acquiescence and approval. Thus, an EO from a president has the force of law as long as it is issued pursuant to one or more acts of Congress. The distinction is a fine one and often leads to collisions between the president and Congress over many issues,

national security in particular. We will shortly examine the main cases brought in the wake of these disputes.

Turning now to the executive branch, the Founders, even the suspicious ones, acknowledged the need for an executive. There was no denying the need for a head of state. The devil was in the details. Consistent with their vision, the Founders crafted an executive that served as a check on the possible abuses of power by the other branches. Congress makes or authorizes law, and the executive has the general obligation to "take care" that the laws are "faithfully executed" (Art. II, §3). The executive branch may not create legislation, but rather carries it out. Just as a single ruler can abuse power, so can a group. In view of this, the executive in our system can act as a check on Congress's attempts to pass unfair, unwise, or unjust laws through the exercise of the veto (Art. II, §3). Pursuant to the presentment clause of Article I, §7, all laws created and passed by Congress must be presented to the president to approve or reject. If a law is signed by the president, it is the law of the land. If rejected by veto, it goes back to Congress where the veto can be overridden, but only if there is a two-thirds majority in both houses. In practice, vetoes are rarely overridden. Thus, the executive serves as a check and balance on Congress. Congress, in turn, can act to check executive acts.

The chief executive is the president, of course, assisted by other officers provided for in the Constitution. Modernly, we have seen a continuous growth in executive personnel and agencies tasked with the original mandate. As with Congress, the president can and does delegate responsibilities. Beyond the basic obligations, the president has certain significant national security duties. The president is the commander-in-chief of the armed forces and the militia (Art. II, §2.). When or if Congress declares war, the president leads and directs the military to engage the enemy. As noted, the president must enforce the law. This is important for national security because of the overlap of criminal law into almost all areas of defending the nation. Through the Departments of Justice, Treasury, Homeland Security, and others the executive branch has vast responsibility for law enforcement and investigation. In fact, most of our approach to terrorism before the September 11, 2001 tragedy was largely one of criminal investigation and prosecution.

There are a host of other laws relating to the common defense and general welfare of the country the president must see are enforced. The president is the constitutional officer designated to receive foreign ambassadors and negotiate treaties (for approval by Senate). The effect of this has been to make the executive branch the unified voice of the nation in foreign affairs. In cases of attack on our interests here or abroad or invasions of our territory, the law permits the president to respond with the necessary force to meet the threat. This comes out of the duty to take care to faithfully execute the laws Congress provides for our defense and welfare. The president need not wait for a congressional declaration of war before committing

our troops to protect American lives and property, but if he or she does, it must be pursuant to lawful authority. Congress can check military excesses or misadventures of a president by cutting funding for the purpose and legislating against them. This scheme has proved remarkably workable in our history, providing flexibility to deal with a variety of major and minor crises. Similarly, the president has the power to respond to national emergencies such as disasters or other calamities.

The final part of the constitutional triumvirate is the judicial branch (governed by Art. III of the Constitution). Less well known and understood, this branch is coequal with the other two. The president appoints federal judges, who are in turn approved by the Senate. Unlike other federal officers, federal judges are appointed for life, thus it is presumed they are free from the influence inherent in having to be beholden to another for your position. However, the lifetime appointment is valid only during the person's "good behavior" in office. Like the president, judges may be impeached and removed from office for misconduct or crimes, and scores have been so removed. Because the judiciary is independent, they can interpret and rule the constitutional validity of laws or government actions. Theirs is the final say (*Marbury v. Madison*, (1803) 5 U.S. (1 Cranch) 137, 177). When a law is struck down, it may no longer be enforced. Thus, the judicial branch may act as a check on both the Congress and the executive branch. The courts can examine and invalidate executive acts as violations of the law. Courts may not, however, rule on purely political questions. These are limited to circumstances where the matter is textually committed to another branch as a duty or there is a dispute between the other branches that the Constitution requires be settled between the branches, and the court will not step in because there are no judicially manageable standards in these cases. It should be noted, though, that the Courts always may say what the law is, in the sense of what it means.

As with the other branches, the judiciary may be checked and balanced by the other two. The president gets to choose who to appoint, the Senate gets to approve or reject the choices. Misbehaving judges may be impeached and removed. The courts may strike down laws or acts as unconstitutional, but Congress may also act in the court's wake and pass legislation that reacts to court rulings. Any law Congress passes is law until it is successfully challenged by someone harmed by the law's effects. The courts may not go out and seek laws to strike down, but must wait for the cases to come to them. Congress also has the power to determine the structure of the court system to a large degree by establishing all courts inferior to the Supreme Court. In this way, Congress can theoretically determine the court's ability to handle caseloads in a timely way. The Supreme Court may not be abolished, however, since it is a constitutional mandate. Since its inception, the Supreme Court and the other federal courts have ruled on matters of national security and

war powers. While the body of law is not as large as with other areas of the law, it is growing continually and is the bedrock for the important national security decisions we face today. The present time is, in many ways, a watershed for the field because many judicial questions left open from past cases must now be answered.

The foregoing is not intended to be a comprehensive explanation of our federal system as it relates to national security. Such an exposition is beyond the scope of these chapters or, indeed, of this book. The preceding is merely a preliminary grounding to permit the reader to understand the underpinnings of national security law and the constitutional players. The basic lesson to take away is that our system is foremost a system of laws, and that no person or institution is above them. The law is the great leveler. This does not mean that people and institutions do not attempt to ignore and usurp the law for their own ends. Human malevolence mandates law in the first place. It permits us to live together, albeit far from perfectly, and survive. The law provides a way to deal with the evil and plain carelessness of people in a consistent and direct way. The law provides the necessary rules and boundaries for how humans conduct themselves toward each other. The law must guide us in all endeavors, war, and national security especially. The U.S. Constitution is the finest example, arguably, of such a legal framework. Following its precepts is essential as we head rapidly toward unknown frontiers in the dark hinterlands of international terrorism. The potential for man's inhumanity to fellow man was never greater than it is now. We have to guard against the inevitable threats that are coming, and we need to conduct ourselves according to our cherished legal principles while we meet these threats. A tall order, but nothing less than we are capable of addressing.

Application of Constitutional Principles to National Security and the Continuing Rise of Presidential National Security Power

> The law spoke too softly to be heard amidst the din of arms.
>
> **Plutarch's Lives: Caius Marius**[6]

The above quote from the great Roman general and consul Caius Marius captures the fear that the Founders had regarding the law in times of war or threats to order and security. It is one thing to follow the law in calm times. It is quite another to follow the law during wartime, an invasion, attack, or other civil unrest. Yet to have a principle, and to have it be meaningful, we must adhere to the law at all times, peaceful or not. The temptation to ignore the law is great under the exigencies of wartime or other national emergency. It is precisely this temptation during such dire circumstances when we must

adhere to the law most strictly. To do any less is to be hypocritical and to abandon any pretense to moral hegemony.

In our modern epoch of international terrorism, one generally dominated by devotees of radical Islam, the executive branch is the primary player in reacting to the threat. The power of the president is probably higher now than at any time in history, possibly excepting that of Franklin Roosevelt during World War II. In any event, presidential power has been on the rise since FDR and now is seen to be quite expansive.[7] Part of this is due to modern interpretations of constitutional grants of executive powers and part is due to the relatively recent phenomena of "executive custom" and "congressional acquiescence" dating from World War II.[8] While there are probably a number of factors contributing to this, two are useful to consider and they are the rise of the administrative state in the form of executive agencies and the need for uniform quick response to national security threats.

Modern technology has made bringing death and destruction to large numbers of people increasingly easier. Our free society, extensive coastlines, and porous borders make it easy for terrorists and others to enter and move within our territory. We are also the world's leading economic engine and greatest military power. All of this, joined with hatred for our freedoms, makes us an attractive target for the forces of terrorism. Because of the speed and ever-increasing destructive potential of attacks against our interests, we have had to develop the ability to rapidly respond to attacks and to develop a capacity to detect and prevent such attacks. Retaliating and defeating the enemy is not enough anymore. The lethality of modern weaponry and terror tactics, combined with the specter of weapons of mass destruction mandate a proactive policy of preemptive action against these threats. The one branch of government equipped to deal with the threats most efficiently is obviously the executive branch via the military, intelligence community (IC), and law enforcement.

The brief survey of our constitutional structure laid out the big picture of how our federal system works. While ours is a system of separate powers, it is not one of separated powers. In other words, the Founders intended the powers be divided permitting checks and balances against excesses, but they also intended that the branches of government interact and cooperate. The powers overlap both by design and in practice. Throughout our history, the executive branch has had to act time and again against foreign and domestic threats to national security. Declared wars have been few while there have been scores of undeclared wars and other military operations during our history. Congress has typically been there to support the executive and has authorized the actions, but not always. The courts have decided the challenges to the actions giving us a growing body of decisional law to guide the legality of future executive actions. It is the nature of executives to give orders in

carrying out their mission. These orders have always been given by our presidents beginning with George Washington. The modern vehicle often employed is the EO. We shall now trace the historic use of presidential powers and directives to act in national security matters and examine the legal issues raised.

Express and Implied Presidential Powers

As noted, only Congress can declare war. Declared wars are said to be "perfect" in the Constitutional sense, but most conflicts are overwhelmingly of the undeclared "imperfect" variety.[9] In addition to declaring war, Congress can authorize force by granting letters of marque and reprisal, which are limited legislative authorizations to use particular force against a particular group (Art. I, §8). Congress also determines the rules of capturing enemy property on land or sea (Art. I, §8). There are only five instances of formal declared wars in our history: War of 1812, Mexican War, Spanish–American War, World War I, and World War II. However, the imperfect wars we have engaged in are legion. We have taken these actions repeatedly from the beginning of our history. Noteworthy examples are our naval responses to the Barbary Pirates from 1801 to 1816, the Quasi-War with France when American merchant ships and our fledgling navy had to confront French privateers,[10] the Boxer Rebellion in China, police actions in Central America, Libya, and Yugoslavia air raids, Grenada, up to Kuwait, Iraq, and Afghanistan. These are but a few, since our armed forces have reacted hundreds of times in large and small ways over history.

The Founders intentionally divided the war-making powers. Congress can authorize conflict, but the president is the commander-in-chief. Congress reacts to events, but generally it cannot do so with the speed necessary to address an immediate threat. The executive branch, in contrast, has usually been capable of rapid responses to threats. A review of Article II shows how few are the president's express powers. The Oath clause of the second section requires the president to defend the Constitution, but does not spell out duties as with Congress. Section Two also provides the commander-in-chief power, but neglects to describe specific powers or limitations. This area is both the president's principal claim to exercise military or intelligence powers and is also the main source of ambiguity and disputation. Some famous cases have determined some contours, but the question of full extent of presidential authority in the face of enemy attacks or other emergencies, especially those falling short of total war, is still open.

In addition to the commander-in-chief power, presidents may make treaties with advice and consent of the Senate (Art. II, §2). However, while needing consent to bind the nation into a treaty, none is required for the president to terminate a treaty [*Goldwater v. Carter* (1979) 444 U.S. 996].

The president may appoint the officers of the U.S. also with Senatorial advice and consent. Congress may and has vested the president alone the power to appoint "inferior" officers or those below judicial or cabinet level. The president receives foreign ambassadors or other dignitaries.

The president has "executive" powers to carry out his office by virtue of the Vestiture clause in Article I, §1. Perhaps deliberately, the Founders did not spell out precise powers, and perhaps wisely, since no one could probably ever foresee all of the powers necessary to carry out the office. Thus, since the express powers are few, a doctrine of implied presidential powers has arisen. The "Take Care" clause of Article II, §3 requires the president to take care all laws are faithfully executed. The precise meaning of this seemingly limitless power is still being debated and determined. This question was examined in the eloquent and seminal case of *Youngstown Sheet and Tube v. Sawyer* 343 U.S. 579 (1952). For many reasons, *Youngstown* is the most important case for weighing presidential actions and, by extension, for national security.

The background of *Youngstown* is important. We were fighting an undeclared war in Korea under Truman. Labor disputes threatened to cut steel production vital to the war effort. We were also at the threshold of the Cold War, desperately building and maintaining a strategic nuclear force to deter the Communists. Via EO 10340, Truman ordered his Secretary of Commerce to take possession of the affected steel companies to keep the materials flowing. The steel companies challenged Truman's authority to seize the factories. In a spirited 6-3 decision, the case established the guidelines for courts weighing whether presidential actions are constitutional or not. The court struck down Truman's act because it could not find any sustaining constitutional or congressional authority for the edict. The court reiterated that presidents may only enforce law, not make it. Justice Black's majority opinion laid out the reasoning and communicated the judgment, but there were five other concurring opinions along with the dissent. The most significant of these is the concurrence of Justice Jackson. It is his opinion that lays out the test for which *Youngstown* is best remembered.

Justice Robert H. Jackson is widely regarded as one of the greatest Supreme Court justices and one of its most artful writers. Justice Jackson never attended college and became an attorney from an apprentice clerk, passing the New York bar in 1913. He rose by merit to become the Solicitor General of the U.S. (the government's chief litigator before the Supreme Court) and was the American prosecutor at the Nuremberg war crimes trials of the Nazi leadership. Like the Founders, Jackson was well schooled in the excesses of governments living as he did through the turbulent first half of the 20th century and being witness to the wars, upheavals, and triumphs spanning the period from World Wars I and II to the Cold War. He prosecuted the Nazi inner circle. He knew firsthand what can happen when governments

run amok unrestrained by the rule of law. He knew also that freedom is not free, that it requires great effort and sacrifices to create, nurture, and perpetuate.

As noted, the court found that the president's power to act, if any, must stem either from an act of Congress or from the Constitution itself. No statute in 1952 authorized executive seizures of private steel industry property, war or no war. Nor were there any laws from which Truman's act could be fairly implied. There were (and are) laws permitting property seizures, but none of the conditions required were applicable in the case at hand. Thus, the court was insisting on an express power for the action, which it found lacking. The government strenuously argued for an expansive interpretation of the president's aggregate powers in that this seizure was part of power *implied* from the "take care" clause. The court agreed with the government that the president was supreme in making decisions in the theater of war, but that the "theater" did not extend to commandeering private factories on these shores in the wake of a labor dispute. Such disputes were the premise of lawmakers not law enforcers. Congress simply had not authorized any such action.

We know Congress has enumerated powers and that the president also has a few such spelled out powers. Justice Frankfurter noted that the president has unenumerated powers like the take-care power and commander-in-chief, but that this did not mean "undefined" powers. We must remember the Supreme Court says what the law means ["It is emphatically the province and duty of the judicial department to say what the law is" *Marbury v. Madison*, (1803) 5 U.S. (1 Cranch) 137, 177]. Therefore, it is the Court who determines what the powers of the executive are or are not. The government argued that Congress had often acquiesced in presidential acts, looking the other way. Frankfurter countered that even so, habitual practice did not magically transmute such acts into ones that could supplant the laws or the Constitution. Thus, presidential powers could not be acquired by some tacit tradition of letting the executive branch simply have its own way.

While all of the opinions made important points, it was Jackson who saw the crucial issue. The debate went beyond whether there was or was not an express executive authorization. Jackson's insight was that presidential power could not and should not be fixed. To function in such a demanding and all-important post, the president's powers would necessarily have to fluctuate to some degree. Jackson also recognized that this very essential fluctuation might prove to be too much of a temptation to some future chief executive seeking to aggrandize his own power. What was needed was a test to assess when presidential acts were in constitutional bounds or out, something the courts had perambulated around but never precisely delineated. Jackson laid out a three factor test: (1) When the president acts pursuant to an express or implied authorization of Congress, his authority is at its maximum; (2) when the president acts in the absence of a grant or denial of congressional authority he must rely on his independent powers, and the

validity of the acts is in a "zone of twilight" where the courts must balance the act against the circumstances necessitating it; and (3) when the president takes measures incompatible with the expressed will of Congress (or the Constitution), his power is at its lowest ebb and courts will heavily scrutinize such acts to see if they upset the constitutional balance.

The first prong is clear enough and guided the court in the case. The other two are more problematic. While cumbersome, the *Youngstown* test is the typical tool in rating presidential actions. Most of constitutional law cases are decided using balancing approaches and those involving presidential actions are no exception. Deciding cases involving executive actions is particularly thorny because of the sparse directions for the office in Constitution. Because of this the courts must take up the slack. Interestingly, there is not a large, well-developed body of case law on the subject. Arguably, we are now in the period where these issues relating to the limits of presidential powers will be decided. Until something better comes along, *Youngstown* has and will continue to guide court analyses of executive actions. Despite the ample gray regions, the test articulated by Justice Jackson can be very useful in assessing EOs in the national security area.

Defining Modern Presidential Actions

Since *Youngstown* and its progeny apply to executive or presidential actions, we should pause briefly and define what we mean by presidential actions, the most important of which for our study here is the EO. Presidents have always issued orders, directives, and proclamations. Such acts are not surprising coming from an executive, but rather expected. The president and other executive officers must give orders to subordinates to carry out their offices. In appropriate situations, orders must be given to citizens. The rub is in whether the order is dictated by law (and is legal) or whether the order dictates law (and is illegal). Since the inception of our current government in 1789, the vast majority of the 13,000 EOs and 7000 proclamations issued have fallen into the former category. There is no problem with orders that are given consistent with the mandate to faithfully execute the laws. The difficulties arise when an order seems to demand something for which there is no other supporting authority other than the language of the order itself.

In our early years, the lines were less blurred and situations less complex. An early example is Washington's proclamation during the Whiskey Rebellion of 1794. In 1792, Congress had authorized the president to command insurgents to disperse and retire and to permit the president to call out the militia to quell insurrections. When distillers revolted against government revenue collectors, Washington issued appropriate orders to deal with the rioting whiskey makers. These proclamations withstood court scrutiny since they were "public act[s] of which all courts of the United States are bound to take notice,

and to which all courts are bound to give effect."[11] Andrew Johnson's unpopular proclamation of general pardons for southerners fighting in the Civil War is another example differing only in that this order was based on the president's express Article II power to pardon people for offenses against the U.S.[12] Both of these acts would be upheld under the first prong of *Youngstown*.

Even though almost every president since Washington has issued such orders, they have rarely been the subject of judicial review.[13] As it is, only two such directives have been invalidated by the courts.[14] About 240 have been modified or revoked by subsequent legislative acts.[15] However, with over 13,000 EOs issued since the first formal designation of this type of executive act in Lincoln's term, it is obvious the EO is a frequently used presidential tool. It is easy to see how such a tool might become a favorite method for a president to exercise power. It is also easy to see the potential for abuses, especially considering the virtual absence of challenges to these acts. The risk of abuse is compounded in the national security area since most of the information and conduct involved is secret for obvious reasons. Most of the substance of a typical EO is open for all to see, generally. However, in matters of war or intelligence—or anything else coming under national security classifications—the executive branch can withhold materials forming the legal basis of these orders by claiming the need for secrecy essential to protect national security. This can make it difficult to evaluate whether the few standards there are governing EO have been followed.

Expanding Use of Executive Orders

Ever since Lincoln, there has been a gradual increase in the use of EOs. Teddy Roosevelt began a 20th century trend of widespread use of the orders.[16] All the modern presidents since have followed suit. Wartime seems to produce particular spikes with Wilson issuing 1791, FDR issuing 3723, and Truman with 905.[17] This is natural, likely, since conducting war is arguably the president's most important duty. War and war powers are also probably the most well-analyzed aspects of national security law. Because we are at war at present and because EOs are likely to increase both in number and impact during wartime, we should look at the war powers jurisprudence. We will then examine the other powers under which presidential EOs are delivered: foreign affairs, emergency powers, and executive privilege.

War Powers/Commander-in-Chief

We now have a basic grasp of the constitutional allocation of war responsibility within our federal government. The last declared war began for us in 1941. All the conflicts since have been of the imperfect variety, including the

Cold War. The same period saw the rise of the U.S. as the dominant world power both economically and militarily. Because we occupy the position of global primacy, we have faced constant threats to our hegemony. Just as Congress can declare a state of war, it may also recognize when one exists (as in when we have been attacked).[18] Defending our place has required the necessary growth of a worldwide intelligence and counter-intelligence capacity. To protect our physical security, our economy, and our way of life it has become imperative to be able to know what our enemies are up to. Our success in intelligence has been uneven, with some triumphs and egregious miscalculations. One thing is certain, true and lasting victory in any war depends on sound intelligence. The War on Terrorism we now wage is no exception.

The perceptive reader will apprehend that federal war-making powers between the branches necessarily overlap. By extension, the legal control of all of the government organs contributing to successful war waging must also overlap, especially the intelligence field. Congress organizes and funds the armed forces and the intelligence community (IC) agencies. Congress also regulates the forces they provide, but only the president may command them, and any attempt by Congress to circumvent this ultimate command authority is unconstitutional and invalid.[19] One conclusion to draw is the Founders wisely intended the branches to cooperate in times of national crises like war. So far their vision has worked reasonably well. The main reason is that Congress and the president have almost always been in agreement about the existence of and response to a threat. The accord after the September 11 attacks is but one example. Congress authorized the executive branch certain emergency powers under various acts like the Patriot Act of 2001 (and its recent renewal), Homeland Security Act, Aviation and Transportation Security Act, Suppression of Terrorism Financing Act, 9/11 Commission Report Implementation Act, among others.

The aforementioned acts along with the Authorization to Use Military Force have arguably equipped George W. Bush with the most sweeping powers since Franklin Roosevelt. The administration immediately promulgated a number of EOs to fight the war on terrorism: Military order (MO) for Detention, Treatment, and Trial of Certain Noncitizens in the War Against Terrorism,[20] EO on Terrorist Financing,[21] EO Establishing Office of Homeland Security,[22] and the Homeland Security Directives 1 and 2.[23] A detailed examination of the contents of these acts (and the resulting EOs) is well beyond the scope of this chapter, but it is fair to say that these acts have granted the president a formidable array of weapons and constitute an expansion of executive power as great as any in our history.[24] Further, because they are acts of Congress, the president is presumably at the height of authorization under *Youngstown* to issue orders since he can claim he is constitutionally acting pursuant to legislative authority.

There is an obvious problem with this seemingly neat authorization, however. It is one of interpretation of precisely what is authorized. The executive branch will generally press for expansive interpretations, whereas Congress or aggrieved parties will seek narrow ones. This tension goes all the way across our history. We noted the Quasi-War with France above. During that conflict Congress passed an act authorizing the president to order naval seizures of American owned or controlled trade vessels bound to French ports.[25] The Secretary of the Navy decided we should nab such vessels going to or from French ports, and our Captain Little seized a Danish flagged vessel, prompting the owners to sue for damages.[26] Our government argued that the law made no sense unless the ships could be seized both ways and that it was easy for American ships to haul up other flags, so the only reliable way to carry out the law was to board and seize all suspect vessels.[27] The court held that the executive was bound to carry out the law as written, and even though the government's argument was reasonable, it was not for the executive to second-guess Congress' will given the plain language of the act.

Thus, the early court was willing to chart boundaries and limit executive actions. However, as time passed courts were less and less willing to interfere and more likely to find ways to defer to the executive and uphold such actions. By the Civil War, this was becoming evident. Lincoln blockaded southern ports before any formal state of war had been determined and seized ships. As with the *Little v. Barreme* case earlier, the owners sued.[28] There was no authorization from Congress for the blockade or seizures, they argued, so the U.S. was liable for damages incurred.[29] This would fit into the second "twilight" prong of *Youngstown.* This time the court sided with the government holding the president was bound to respond to an armed rebellion, a war, whether or not the conflict had been formalized.[30] This decision established that presidents in the future could take action in cases of attack or other military exigency and were authorized to do so by the Constitution itself under both the "take care" and commander-in-chief clauses. Obviously, this freed the executive branch up considerably and the decision seemed to place an important responsibility on the president to waste no time in acting to defend the country by waiting for formal congressional acknowledgments of war. The effect of *The Prize Cases* was to mandate the president to act whenever American interests were threatened. The executive branch would now be increasingly proactive instead of merely reactive.

The trend continued. Lincoln continued to hack open new paths of presidential power. In fact, he fought the war for 3 months purely by directives, as Congress was not in session.[31] Lincoln called up militias, blockaded ports, appropriated Treasury money, and even suspended the writ of habeas corpus for the duration of the war.[32] Congress later approved Lincoln's actions, but what was remarkable was how all this transformed the presidency into a dynamic take-charge office. Except for a short lull after the Andrew Johnson

administration, the executive branch has kept rolling forward. Andrew Johnson followed Lincoln's lead in using the new-found power of the office and it got him impeached. He survived, and Congress temporarily managed to restrain the new thrashing executive beast, but nothing could take things back to the way they were before with a dominant Congress and suppliant executive. Rutherford B. Hayes noted:

> The executive power is large because it is not defined in the Constitution. The real test has never come because the presidents have down to the present been conservative, or what might be called conscientious men, and have kept within limited range. And there is an unwritten law of usage that has come to regulate an average administration. But if a Napoleon ever became president, he could make the executive almost what he wished to make it. The war power of President Lincoln went to lengths which could scarcely be surpassed in despotic principle.[33]

A new executive era was dawning. Teddy Roosevelt came along like a force of nature busting trusts, projecting American might globally, subjugating far-flung territories, arresting social problems, and so on, and issued 1006 directives.[34] Twentieth-century presidents never looked back. Wilson, like Lincoln, had almost "dictatorial" powers following his unprecedented declaration of a national emergency.[35] The lessons were not lost on Franklin Roosevelt. He issued 3723 EOs in his term, beginning his tenure with a declaration of national emergency during the depression.[36] As the commander-in-chief, FDR took forceful measures to preserve national security. The most controversial were his orders to relocate Japanese–Americans to internment camps in the interior.[37] FDR claimed this power to severely curtail the civil rights of 112,000 American citizens solely under his commander-in-chief authority.[38] The courts upheld the acts and the authority claimed.[39] FDR's presidency was just one long national emergency where he assumed not only full executive power, but legislative power as well, his word was simply law, and Congress acquiesced in what he wanted.[40]

Truman followed suit, but like Andrew Johnson, Truman would be a target for the other branches of the government when they came to their senses. Truman, like FDR, tried to seize essential war industries, but this time the court was the one to thwart him in *Youngstown* as noted. Despite this reining in, Truman still acted decisively and to the ever-expanding limits of presidential power. At least, the *Youngstown* decision was there to set some guidelines to assess future executive acts and it remains the principal yardstick. Truman was the first Cold War president and it was during his tenure that our modern IC was born.[41] We were now the dominant world power and, despite critics, the leader of the free world. We would now be deeply involved in foreign affairs.

This new world, its new problems, and our new commitments and involvements would begin to blur lines between presidential powers. Deciding when and how to make war or engage armed forces would now become inextricably linked to our foreign relations and global interests we now had to protect.

Foreign Affairs

We have seen how the president is the officer identified in the Constitution with specific foreign affairs powers. He negotiates treaties and receives ambassadors. He appoints our officers and consuls. He is our most visible representative to the rest of the world. In a world of around 200 nation–states, the national security implications of relating to all these entities are significant, particularly where some nations are in competition with us or are hostile. Complicating the picture are the stateless global terror organizations, we must deal with like Al-Qaeda. Equally vexing are the blurred lines between what is foreign and domestic in a globalized economy. We are beyond the era of formalized warfare and clearly identified foes. We are now into a fluid, shifting period of "enemy combatants" and terrorists. Are they criminals, soldiers, or something else? How we define them makes a significant legal difference relevant to their status and the rights they receive. Even defining warfare has become murky. To survive, we must adapt and meet the threats. To maintain our principles, we must do it constitutionally.

Since World War II, we have been in scores of quasi-wars around the world. Our IC has fought desperate battles with our rivals. We have been challenged on every front from military to economic to cultural. The main branch of government meeting the new threats has been the executive. Most Americans think of the president as the leader of the country and with some sound justification. The president is the personification of the U.S. to the rest of the world. Since the office is so essential to how the world perceives us and foreign affairs is essential to national survival, we need to survey the background of the foreign affairs powers.

The notion of the president as the foreign affairs focal point has existed throughout our history, but it took a court case to solidify it into a concrete one. In *United States v. Curtiss-Wright Export Corp.*, the court declared that it was essential the president be the "sole organ of the federal government in the field of international relations."[42] Nor did this power need to come from some act of Congress; rather it need only be exercised consistently with constitutional principles.[43] Sovereignty and relations between sovereigns are inherent qualities of nationality and a nation must speak with one voice to the world. The *Curtiss-Wright* court noted the absurdity and danger to our position in the world if different branches of government took different positions, showing different faces to the world. The only exception, and a prudent one, is the Senate ratification of treaties the president negotiates.

Otherwise, it is the president who speaks for us. This case establishes another deep and abiding presidential power and one that is frequently wielded through EO.

Thus, the president is the foreign policy generator. Because he is the sole organ of foreign relations, the executive branch is the one with the expertise and quick response capability necessary to cope with the modern world. *Curtiss-Wright* establishes this primacy in foreign affairs. The problem is what is foreign and what is domestic in the modern world. Everything is global this or global that. Modern travel, commerce, and the Internet are eroding traditional border concepts. "Here" is now "there" in many ways, and us vs. them is less meaningful because often "they" are us. Once it becomes difficult or impossible to determine foreign vs. domestic, it is equally difficult to determine the scope of presidential authority. No one disputes presidential power in foreign relations. The open question is what happens when the line between foreign and domestic disappears. Right now there is no complete answer. For the moment, if the matter is arguably or mainly one of foreign affairs, the executive branch calls the tune. As it stands, the president has wide discretion in choosing how and when to commit American forces and resources.

Emergency Powers and Executive Privilege

As noted, the notion of a national emergency originated with Woodrow Wilson.[44] We have seen how *The Prize Cases* granted the president the freedom to act quickly when we are attacked. It is his duty to react to threats. We shall continue here with some other cases that outline more of the contours of presidential powers to act. In 1890, a U.S. Marshal shot a man attempting to attack a Supreme Court Justice riding circuit (as they did back then), whereupon the California authorities tried to arrest and prosecute the marshal for murder.[45] The U.S. government promptly challenged the marshal's detention as illegal and sought his release via writ of habeas corpus. The case went to the Supreme Court. *In re Neagle* is significant for several reasons. The state authorities argued no federal law authorized Marshal Neagle to protect judges or shoot people attacking them. The court held the president had clear power not only to take care the laws were faithfully executed, but also to protect the personnel tasked to do this. Thus, the executive branch has the ability to order personnel to preserve the integrity of criminal justice systems of the U.S. This is the beginning of the vast powers of the U.S. Justice Department. Even though Neagle was protecting a judge, the implication was that federal officers had the power to enforce the law by all reasonable means at their disposal in the states. Thus, federal officers had clear independent power to carry out their constitutional functions

unimpeded by state authorities. In federal matters, the federal government would trump the states. Obviously, this is a very significant source of power for the president.

Neagle involved a law enforcement officer doing his duty. One of the open questions still debated was the role of the military in civilian law enforcement. It is clear that in warfare or invasions the armed forces would be in control, what is less clear is what things short of open armed conflict or insurrection would permit the president to use troops to keep order. In our history, there has been a strong distaste for giving troops authority over civilians. It goes against the whole notion of a civilian commander-in-chief. Remember, the Founders feared tyranny and one sure route to despotism is unadulterated martial law. Because of this fear and our value for civilian law enforcement authority, Congress passed the Posse Comitatus Act in 1878.

This act forbids the military from executing the law in the sense that civilian law enforcement does. The idea is to prevent the creation of a national military police. As with almost everything else in the law, however, there are exceptions. The act prohibits federal (or state) civilian authorities from calling on troops to do the job normally done by police. Yet, we all know troops get called out all the time to patrol the streets in the wake of disasters. We all saw the military patrolling our airports after September 11. Another law, the Insurrection Act,[46] provides a number of exceptions permitting the president to call forth troops for quelling riots, civil unrest, or disasters. The law permits calling up the armed forces whenever circumstances make it "impracticable" for civilian authorities to keep order.[47] This begs the question as to what happens to civilians arrested by troops in these situations. The answer, for now, is that military courts do not have jurisdiction over American citizen civilians in general.

The foundation law is set forth in *Ex parte Milligan*.[48] In this case, the Union Army tried a civilian for planning a raid to free Confederate prisoners after the end of the Civil War. Milligan was arrested by soldiers, tried by military court, and sentenced to hang. The Supreme Court said his detention and trial were unconstitutional and ordered his release. The court held that civilian citizens like Milligan were entitled to the full constitutional safeguards because his home state of Indiana was not under siege or in a war zone, he had not violated any law (then) that was punishable in a civilian court, and he was not in any way connected with the military services. In *Reid v. Covert*, the court held that civilians living on a military base are still entitled to an Art. III (civilian) court even for criminal offenses they commit on the base.[49] As always, there are exceptions to the general rule of these cases.

Civilians of belligerent nations we are at war with may be tried by military courts when our armed forces occupy their territory.[50] Enemy civilian belligerents who commit hostile acts against us or our forces may also be tried by the military (spies, saboteurs, and terrorists).[51] Congress gave the military

the right to try civilians who accompany the armed forces overseas and who are "service connected" because of jurisdictional problems with U.S. courts in trying offenses connected with such people.[52] The foregoing categories seem clear enough, but the lines are often blurred when dealing with stateless terrorists, international criminals, American citizens joining or aiding terrorists, and "enemy combatants." President George W. Bush issued an MO specifically permitting the armed forces to detain, investigate, try, and punish operatives of Al-Qaeda or related groups.[53] This was done pursuant to both his constitutional power and congressional authorization under the Joint Resolution to Use Military Force. In any event, Bush is on strong *Youngstown* first prong ground here. It remains to be seen how far a president could go in issuing EOs that expanded the classes of persons subject to military justice. The matter would have to be resolved in the courts.

The foregoing apparatus is set up to potentially collide with our traditional methods of dealing with terrorists. Up until the aftermath of September 11, the matter was one of criminal justice. If we could apprehend an offender who perpetrated some proscribed act of terrorism (through the FBI, DEA, U.S. Marshals, Border Patrol, U.S. Customs, Coast Guard, etc.), he was tried in U.S. District Court under our criminal laws, with full constitutional rights. The War on Terrorism has changed that landscape as numerous laws have been passed to change the status of terrorists. The most notable change is to put these persons into a system of military justice. This sea change in tactics is the subject of heated court litigation at this very moment. A number of cases are working their way through the system right now on these very topics. Some civil libertarians might be tempted to say we are abandoning cherished principles, whereas others might counter that terrorism is a new and destructive force requiring new approaches. The issue is whether it makes sense to grant noncitizens the full panoply of constitutional rights when those same persons are dedicated to the outright destruction of this nation and the very Constitution that offers these rights. The outcomes will govern our approaches to terror and terrorists in the future (for more on these topics, the reader is directed to Chapter 13 of this text.)

The next area of presidential power is found in what has come to be known as the doctrine of executive privilege. This is simply the executive branch's justifications that some information must be kept secret either to protect the national security of the country or to permit complete debate and analysis of alternative courses of action when the government is creating policies. The first one is easy to understand. Obviously, there is a compelling need to keep some secrets to protect ourselves. There is a vast array of diplomatic, military, scientific, economic, and political information that must be managed and preserved for our nation to survive and prosper. But presidents must also be able to fully and candidly discuss matters of state with advisors and attorneys without fear the discussions will become public.

Any risk of disclosure might tend to foreclose options or stifle debate. More options are always better than fewer in statecraft. Thus, secrecy is a necessary thing, but it has the capacity for abuse like anything else in governance.

As with other powers, the courts have shaped the privilege doctrine. As is their habit, the courts give the executive the widest discretion in what they can conceal. In fact, national secrets in the form of presidential communications are presumed to be privileged, absent a specific showing of adequate need.[54] At least one example of this need is where there is a specific need for evidence in a pending criminal investigation as when Nixon had to give over the famous tapes of Oval Office conversations to Watergate prosecutors.[55] However, many unresolved questions remain about the extent of claims of privilege by the executive. No doubt some will make it into the courts for determination. As of now, it remains a gray area like much of the rest of executive power.

The Intelligence Community

Intelligence is one of the most important functions of our government. It is simply the gathering of all possible information from all possible sources for leaders to consider in deciding on courses of action or policy. It has also come to refer to actions done to influence events in a nonattributable or surreptitious manner.[56] Intelligence tradecraft modernly includes counter-intelligence or actions performed to thwart others from gaining intelligence from us, provide them with useless information instead, and to penetrate and gather information from rival clandestine agencies. Obviously, a detailed look at intelligence is a vast subject beyond the scope of this chapter. The examination will be limited to its relation to the EO we have been examining. If there is any field of executive branch enterprise that should be bound by legal controls, intelligence is the one. This is essential because the very nature of intelligence work, its inherent secrecy, makes the potential for abuses by an over-reaching executive very high. That same nature makes judicial review and control very problematic. Equally disquieting is that intelligence agencies, because of inherent secrecy, can insulate themselves from outside control, even that of the president, and carry on as they please answering to no one. Neither situation is one a free people can tolerate.

While we have had an intelligence capacity throughout our history in one form or another, the U.S. was late in creating a formal intelligence structure. This was accomplished by the National Security Act of 1947 that created the CIA and other agencies and the National Security Council (NSC) framework. There are about 15 "spy" agencies in our government and all were theoretically supposed to be coordinated under the NSC. The NSC is a body headed by the director of the Central Intelligence (DCI) Agency and made up of various cabinet, intelligence, and military officials and whose

purpose is to collect and analyze intelligence vital to national security. It is a purely executive branch enterprise and it answers to the president. Combined, it is an enormous part of our government, largely autonomous, and one vested with vast responsibility to protect us and our way of life. The rest of the government, the military in particular, depends directly or indirectly on timely information gathered, processed, and disseminated by the IC to make decisions that affect our lives everyday. The importance of the IC is hard to overstate.

While it is easy to understand the need for an IC, it nevertheless seems to be incongruous with the basic American value of free and open government. We do not like secrets. We have a free press whose job it is to inform us about things. Yet, we probably could not survive long if we gave away all of our secrets. Secrecy in the modern world is just something we cannot live without. Further, also essential to our survival and prosperity is to have a well-developed capability to discover the secrets of others, particularly those of our enemies. No lesson can drive this point home better than the failings of the IC leading up to September 11.[57] There are a number of reasons we did not get the information in time to be useful. One is the problem of processing the immense volume of material we obtain every day. Another is recognizing its value. There are translation issues. However, the biggest problem was probably the lack of real coordination among all the disparate agencies within the IC. They just did not talk and share enough, and some actually competed against one another. Despite its horrendous cost, September 11 woke us up to the deficiencies in our IC. George W. Bush and Congress both acted to begin to correct them.

Combating terrorism has been typically approached in two ways in nations having to deal with this scourge. The first is a crime model and the other is a war model. It remains to be seen if a new model should be developed that addresses the shortcomings of the existing models. Before September 11, the American response was generally one of crime and law enforcement. The IC figures in both models. The crime model is reactive to a large degree and confers upon the terrorist suspect a host of procedural and substantive rights as he is prosecuted through the criminal justice system. Those rights are at a maximum if the act is on these shores and the actor is found here or is a citizen. The rights are those of any criminal defendant, the fourth, fifth, sixth, and eighth amendment rights in particular.[58] Each crime and defendant involves criminal investigations, arrest, arraignment and charging, extradition, and trial. The aftermath of September 11 revealed the limitations and potential risks of strict adherence to the criminal model.

The alternative model is the war model, which uses military and diplomatic means to fight terror. This is a proactive approach where the government aggressively pursues and engages terrorists and those who harbor and support them at or near their bases of operation. The idea is to interdict the

terrorist before he can strike. This approach does not require the full array of constitutional protections due a criminal defendant because the terrorist's status is now one of "enemy" or "unlawful" combatant and subject to the Uniform Code of Military Justice or possibly various treaties.[59] Put simply, under the criminal model, if a terrorist is a criminal, every accused terrorist gets a day in court with all the rights of any defendant. Under the war model, our armed forces may capture, incapacitate, and kill our enemies with whom we are at war. George W. Bush opted for the latter model and it is at the core of what is now called the Bush Doctrine.[60]

The doctrine adopted by Bush was one of preemptive prevention in the war on terrorism. The central idea was to pursue, capture, and destroy terrorists and to destroy any capacity of any entity to support, harbor, or train terrorists. The main theme is to stop them before they do any (more) damage. Given the magnified destructive power available to well-funded terrorists, Bush's strategists reasoned this was the only expedient approach. Putting the U.S. on a war footing was the most efficient and prudent step to eliminating existing terror operations and the capacity to mount continued terror strikes. No one knew what risks were in the offing, not even the IC with any degree of precision. A war model is probably the only long-term approach to deal with an implacable, ideological enemy who has sworn the destruction of the Western world. The Bush administration had to choose, and quickly, how best to prevent a potentiality for a succession of September 11 level attacks. While debate rages in hindsight, it is probably significant to note not another single such massive attack has occurred in the interim since the Bush policies have gone into implementation.

The main advantage to a war model is that warfare does not implicate the inherent protections, constitutional and otherwise, that criminal proceedings do. The war model is obviously desirable from the executive point of view since it frees the executive to act quickly and decisively. Rapid response to threats of mass murder or infrastructure destruction is paramount. Further, at least for now, the current administration has the backing of Congress under the aforementioned Authorization to Use Military Force and the U.S.A. PATRIOT Act. Until Congress revokes it, or passes something else, the president has authorization to use "all necessary and appropriate force" to *prevent* acts of international terrorism against us or our interests.[61] This is fertile ground indeed for a host of EOs.

How does the IC relate to this war vs. criminal prosecution discussion? Intelligence is paramount to the success of both endeavors. Nor should the two terrorism models be viewed as mutually exclusive. Rather, both should be used to complement each other. It is even possible what we are seeing is the development right now of a third model that takes useful elements from both of the older extant models. Neither of the two traditional models precisely fit the emerging definition of the stateless international terrorist.

What we are seeing right now is the evolution of a policy approach to a new problem. An old adage is that necessity breeds invention. The international stateless terrorist is a new paradigm. As we have adapted to changing security climates in the past, so too will we adapt to this one, but we will do so within the guidelines of our constitutional principles. Sound intelligence gathering and analysis will remain essential.

Basic Primer in Intelligence Law

Because of its crucial role, we need to have a basic blueprint of the IC legal architecture. Intelligence is information for action typically divided into three parts: (1) foreign intelligence (espionage), or information relating to the capabilities, intentions, and activities of foreign powers; (2) counterintelligence (CI), or acts conducted to protect against espionage and penetration of U.S. assets by foreign intelligence services; and (3) covert action (CA), or clandestine actions designed to influence events abroad (and ominously, at home, some fear) without the involvement of the U.S. being immediately apparent.[62] Obviously, sound intelligence permitting us to know things ahead of time is desirable. So too is sound counterintelligence to protect our own secrets. CA remains controversial, but the CIA is authorized for such actions in peacetime unless the president designates other operatives to do so via an EO.[63]

The president is at the apex of the IC pyramid. Next are the National Security Advisor, the Director of National Intelligence (DNI), and the heads and deputies of the various agencies.[64] The president chairs the NSC composed of the vice president; secretaries of State, Defense, and Treasury; National Security Advisor; Chairman of the Joint Chiefs of Staff; the DNI; the DCI; White House Chief of Staff; and Chief White House Counsel. The Attorney General is usually present and other government heads are invited to meetings as necessary.

How does it work? The president or the NSC (with presidential approval) identifies an area of concern: foreign intentions, capabilities, threats to our vital interests, military, political, economic issues, and so on. Planners, operatives, analysts, technicians go into action. Plans are developed and then agreed upon in three stages. The first is the Deputies' Committee, made up of all the "No. 2s" in the various agencies (titles like deputy, undersecretary, etc.). Next, plans go to the Principals' Committee, made up of the vice president, the NSA, the DNI, the DCI, and the secretaries of State and Defense. The final stage is approval by the president, when a given intelligence plan is signed off as a presidential directive, a presidential decision directive, or as a full-blown EO. This three-stage process is mandated by the 9/11 Commission Report Implementation Act (9/11 CRIA) and is regulated by all branches of government. The executive branch plans, implements, and reviews the proposed intelligence actions (via the Department of Justice). Congress has oversight

responsibility through its intelligence committees. The courts regulate the IC activities through the Foreign Intelligence Surveillance Court (FISC; warrant applications, domestic surveillance, etc.) or by direct review of cases brought by aggrieved parties. In addition, citizens may request declassified materials under the Freedom of Information Act (FOIA).

Espionage is as old as humankind. All nations do it to some degree, and so it is expected and tolerated. More problematic is CI and CA. On our end, CI is very criminal prosecution oriented since we are often looking for leaders, turncoats, moles, double agents, and the like. There are a host of laws dealing with breaches of classified information and the people involved.[65] Some spies are protected by diplomatic immunity depending on their status, but many are not. Our own people who betray us are subject to the full weight of criminal prosecution. IC agencies are often required to clear proposed actions with special intelligence courts sitting in closed sessions (the FISC noted earlier) consistent with the terms of the Foreign Intelligence Surveillance Act (FISA) of 1978. The basic requirement, for domestic operations, is for the IC agency (remember, all are part of the executive branch) to initiate the approval process in the FISC for an action, and then the FISC, sitting in secret, decides if the government has the authority to carry out the action. FISC judges are all Article III federal judges who take turns in the FISC. The Chief Justice of the Supreme Court selects the court (usually a federal district court in or near Washington, D.C.). There are about 600 to 1000 requests a year and the vast majority are approved by the court.

The FISA applies only to completely domestic operations. The IC has carte blanche in foreign operations. Also, monitoring communications that have one end overseas and one in the U.S. are also fair game for automatic monitoring not requiring court approval. If the communication is totally within the U.S., at least one of the parties must not be a U.S. citizen, or else the monitoring requires full Fourth Amendment protections. Thus, embassies are fair game in most cases. FISC hearings are all in secret in hardened rooms and only government officers are permitted, no defense attorneys are allowed. All records of proceedings are secret as well. The need for this secrecy should be obvious. The good thing about FISC is that ordinary sitting federal judges are on its bench, members of an independent branch of government. This system is a workable one, despite criticisms, and is faithful to the constitutional ideal of the branches cooperating in an essential area of government each checking and balancing the other.

There are numerous other laws on the books regarding intelligence, homeland security, and the like. The most notable addition is the Uniting and Strengthening America by Providing Tools Required to Intercept and Obstruct Terrorism Act of 2001(U.S.A. PATRIOT Act). The PATRIOT Act enhances certain surveillance authority, monitoring, seizures, and other acts the executive branch has in dealing with terrorism, but it was approved by

Congress, thus the presidential authority under the act is consistent with *Youngstown's* first prong. The act, however, must be renewed by Congress at intervals and its does not replace or diminish FISA or the FISC requirements. The PATRIOT Act should be viewed as one of those measures passed to deal with the exigencies of the moment. Congress retains the ability to withdraw the extra powers it provides the executive branch.

The area of intelligence where the executive branch traditionally has the greatest power is overseas. However, this distinction may be losing meaning in an increasingly global world. What does it mean anymore to distinguish between foreign and domestic? Is it geographical? What about cyber attacks? Does it refer to citizens of the U.S. and those of other countries? Where do stateless "enemy combatants" fall in? Where do we put terrorists who claim no national identity? What is domestic? What about threats to our oil supply or economy? Are those threats foreign, domestic, or both? If both, what does that do to our legal schema? Do noncitizen terrorists living here illegally as moles planning mass attacks of devastation qualify for full constitutional rights? Should they? Or do we need a new model to deal with the new threats the 21st century world burgeons with. These questions are just beginning to be asked, let alone resolved.

This period will most likely prove to be one of the most interesting and dynamic in terms of our constitutional system of government. No doubt we will rise to the occasion, but it will be exciting to see how we create a just and responsive system to the threat of international terrorism that remains true to the Founders' vision. It is true that the IC is an area where there is a great potential for abuse, but all the checks and balances are still in place. The courts are there to keep a watchful eye, and Congress can still approve or withdraw enabling legislation and Congress can cut off the financial tap. The fear of a runaway executive is not altogether hysterical, but the acts of the executive are always, sooner or later, illumined by the searing light of the Constitution. Presidential orders, EOs in particular, are seen by many eyes and pass through many layers of review. The strong and intricate constitutional lattice woven by the Founders does not lend itself to ready unraveling.

Though on the surface, executive action in the IC arena might seem the one most capable of abuse, it is actually one with the highest level of scrutiny at least from a checks and balances vantage. Any conspiracy to usurp power in some grand presidential gambit would have to be monumental. Numerous senior administration officials, military officers, and executive staff would have to be complicit. Next, judges would have to be bought off or intimidated. In turn, Congress would have to be fooled or cowed in some way. Lastly, it would have to be kept from the American people. The genius of the Founders' design becomes apparent. No matter how determined one group might be in seizing unwarranted power, it could never be completely successful because of the inherent checks and balances in our system of

separated yet inter-cooperative powers. As long as the balance of government remains faithful to the original design, no one branch can over-reach the others, even in an area so secretive and abuse-prone as that of espionage.

Concluding Remarks

This chapter is intended only to provide a basic grasp of the legal issues involved with the modern EO, the tool most frequently employed by presidents to affect both policies and actions. They often have the force of law, but not always. They arise in a variety of contexts, but most significantly for our study in the area of national security. A variety of topics have been raised in this chapter, many are vast in scope deserving encyclopedic treatments. We have examined the basic Constitutional framework of our government and the role of the three players. It is the executive branch's role to carry out and enforce the law. It is the executive who must defend the nation and carry on foreign affairs. The president is the commander-in-chief of the armed forces. In a very real sense, modernly, it is the president who is the "leader" and who is seen to command and direct the nation. Leaders lead by giving orders to subordinates who carry them out. Power to make others follow orders is a great power indeed and one subject to the potential for great abuse.

The Founders were eyewitnesses to such abuses. They knew the risks of an unbridled executive. They also were aware of the risks of the tyranny of the mob, especially if the mob were the ones making the laws. They also recognized the essential nature of an independent judiciary who could sit in dispassionate judgment on the correctness of the actions of citizens and those who governed the citizens. They forged a charter, a basic Constitution to be the supreme law of the land specifying principles from which no one could deviate. The Constitution is a product realized from the Founders' knowledge of the best and worst of the human character. The worst comes from concentrated power to rule others devoid of any accountability. The best comes from a free people consenting to ruling themselves with full accountability. Ours is not a perfect system, but it probably comes as close as any can devised by mere human beings.

The changing nature of the nation's role in the world has determined the scope and frequency of the EO. As the world grows more complex and dangerous, the challenge for American presidents becomes more daunting as they carry out their constitutional duties. National security is the most important job of any president and it encompasses many things. War, terrorism, espionage, weather, disease, and natural disasters all figure into the equation. Immigration, crime, and border security are salient issues pressing to be addressed. The economy, energy, and the quality of life are all certainly important national security issues. The president can affect all of these areas

by the vast power he wields in the modern era. Yet, we have seen how presidential orders are tempered by the other branches. There is a necessary push and pull. Modern presidents, even the most independent, took pains to make sure their orders were constitutional, even if they operated, consciously or not, at the edges of their power. We have seen that the truth is that the lines are not sharply delineated, and this was by design to allow the executive branch to be resilient, adaptive, and to grow.

The contours and boundaries of executive power are being shaped right now by global forces. A new era of law is taking shape before our eyes to guide future presidents. The powers of the executive branch evolve as new situations unfold, are debated, and finally decided by the courts. Those decisions are honored by the rest of the government because of the high value placed on the integrity of our constitutional system. Were it otherwise, an unscrupulous executive could simply ignore the courts. After all, they are powerless from a coercive standpoint, their authority being purely moral. The deference and respect we have for the authority of the courts in itself is amazing, especially when compared to the rest of the world. Our homage to the law, our commitment to the rule of law is something that sets our system apart. Our presidents have not always been fond of the decisions handed down, but they have abided by them. As long as this commitment remains sacrosanct, we shall endure. Contests between our governing bodies are settled by us in courtrooms without bloodshed or anarchy.

The president of the U.S. has the power to order things be done, but it is not an absolute power. It is a power tempered by the sensibility of checks and balances installed by the Founders. The likelihood of a future runaway president usurping the two centuries of constitutional review of executive action is remote. Respect for the law is one of the most American of sentiments. It is part of the American tradition, inseparable from our identity. Law is our governance; it is the great regulator and leveler. To deny the rule of law is to deny the defining characteristic of what it means to be an American. We were the first nation to put the principle to the test. To date, we remain the most successful.

References

1. See generally, Stephen Dycus, et al., *National Security Law*, 3rd ed., Aspen Publisher, New York, 2002, chap. 2.
2. Ibid.
3. Ibid.
4. Ibid.
5. Letter to Thomas Jefferson from James Madison, Oct. 24, 1787, Personal Papers of James Madison 10:207–215.

6. *Plutarch's Lives Translated from the Original Greek, with Notes Critical and Historical, and a New Life of Plutarch*, John Langhorne & William Langhorne (Edmond and Charles Dilly Publishers, London, 1770 ed.).
7. See generally, Stephen Dycus, et al, *National Security Law*, Chap. 3.
8. Ibid.
9. See *Bas v. Tingy*, 4 U.S. (4 Dall.) 37, 1800.
10. *Little v. Barreme*, 6 U.S. (2 Cranch) 170, 1804.
11. *Armstrong v. United States*, 80 U.S. 154, 156, 1871.
12. U.S. Constitution, Art. II, § 2.
13. Olson, W.J. and Woll, A., Executive Orders & National Emergencies: How Presidents Have Come to "Run the Country" by Usurping Legislative Power, Policy Analysis, No. 358, Oct. 28, 1999, p. 9.
14. Ibid.
15. Id., Appendix 3.
16. Id., see chart at p. 13.
17. Ibid.
18. See *Bas v. Tingy*, 4 U.S. (4 Dall.) 37, 1800.
19. Ex parte Milligan, 71 U.S. (4 Wall.) 2 (1866); *Youngstown Sheet & Tube v. Sawyer*, 343 U.S. 579, 1952.
20. Federal Register: Nov. 16, 2001 (Vol. 66, No. 222) pp. 57831–57836. Like an EO, an MO is a presidential directive to the armed forces to do something, and all presidential orders and proclamations, as well as federal agency regulations, are printed in the Federal Register.
21. Executive Order 13224.
22. Executive Order 13228.
23. Available at: http://www.whitehouse.gov/news/releases/2001/10/20011030-1.html and http://www.whitehouse.gov/news/releases/2001/10/20011030-2.html, respectively. These two directives set up the giant Department of Homeland Security and aggressive immigration policies to locate, detain, prosecute, and deport suspected terrorists.
24. See generally, Dycus, Chap. 4.
25. The Non-Intercourse Act, see *Little v. Barreme*, 6 U.S. (2 Cranch.) 170, 170, 1804.
26. Id. at p. 176.
27. Id. at pp. 176–179.
28. The Prize Cases, 67 U.S. (2 Black) 635, 1863.
29. Ibid.
30. Ibid.
31. Olson and Woll, *supra* note 13, p. 12.

32. Id. pp. 13–14; U.S. Const., Art. I, § 9 permits suspending the Great Writ in emergencies.
33. Watson, D., *The Constitution of the United States, Its History, Application and Construction*, Callahan & Co., 1910, p. 930 (from an interview with President Rutherford B. Hayes).
34. Olson and Woll, *supra* note 13, p. 15.
35. Ibid.
36. Id. p. 16.
37. Executive Order 9066.
38. *Hirabayashi v. U.S.*, 320 U.S. 81, 91, 1943; *Korematsu v. U.S.*, 323 U.S. 214, 1944.
39. *Supra* notes 37 and 38.
40. Olson and Woll, *supra* note 13, p. 17.
41. *See* The National Security Act of 1947, 50 U.S.C. 403-3 et seq.
42. 299 U.S. 304, 1936.
43. Id. pp. 312–320.
44. *Supra* note 35.
45. See *In re Neagle*, 135 U.S. 1, 1890.
46. 10 U.S.C. §§331–335.
47. 10 U.S.C. §332.
48. 71 U.S. (4 Wall.) 2, 1866.
49. 354 U.S. 1, 1957.
50. *Leitensdorfer v. Webb*, 61 U.S. 176, 1857.
51. *Ex Parte Ouirin*, 317 U.S. 1, 1942.
52. Unif. Code of Mil. Justice Art. 2(a)(11).
53. Military Order of Nov. 13, 2001: Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57, 833, 2001.
54. *In re Sealed Case*, 116 F.3d 550 565, 1997.
55. *U.S. v. Nixon*, 418 U.S. 683, 1974.
56. Armeringer, C.D., U.S. Foreign Intelligence: The Secret Side of American History I, Lexington Books, New York, 1990.
57. 9/11 Commission Report, available at: < http://www.gpoaccess.gov/911/>
58. U.S. Const. Amends. IV, V, VI, and VIII.
59. Uniformed enemy soldiers are typically imprisoned and adjudicated according to the terms of the various Geneva conventions. However, stateless terrorists, designated "enemy combatants," are held by the Bush administration to not fall within the Geneva terms. They are only entitled to basic human rights, such as food, water, shelter, and are also allowed to practice their faiths.

How and who may try enemy combatants is the subject of heated litigation working its way through the courts right now. More on this topic is examined in Chapter 13 of this textbook.

60. Speech by President George W. Bush at West Point Military Academy, June 1, 2002; National Security Strategy of the United States, Sept. 2002.
61. Joint Resolution for Authorization to Use Military Force, Public Law No. 107–140, 115 Stat. 224, Sept. 18, 2001.
62. O'Connor, T., Lecture Notes, North Carolina Wesleyan University, Sept. 16, 2005.
63. *Supra*, note 62; EO 12333 permits the president this latitude.
64. The DCI used to have the role of DNI, set up in the original National Security Act of 1947, 50 U.S.C. §§ 401, et seq. The 9/11 Commission Report Implementation Act of 2004 and the Homeland Security Act of 2002 changed the landscape by creating one cabinet level officer, the DNI, overseeing all the IC. Formerly, the DCI had been required to both take on this role and to head the CIA. Now the DCI reports to the DNI, a true national intelligence chief. Besides the CIA, the other agencies include: NSA, all the military branches intelligence units, the Defense Intelligence Agency, National Reconnaissance Office, National Geospatial Intelligence Agency, Departments of State, Treasury, Energy, and Homeland Security, and the FBI.
65. See generally Title 18, Chap. 37 U.S.C. §§792–799.

Courts-Martial, Military Tribunals, and Federal Courts

13

ROY SHANNON

Contents

Introduction

Chapter 12 examined the broader legal issues surrounding the modern executive order in our national security strategy. This chapter will focus on the narrower role military jurisprudence plays in the 21st century epoch of international terrorism. The last chapter provided a basic grounding in our constitutional system as it relates to national security law.

The last chapter also discussed the heretofore traditional approaches to terrorism: criminal prosecution and the war model. There was an analysis of the basic features, benefits, and drawbacks of the two models. The reader is urged to review Chapter 12 for a basic understanding of the U.S. Constitution in the national security strategy. This chapter will review the basic structure and legal issues surrounding the "war model" and the resulting military trials and detention that form an essential part of this approach.

Persons accused of crimes in the U.S. have a host of civil rights under the Constitution.[1] As noted earlier and in the previous chapter, the primary approach to terrorism prior to the formulation of the Bush Doctrine[2] was one of criminal investigation and prosecution. The Bush Doctrine redefines terrorism as a primarily military threat in that the terrorists have declared war against the United States and thus our armed forces may capture,

incapacitate, and kill our enemies with whom we are now at war.[3] The most striking difference between these two models is that terrorists apprehended under the war model are not afforded the full panoply of civil rights criminal defendants receive. They receive basic human rights similar to those of prisoners of war and are entitled to food, water, shelter, basic medical care, and the right to practice religious faiths.[4] As we shall see, they also receive other significant rights.

The war model is useful for many reasons, not the least of which is its capability to rapidly respond to threat conditions. Our military machine is the most formidable force in the world in terms of training and technology. We are also unexcelled in our mobility and response time. No force in the world today can match us, and most modern nation states, even the unfriendly ones, would not dare to challenge us. However, the modern era of stateless terrorists presents, at least superficially, a seeming departure from the traditional notion of uniformed armies and navies of sovereign nations meeting on the field of battle. We are used to the idea of a civilian vs. military dichotomy, but the recent religiously (and politically) inspired terrorism from groups like Al-Qaeda seems to blur that neat distinction. However, maybe there is not such a departure after all. What is needed is to perhaps begin thinking outside of the nation–state box when it comes to terrorists who wage war against us and the Western world in general.

The concept of war is one of those ideas most people think they readily understand, but it is hard to define precisely. Clearly, a World War II scenario is the classic example. War in that example is characterized by two or more armed national forces engaged in a contest authorized by the respective governments toward some end important to the government. The government of a nation who is attacked might react to protect its territory and people. A government bent on conquest might attack another nation. These are simplistic examples but they make the basic point. What about other concepts of war? Revolutions, insurgencies, police actions all involve armed forces and violence or the potential for violence. Even these differing manifestations still involve well-defined groups in conflict with each other. What is unique about the war on terrorism is that terrorists come from across all borders, ethnicities, and economic strata. They are looser coalitions of individuals not answering to a particular nation or government. For all intents and purposes, they may be said to be stateless.

There have always been anarchist or terrorist movements. They arguably differ from revolutionaries or resistance fighters in terms of their goals. The revolutionary seeks to overturn one government to replace it with another. The resistance fighter may be in an occupied country fighting to drive the invaders out, like the various underground resistance movement in Europe resisting the Nazis or the Soviets. Terrorists seem more dedicated to a creed of pure destruction of the West. They would argue that they seek to replace

the corrupt West with a pure Islamic theocracy, but there is scant indicia Al-Qaeda or similar groups are interested in anything like nation building. The primary focus is on destroying offensive things, people, ideas, and institutions. Even the Taliban who briefly controlled Afghanistan spent their time destroying rather than building anything. The Taliban was even threatened by 2000-year-old Buddhist rock carvings, which they dynamited.[5] These groups may have commonalities, but they are not unified in the traditional nationalistic or military sense. This diffusion does not make them any less dangerous or easier to comprehend.

Whether or not politicians and critiquing scholars agree on what to call terrorists, the fact remains they can and do represent a real, credible physical threat on the order of a military attack. More people died in the September 11, 2001 attack than in the Pearl Harbor attack of 1941. Labels are useful when there is leisure time for discussion, right now we have to fight the people who are trying to kill us. It does not matter whether they are in a uniform or a caftan. It is enough they have guns and explosives and the intent to harm us. It is time to expand the definition of warfare to meet the new threat. The nation is under attack from committed enemies be they "enemy combatants" or terrorists or jihadists or any other label. Because we are under attack, it is the job of the president to call forth the military to protect and defend the nation. This is the thrust of the Bush Doctrine noted earlier and in Chapter 12.

Because the military is the primary institution confronting the combatants of the War on Terror, it is essential to understand the underlying infrastructures comprising the military justice system as it processes the terror combatants it encounters. Many will be killed as a result of engagement with our forces. Many more will be captured and processed other ways. Some will be interrogated and either detained or interned in prison camps or disarmed and released. Some will require medical attention. Some will possess a status that brings them within the federal criminal justice system as with Jose Padilla and John Walker Lindh. The vast majority of battlefield survivors, however, will come under the jurisdiction of the military justice system.

Overview of the United States Military Justice System

The U.S. military justice system is one of the largest court and dispute resolution systems in the world as well as one of the largest criminal justice systems.[6] A detailed look at this vast system is well beyond the scope of this chapter. The system deals with all aspects of military life, personnel, and property. All service members are subject to the system. We confine our inquiry to the basic structure of the system and the principles of military law. Military law has two

concerns: (1) command and control necessary for an effective fighting force and (2) ameliorating the effects of warfare on noncombatants. With the advent of modern stateless terrorism, it now arguably has a third concern of what to do with the captured and detained terrorists.

Because of the sensitive nature of the conflict and the players, there are important intelligence and secrecy implications, all of which in turn have obvious implications for national security. All wars require intelligence tradecraft and this one is no exception. The difficulty in penetrating organizations comprised of persons from Middle Eastern cultures is daunting. This makes almost every captured terrorist a potentially significant intelligence asset. Further, the nature of the conflict makes it essential that we protect all of our own intelligence operations and assets. The high value we place on freedom of speech often makes the business of government secret-keeping problematic. Equally challenging is staying faithful to our cherished constitutional principles while coping with the demands of a state of war. Before determining what happens to enemy combatants in the system, we must also understand what happens to our own people in this system.

Basic Structure of Current Military Law

The military justice system is similar to the federal court system in many respects. Both are hierarchical in substance and procedure and both are subservient to the Constitution.[7] From there, the military system is obligated to follow federal law, regulations promulgated by the president (as commander-in-chief), the Secretary of Defense, the various branches of service, and the commanders.[8] Trials are generally conducted in courts-martial with review by a military appeals court, a civilian appellate court, with final review by the U.S. Supreme Court.[9] However, because of the specialized role of the military, it is appropriate that the system parallel that specialization. The Supreme Court recognizes the need for such a specialized system of jurisprudence.[10]

Due process is a basic theme in American law and it extends to the military as well. While our main focus is the national security implications of military detention, it is important to also understand the military justice system as it has evolved to the present day. The military is regulated by what is called the Uniform Code of Military Justice (UCMJ). The UCMJ was promulgated by an act of Congress under its Article I, Section 8 powers under the Constitution in 1951.[11] Thus, the UCMJ, like all other American law, rests upon a constitutional foundation. The Constitution provides that Congress has responsibilities to make rules to regulate the military and further establishes the executive branch in the person of the president as the commander-in-chief of the armed forces.[12] Congress chose to finally exercise its authority

in 1950 in order to streamline and unify the military justice system. Becoming effective the following year, the UCMJ represented a major revision to the system and is basically a complete set of criminal justice. Almost all of the familiar civilian crimes like murder, rape, robbery, theft, and drug abuse are codified, but it also includes the unique military offenses for which there are no civilian counterparts.[13]

The UCMJ is implemented through an executive order (EO) of the president, which Congress authorizes under the code.[14] This EO takes the form of a comprehensive legal volume known as the Manual for Courts-Martial (MCM). A great leap forward at the time, the law has remained current because as an act of Congress, it has been amenable to amendments added as necessary.[15] In 1984, we saw the introduction of a uniform code of Military Rules of Evidence (MRE) for court-martial proceedings.[16] The same year Congress reorganized the text of the act to follow particular procedural rules with these requirements grouped under what is called the Rules for Courts-Martial (RCM). Grouped together in the MCM, courts-martial law is divided into five parts: (1) preamble, (2) RCMs, (3) MREs, (4) punitive articles, and (5) nonjudicial punishment procedures.

A thoroughgoing examination of the history of military law is another expansive topic exceeding the scope of this chapter, but some salient points are worth noting because they bear on why the UCMJ is such a great feat of legislation. Our military law has its beginning in the British Articles of War in 1774. Both the American Articles of War and the Articles for the Government of the Navy predated our Declaration of Independence and the Constitution.[17] This fact is noteworthy because these systems were in place before the drafting of our basic rights and the creation of Article III federal courts.[18] Persons who went into the military were (and remain) subject to this alternate system. A complete analysis of all the differences between the systems and their consequences is a vast topic, but it is useful for our narrow inquiry to note that the old system did not afford a service member the protections guaranteed a civilian citizen under the Constitution. This disparity led to resentment and a gradual awareness of the inequity between the two systems. The two world wars saw huge numbers of persons joining the service, further highlighting disparities between the two systems. Finally, by 1947 Congress was holding hearings to overhaul the system. The hearings would lead to the UCMJ.

Thus, military law was moved into constitutional consistency with the rest of American law. Basic concepts of jurisdiction (the right of a court to hear and decide a matter and to have a right to have judicial power over the persons before the court) and due process[19] were included. Because the military is a command hierarchy, certain provisions had to be tailored for this difference from the civilian world. In the civilian realm, police agencies investigate crime and then the district attorney prosecutes the offender. The military has police-type investigation and enforcement, but the commanders

fulfill the role of the prosecution. The commanders decide when or if an offense is to be prosecuted.[20] The source of an offense report also differs from the civilian norm. Offenses covered by the UCMJ may come from military police, federal agents, local civilian police, or fellow military members.

Once a suspected violation is reported, a commander makes a preliminary inquiry.[21] From there, the commander can personally investigate or appoint investigators. Outside investigatory assistance may also be had. The investigation can range from quite informal to formal with a written report. Once the investigation is complete, the commander has several options in resolving the case. The choices range from no action, to administrative sanctions, to listed punishments under Article 15 UCMJ, to a full court-martial. With the final option, a charge is said to be "preferred," which is tantamount to a civilian swearing out of a complaint.[22] Short of a court-martial, commanders may choose punishments from the aforementioned Article 15. These include demotions, pay loss, restrictions to base, or duty alterations (extra work, like the infamous "KP"). This punishment is administrative in nature and does not equate to a federal conviction and, because of the relatively innocuous nature of the offense and adjudication, the accused does not enjoy a right of counsel. However, should a service member refuse the Article 15 sanction (as is his option), he may face an outright court-martial.

The hallmark of the UCMJ is the inclusion of constitutional rights and due process of law. Because of this, accused service personnel now enjoy rights against self-incrimination, to be informed of all charges before any questioning, and to have free military counsel be appointed or even to have civilian counsel if they can afford it.[23] If a commander deems a court-martial is called for, the accused may be confined pretrial if the commander feels circumstances warrant or the accused may be free on their own recognizance pending the outcome of trial. There is no bail. Once court-martial is chosen, it may take one of three forms: (1) summary court-martial, where one officer acts as prosecutor, judge, and defense counsel (only indicated for minor offenses and punishments); (2) special court-martial, or one presided over by a military judge, separate prosecution, and defense counsels, and with three "members" or persons who function like a jury (the members can be officers or enlisted if the accused is also enlisted, but the enlisted members must all be of superior rank to the accused); and (3) general court-martial, for the most severe offenses, with punishment up to death.

The general court-martial is the highest level reserved for the most serious offenses and punishments. It has the highest level of due process and is only indicated after a lengthy and impartial pretrial investigation.[24] The general court-martial is presided over by a judge and has five members, and the accused has full rights to counsel, confrontation, evidence production, and inspection very similarly to a civilian trial. What sets this proceeding apart is that the convening authority, or commander, can choose to follow the court

determination or disapprove of the findings and/or the sentence. In all general court-martial cases involving death or more than 1-year confinement approved of or not by the convening authority, the Military Court of Criminal Appeals automatically reviews the case. This court has the ability to reduce sentences it considers excessive. From there, a given case may be reviewed by the U.S. Court of Appeal for the Armed Forces (USCAAF). This review is purely discretionary as with other Federal Appeals courts. Also, as a last resort, a case may be appealed to the U.S. Supreme Court.

The foregoing is a very basic survey of the military justice system as it relates to military personnel. In addition, all military service members are bound by all other federal law and most local and state laws as well. The main difference for service members is who sits in judgment of them. It makes sense for the military to be the one to prosecute and judge its own members. It is fair and in keeping with the tradition of American law to be tried and judged by a system comprised of one's peers. The UCMJ is a complete system of justice in full accord with our cherished constitutional principles. However, the military justice system is required to adjudicate more than just the disposition of its own members. Often, the military must try and judge the people we go to war with. This responsibility looms conspicuously and perhaps controversially in the War on Terror.

Detention of Enemy Terror Combatants and Military Tribunals

War crimes. What does that expression mean? Like so many things we hear about the law and civil rights we think we know, but it becomes hard to precisely articulate. War is bringing destruction and death to our enemy until they yield or disappear. War involves using terrible measures to achieve victory. Civilian populations are fair game in modern warfare; just witness the bombings of European and Japanese cities during World War II. Was that a crime? The answer depends on the purpose of the action. If civilian targeting is done to hasten an end to the war effort by crippling the enemy's morale, manpower base, industry, and infrastructure, then the answer is likely no. If the goal in targeting civilians serves no strategic objective and is done to terrorize and eradicate a population, then it is yes. Torture, rapacity, and genocide are clearly over the line, as is the massacring of unarmed noncombatant civilians and prisoners of war. Yet many would find troubling the use of massive aerial bombardment or missile attacks because of the potential for collateral damage to civilians. Obviously, so-called smart weapons diminish this possibility, but they can never completely eliminate it. Is the unintentional but inevitable civilian casualty a war crime? Is it the victor who gets to decide what constitutes a war crime and who the war criminal is? These

complex unsettling questions admit of no easy answer and a detailed analysis is not properly had in this writing. However, one path to clarity in the war crime analysis might be the following: as it is with so many criminal questions, whether or not an action is criminal even in the war context has to do with intent and policy.

In the criminal law, the intent of the actor is generally an essential element in a criminal offense.[25] Thus, to be culpable for a crime one must have the requisite mental state. If one commits an act without intending a criminal result, there is no criminal intent and, therefore, no crime, even though there may be harmful consequences. This approach probably works for the war crime as well. While general criminal acts are those committed by an individual or groups of individuals for personal reasons, war crimes are acts committed by a person or persons adhering to a generalized policy or goal. An easy example is the Nazi regime under Hitler; another is the recent "ethnic cleansing" and other atrocities in the former Yugoslavia committed by all sides at one time or another during the conflict. The Japanese "rape" of the city of Nanking in 1937 is another, as might be the Iraqi actions in Iran in the Iran/Iraq War and by Saddam Hussein against the Kurdish people. If the policy or goal of a regime or organization is partly or wholly dedicated to the terrorization and extermination of a people or country, then acts in furtherance of that policy are probably war crimes. Most wars stop when the objective is realized. When you purposefully carry the destruction past that point as in seeking to wipe out a race or a faith, then you have crossed into the realm of the war crime.

The Nuremberg Trials (and the later trials of Japanese leaders) represent the most readily understandable modern recognition of the war crime.[26] The official policy of the German Government was the extermination of "impure" races, primarily Jews, but included other "non-Aryans."[27] The intent of the government in conducting warfare was not only conquest and military success, but also the genocide of entire ethnicities. Civilians in occupied countries already subjugated were targeted for torture and reprisals. Large numbers of innocent people were targeted for the acts of partisans resisting the occupation. Prisoners of war were tortured and executed in violation of Geneva Conventions, despite the fact that Germany was a signatory of the treaty.[28] It might be said the intent of the Nazi leadership was this genocide and nonstrategic liquidation of civilian noncombatants. By making this a national policy implemented by its military, the leaders of the government and military became complicit in war crimes. The book documenting the judgment at Nürnberg describes war crimes thus: "violations of laws or customs of war" including but not limited to "murder, ill-treatment or deportation to slave labor or for any other purpose of civilian populations … murder or ill-treatment of prisoners of war, … plunder of public or private property, wanton destruction of cities towns, villages, or devastation not justified by military necessity."[29]

The same document also describes crimes against peace as "planning, preparation, initiation, or waging of a war of aggression …"[30] It goes on to describe crimes against humanity as "murder, extermination, enslavement, deportation, and other inhumane acts committed against any civilian population, before or during the war or persecutions on political, racial, or religious grounds …"[31] Further, "[l]eaders, organizers, instigators, and accomplices participating in the formulation or execution of a common plan or conspiracy to commit any of the foregoing crimes are responsible for all acts performed by any persons in execution of such plan."[32] These definitions seem to need little in the way of improvement and seem eminently applicable to the War on Terror we face today. The useful thing about these definitions is that they do not require the offenders to be a national government or nation–state. Even though the Allies prosecuted the Axis national leaders, there seems to be no barrier to prosecuting organized international terrorists dedicated to identical goals. The overwhelming majority of victims of September 11, 2001 were innocent civilians. Nor is there any military justification for the destruction of office buildings, passenger planes, and innocent people by the thousands. Lastly, the terrorists could certainly be said to be waging a war of aggression against the American people.

Above we noted the current American approach to the War on Terror is a war model. This model has the advantages of speed, efficiency, and efficacy. It also takes most terrorist combatants out of the realm of criminal prosecutions where they qualify for full Article III court jurisdiction and constitutional rights. The issue is simple: should terrorists receive the full protection and due process that American citizens (or aliens) subject to typical criminal prosecution receive? The answer should be equally simple: no. The war enemies of this nation have never received such rights unequivocally. They have received a measure of due process doled out by the courts. The normal manner of trial and adjudication of "enemy combatants" has been by military tribunal. This form of justice has been upheld by the courts time and again. Can you imagine the absurdity of trying every individual soldier or camp guard who committed an atrocity in World War II in a federal court? Or the further absurdity of even making our courts available to every terrorist captured on the battlefields of Afghanistan or Iraq? Just because a terrorist is not getting a full day in federal court with appointed lawyers and appeals does not mean they are being denied all rights. Military tribunals provide such persons with due process protections, and even though the terrorists do not actually fall within the Geneva Conventions, they largely still are treated as if they did.[33]

Nevertheless, critics abound decrying the hypocrisy of a constitutional system such as ours providing a Bill of Rights for people here at home whereas denying it to the terrorists. We are said to have abandoned any pretense to moral hegemony by catching and warehousing these terrorists without resolving

questions about their legal status.[34] The truth is there are resolutions to many of these questions in well-settled cases. The courts are also presently working through a series of cases to settle other questions. We will turn to an examination of these cases and how the military tribunal process currently works in processing those captured on the battlefields of the War on Terror.

Military Tribunals and the Military Commission

The Roman maxim *Inter arma silent leges* (During war, the law is silent) might be said to be the guiding principle of national security law.[35] This might seem to mean that lawful authority is ignored during warfare, but it really stands for a different concept. The law of necessity, of preservation, has to take precedence in an armed conflict. If the nation is not preserved, the remainder of all laws preserving civil liberties are rendered null and void.[36] Our civil liberties are first and foremost a privilege of American citizenship. They also extend to persons coming under the civil and criminal jurisdiction of our courts (aliens, foreign civil claimants, treaty claimants, etc.). They have not historically been so radically extended as to include persons captured on the battlefield of a declared or undeclared war. Abraham Lincoln was criticized for the many steps he took that temporarily curtailed civil liberties, the most serious of which was the suspension (with Congress's approval) of the writ of habeas corpus.[37] The U.S. Constitution specifically permits the suspension of the Great Writ in times of invasion, rebellion, or when public safety requires it.[38] Lincoln responded to critics with typical eloquence saying, "Are all the laws, but one, to go unexecuted, and the government itself go to pieces lest the one be violated?"[39]

Well intentioned but unprecedented extension of full constitutional civil liberties to terrorist combatants is foolish if it diminishes the power of the nation to effectively wage a successful war on terror to defeat an implacable and dedicated enemy. The denial of full constitutional rights to captured terrorists is both sensible and legal as we shall see. This debate has not sprung full-grown from events of the last 5 years; it is rather an old one going deep into our history. One reason perhaps that it is so hotly disputed now is because up until the Congressional and presidential responses to September 11, 2001 our approach to the problem of international terrorism was one of criminal prosecution. September 11 revealed starkly the inadequacy of that approach and that is one reason the war model was prudently substituted. Looking at the case law may help illustrate the disparity.

In 1993, the World Trade Center suffered a bombing in its basement, bringing terrorism to these shores in earnest. Sheikh Abdel Rahman and a cabal of terrorists planned and carried out the attack. The attackers were tried as criminals for "seditious conspiracy and other offenses arising out of

a wide-ranging plot to conduct a campaign of urban terrorism."[40] Their First Amendment argument failed in a general denial of the appeals of their criminal convictions. The terror warning signs were there, but the U.S. was slow to recognize them. The crucial recognition did not come until after the tragedy of September 11, when the exigencies of a full-scale War on Terror forced the realization and a new approach was dictated by the circumstances.[41] The realization was simple and profound: One tries and punishes criminals; a nation in an urgent war must kill and incapacitate its enemies before they do greater harm; criminal law processes by their very nature are after-the-fact and secondary, whereas war is a primary response to defend and preserve the nation and its people.[42]

The *Rahman* approach was perhaps useful for limited, isolated, and sporadic terrorist attacks. Once they became massive in scale or potentially frequent, the war model was indicated instead. Once we began waging the war, the legal issues began arising and the courts began deciding them just as they have in all the wars preceding the current one. Two of the major ones are: (1) what rights and what legal status do terrorist combatants enjoy and (2) what distinctions, if any, do we draw between terrorists with citizenship vs. those who are noncitizens?

Enemy civilian belligerents who commit hostile acts against us or our forces may also be tried by the military (spies, saboteurs, and terrorists).[43] The case of *Ex parte Quirin* stands for this proposition. A German submarine deposited spies and saboteurs off of Long Island, N.Y. They were caught and tried by a military commission set up by the Roosevelt administration.[44] Haupt, one of those captured, had dual U.S./German citizenship and had returned to Germany to be a spy. He filed a writ of habeas corpus challenging the authority of the military court to try him. The court denied the writ finding Haupt was an admitted national of a nation with which we were at war, and he was even wearing a German Marine Infantry uniform when he landed (which he shortly buried on the beach). The court found Haupt to be an unlawful enemy combatant because he was an ununiformed spy/saboteur and as such was subject to capture and detention *and* also subject to trial and punishment by a military tribunal for the very acts which rendered his belligerency unlawful.[45] Further, the court held: "Citizenship in the United States of an enemy belligerent does not relieve him from the consequences of a belligerency which is unlawful because [it's] in violation of the law of war. Citizens who associate themselves with the military arm of the enemy government, and with its aid, guidance and direction enter this country bent on hostile acts, are enemy belligerents within the meaning of the Hague Convention and the law of war. It is as an enemy belligerent that petitioner Haupt is charged with entering the United States, and unlawful belligerency is the gravamen of the offense of which he is accused."[46]

Thus, the *Quirin* case provides a precedent for the detention and trial by military tribunal of unlawful combatants. It also provides that once one is deemed an unlawful combatant, American citizenship protections are effectively waived by the choice to become an unlawful combatant. Much of the reasoning in *Quirin* is based on an older case, *Ex parte Milligan*, 71 U.S. (4 Wall.) 2 (1866). Milligan was an Indiana resident during the Civil War who allegedly planned a raid on a federal arsenal in Indiana to obtain munitions to free Confederate troops who would help him assassinate the governor of Indiana. He was caught and the commander of the Indiana Military District sought to try him in front of a military tribunal. By a writ of habeas corpus, Milligan challenged the legality of the tribunal to have jurisdiction over him. Milligan was neither a resident of a rebellious state nor a member of any armed force. The court disagreed with the government's characterization of Milligan as violating the laws of war because Milligan's goal was to break in and steal federal property, aid and abet federal prisoners in escaping custody, and conspiring to kill the governor. The rule from the case is civilian courts have jurisdiction over citizen civilians and trumps detention and trial by a military court. Milligan was a civilian committing federal offenses. Indiana was not in a state of emergency and its regular courts were open for business. Even had the courts been closed due to national emergency, the most the military could have done was to hold Milligan until the federal courts reopened.

The *Quirin* case thus added an unlawful combatant exception to the *Milligan* rule. *Milligan* is still the law, generally speaking, and when some citizen comes along and joins a terrorist organization and takes up arms against his former homeland, he falls under the rule from *Quirin.* This should give some pause to native-born or naturalized persons who decide to abandon their country to join terrorists; by doing so, they lose their right to be tried in federal court with their full complement of rights. Some citizens have made this mendacious choice: John Walker Lindh, Jose Padilla, and Yasir Hamdi. Each has been apprehended and, predictably, the government has asserted a position that they can all be tried by military tribunals. Also, predictably, the matters have ended up in court. We shall shortly examine each in turn.

Studying case law is obviously instructive. The law revolves around rules and definitions and then applying rules to the real-world facts at hand. It is useful to define terms as we go along. Thus far, we have seen how the law draws a distinction between lawful and unlawful combatants. While the origins of who is a lawful combatant go deep into the *jus belli* (law of war) history,[47] a clear and steady concept of combatant status has evolved from treaties, customs, manuals, military tribunals, scholarly treatises up to the Geneva Conventions and international agreements of today.[48] Modernly, lawful combatants are defined in the Geneva Conventions as members of a nation's regular armed forces or, if not a regular, by four criteria each of which must be met: (1) being commanded by a person responsible for

subordinates, (2) having a fixed distinctive sign recognizable at a distance, (3) carrying arms openly, and (4) conducting operations in accordance with the laws and customs of war.[49] If there is doubt about a captured person's combatant status, a tribunal is required to hold a hearing to determine if a person is a lawful or unlawful combatant or possibly a civilian.[50] Clearly, traditional national armed forces fit the definitions as do most militias and the like. Spies and saboteurs, terrorists, and private persons do not. Lawful combatants get the protected prisoner of war (POW) status, whereas the unlawful do not.[51] This is significant for our discussion because lawful combatants may not be tried by military tribunals.

Having established the lawful combatant from the unlawful, it is easy to see people belonging to groups like Al-Qaeda fail at least the last three criteria. Taliban fighters are a closer call, but they probably fail the second and fourth criteria. Since terrorists do not meet the Geneva criteria, it might be useful to know why, and to do this we should define terrorism. According to federal law, international terrorism is a violent act dangerous to human life and would be a violation of criminal laws, which are intended to intimidate or coerce a civilian population, to influence a policy of government by intimidation or coercion, to affect the conduct of government by mass destruction, assassination or kidnapping, and occur primarily outside of the territorial jurisdiction of the U.S.[52] To cover domestic terror acts the code also proscribes hijacking, kidnapping, killing, seizing, detaining (including threats to do all these) in order to compel a third party (individual or government) to do or refrain from doing anything.[53] In another section, terrorism is "premeditated, politically motivated violence perpetrated against noncombatant groups by subnational groups or clandestine agents."[54] The PATRIOT Act added a domestic terrorism definition: "activities that (A) involve acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any state, that (B) appear to be intended (i) to intimidate or coerce a civilian population, (ii) to influence the policy of a government by intimidation or coercion, or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping, and (C) occur primarily within the territorial jurisdiction of the U.S."[55]

Thus, a terrorist is any person who does any of the aforementioned proscribed acts. Also, it is by now axiomatic that terrorism violates not only the law of most nations, but it clearly violates the law of war, so persons who commit terrorism are violating the fourth criterion of the Geneva combatant definition. Coming full circle, terrorists, therefore, are unlawful combatants. Because terrorists are unlawful combatants, they may be tried by military tribunals under the existing case law. Nevertheless, the Bush administration carried it a step further by issuing a military order pursuant to the authority granted it by Congress to carry on the war. The order for "Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism" specifically

authorized military detention and trial for terrorists traceable to the attacks on September 11, 2001.[56] When three American citizens, Padilla, Lindh, and Hamdi were apprehended for terror offenses, the government sought to try them pursuant to this authority.

Jose Padilla was a native-born Chicago gang-banger involved in numerous felonies since adolescence.[57] He became a Muslim in prison and when released left for Egypt, fell in with Al-Qaeda, and called himself Abdullah al Muhajir.[58] Intelligence was tracking him and he was arrested at O'Hare Airport first as a material witness and later declared an unlawful combatant by the administration for planning to set off a radiological "dirty" bomb in Chicago.[59] He challenged the legality of his detention with a habeas writ, which the court dismissed for want of jurisdiction.[60] Padilla refiled in the correct district and the judge there ordered the president to charge him criminally or let him go.[61] Ultimately, the administration decided to proceed with a criminal trial and got an order from the Supreme Court transferring Padilla to a federal jail.[62] The decision to try Padilla criminally sidestepped the issue of whether people like him could be tried by a military tribunal, even though the *Quirin* rule would seem to apply to Padilla as it did to Haupt. Doubtless, another traitor will take his place, forcing the issue to be adjudicated.

What did emerge was that people like Padilla could challenge their detention with a writ, settled by the *Hamdi* case that was moving along at the same time.[63] Hamdi was also a citizen, born in Louisiana, and he was captured on the battlefield in Afghanistan rifle in hand. He, too, was declared an enemy combatant, but the court held fast to *Milligan* reiterating the rule, absent a suspension of the writ, all citizens could challenge detentions by the Great Writ.[64] The court also found some authority for the administration to detain citizens who become enemy combatants on the terror battlefield, but they declined to reach the question of what the detention and trial should resemble, rather only suggesting due process standards that such a tribunal might incorporate.[65] The court was likely hinting to Congress and the president to create a system resolving the due process issues raised in *Hamdi.*

John Walker Lindh, the first citizen terrorist in the War on Terror, was originally set to be criminally prosecuted with full due process.[66] That trial would have been fraught with difficulty because of the national security issues of secret government information colliding with Lindh's full array of constitutional rights. The case illustrated the problem of an open, public trial in trying terrorists. It was proving to be almost unworkable, balancing full constitutional rights against the equally important security of the nation's secrets in a terror war. Ultimately, the government offered a plea bargain, which Lindh accepted.[67] Fortunately, citizen terrorists are few. Unfortunately, enemy alien terrorists are legion. At least with aliens, the legal landscape is clearer.

What about noncitizen terrorists? The case of *Johnson v. Eisentrager* holds flatly that enemy aliens who have not entered the U.S. are not entitled to access

to our courts.[68] The court stated: "The nonresident enemy alien, especially one who has remained in the service of the enemy, does not have even a qualified access to American courts, for he neither has comparable claims upon American institutions nor could his use of them fail to be helpful to the enemy."[69] The court also noted that "[i]t is the alien's presence within its territorial jurisdiction that gives the judiciary power to act. The Fourteenth Amendment provisions are universal in their application, to all persons within the territorial jurisdiction, without regard to any differences of race, of color, or of nationality. An alien, who has entered the country, has become subject in all respects to its jurisdiction, and a part of its population, although alleged to be here illegally."[70] Thus, while an alien residing inside the U.S. might come within the Constitution for most civil or criminal purposes, the court also held the Constitution does not confer a right of personal security or an immunity from military trial and punishment upon an alien enemy engaged in the hostile service of a government at war with the U.S.[71] This seems to suggest that enemy alien terrorists captured within the U.S. before, during, or after an attack can be subject to the military tribunal. "A resident enemy alien is constitutionally subject to summary arrest, internment and deportation whenever a 'declared war' exists. Courts will entertain his plea for freedom from executive custody only to ascertain the existence of a state of war and whether he is an alien enemy. Once these jurisdictional facts have been determined, courts will not inquire into any other issue as to his internment."[72] The court here refers to a declared war, which is one authorized by Congress pursuant to the Constitution.[73] However, the rule would seem to apply to any war authorized by Congress, particularly one endorsed with the forceful unanimity of the authorization for the War on Terror.[74] Lastly, the jurisdiction of military authorities, during or following hostilities, to punish those guilty of offenses against the laws of war is long established according to the *Eisentrager* court.[75]

The seemingly clear precedent of *Eisentrager* notwithstanding, challenges to detentions of enemy aliens captured abroad were immediate. Salim Ahmed Hamdan was Osama bin Laden's driver and bodyguard and was captured in Afghanistan in November of 2001.[76] One of 200 detainees at Guantanamo Bay to have legal cases mounted, Hamdan filed a habeas writ.[77] The U.S. military determined him to be an unlawful enemy combatant as a member of Al-Qaeda pursuant to the MO of November 13, 2001 and set his case for trial by military commission (tribunal).[78] Formally charged with a number of terrorist offenses, Hamdan's habeas challenge was rewarded by a federal district court that said Hamdan could not go before a military commission until a determination was made as to whether he was a POW under the Geneva Convention.[79] The government appealed, and during the interim the military was obligated to conduct the requisite combatant status hearings.[80] The D.C. Circuit Court reversed the district court and made several important findings.[81] The court found, among other things, that the president and

the military had authorization to try unlawful enemy combatants, that it was an "important incident" of successful warfare for commanders to try those who violate the laws of war, and that the Geneva Convention protections did not apply to Al-Qaeda members.[82] The decision both righted and launched the military trial ship. It established that wars are ongoing enterprises, that military trials are appropriate under the circumstances of the case, Geneva Conventions do not apply to captured terrorists, that the Conventions are treaties between signing *nations* thus excluding stateless entities, and that unlawful combatant detainees may challenge detentions by habeas writ (but a right to challenge does not mean the detention is unlawful).[83] Equally significant is the signal by the court that military tribunal decisions may yet be subject to appellate review.[84] For now, *Hamdan* is the law, although the Supreme Court has granted a writ of certiorari and will hear the case for a final determination of the issues revolving around the military detention and trial of unlawful enemy combatants.[85]

Military Tribunal Procedures

Now that the courts permit military tribunals to proceed, we turn to the procedures and due process in these judicial proceedings. As noted earlier, the MO of November 13, 2001 promulgates the authority and circumstances to try terrorist combatants. The order relies largely on the Congressional authorization giving him the power to use "all necessary and appropriate force" against the forces of terrorism, whatever their source.[86] Roosevelt's World War II proclamation was more sweeping since it applied to anyone, citizen or not, who acted to support any nation with which the U.S. was at war.[87] The Bush MO applies only to noncitizens and the military tribunal authority seems to be strongest when applied to noncitizens. However, as we have learned there is a plausible legal basis for military trials for citizens in some situations, like Haupt in the *Quirin* case. How much more basis remains to be developed. In any event, most of the business of the military tribunals will be directed at noncitizen terrorists captured on the terror battlefields around the world. One other federal law may also provide a basis to summarily prosecute lawfully admitted aliens who commit terrorist offenses.[88] This law allows the government to detain, try, and deport aliens who are citizens of nations we were at war with and to confiscate their property.[89] Unfortunately, the key word is "nation" and while the concept is sound, the law's wording may have to be altered to include war with stateless entities like terror organizations as well as terrorist nations such as the former Taliban Afghanistan. It could still be a useful tool.

What then does the process look like? What offenses are covered? The order says any and all offenses violating the laws of war and other applicable

laws.[90] Thus, all the laws covering international or domestic terrorism would be covered.[91] The Secretary of Defense sets up the rules and regulations for the military commissions, and they will apply the general principles of recognized criminal and evidence law.[92] The commissions are to provide a full and fair trial, military officers decide questions of law and fact, evidence is admissible for both sides where it has probative value to a reasonable person, all classified information is protected, and convictions require a 2/3 vote.[93] Attorneys conduct both the prosecution and defense.[94] Review of convictions and sentences, including death, are by the secretary or the president.[95] The troublesome part for civil libertarians is the attempt to preclude any review by regular Article III federal courts .[96] However, as we have seen in the *Hamdi* and *Hamdan* cases, the courts are already indicating that there must be some civilian review, particularly by the Supreme Court (since it agreed to review both cases), and that the *Hamdi* opinion took the trouble to begin laying out due process contours for military commissions and tribunals.

The fear, not wholly unreasonable, is that the trials will be rigged or appear to be rigged.[97] Critics objected to the conspicuous lack of review by civilian courts, the potential for using secret evidence damning to an accused terrorist, but which is off-limits to defense counsels because of legitimate national security concerns (i.e., intelligence reports, assets, military locations, operations, etc.).[98] As written, the rules permit introduction of hearsay evidence and even coerced statements a detainee might make against himself (as in where a detainee is tortured by local police or military and gives up a statement used in the American military court).[99] No doubt this might tend to tilt the trial in favor of the government, but since our constitutional protections are for our citizens or people under our courts' jurisdictions, this does not necessarily operate to make the trial inherently unfair. Even the judge who ordered Salim Hamdan to get his combatant hearing noted "in most respects, the procedures established for the Military Commission at Guantanamo under the president's order define a trial forum that looks appropriate and *even reassuring* (emphasis added) when seen through the lens of American jurisprudence."[100] Moreover, defendants get to have civilian attorneys or appointed military defense counsel at their choice.[101] Further, all members of the bar in the U.S. have to abide by the highest standards of ethical conduct and must represent their client zealously and competently or risk disbarment or other prosecution themselves.[102]

Assessing the foregoing, it is hard to say these courts are the feared "kangaroo" courts critics bray about.[103] The federal judge in *Hamdan* who insisted on due process and misunderstood the Geneva Conventions found the structure of the proceedings palatable. Thus, it appears the system has due process aplenty. Add to this the anticipated layer of civilian federal court review, and the system will truly be full and fair. What then will the military commission look like in the actual practice? The Appointing Authority (an

officer named by and acting for the secretary of defense and the president) appoints between three and seven commission members of which the presiding officer must be an attorney.[104] As noted, these members decide the facts and the law. As to other due process, the accused also get prior notice of charges and may only be convicted under a reasonable doubt standard as in any criminal court.[105] Accused persons also get a right not to incriminate themselves.[106] Both sides also get discovery rights to each other's evidence except in cases of legitimate national security information, and the prosecution must provide to the defense any exculpatory information subject to the same secrecy limitation.[107]

Defendants get to call witnesses on their behalf and confront witnesses against them just as in any trial. However, again where national security concerns override, some hearings can be *ex parte* (one side present only) or *in camera* (in closed chambers) to protect sensitive information, witness identities, or assets.[108] Convictions, as noted, require a 2/3 vote of the commission members, unless the penalty is death, for which unanimity is required.[109] The actual structure and evidentiary standards greatly resemble the Nuremberg trials of World War II referred to above and which are oft-celebrated examples of adequate due process.[110] Hearsay, coerced statements, sensitive information, and shielded witnesses were all used in that landmark case tried for the American contingent by the able Robert H. Jackson, a one-time solicitor general and U.S. Supreme Court justice.[111] Readers of Chapter 12 in this book will recall Justice Jackson was the author of the brilliant concurrence in the *Youngstown* case, which articulated the test for assessing and curbing presidential executive actions. No stranger then to the abuses of power both political and military, Jackson, with his immense integrity, was comfortable prosecuting the Nazi leadership with the due process afforded in the trial. If the level of due process in that trial was good enough for a man of Jackson's stature, then a similar, if not greater, level present today in Bush's military commissions should be good enough for the accused and the critics.

The world lauded the cooperative international justice that brought the Nazi leaders to book. Today, it is a different era in that American action, values, and motives are always called into question. Yet, the system called for by Bush's MO is as good if not better than that of Nuremberg. The Nazis had no right of appeal, which the detainees of the War on Terror already have in the military system and are almost certain to get another layer of review by the federal courts before it is all settled. It seems that a system that could fairly prosecute history's greatest monsters (to date) should be adequate to prosecute persons who perpetrate the latest evil of global terrorism. The enemy in the War on Terror is no less dangerous, perhaps just not as organized or equipped yet. There can be no doubt they have the same genocidal lusts (even unto destroying the Jewish people along with the West) and territorial ambitions.

A Word on the Federal Courts in the War on Terrorism

This chapter's title refers to courts-martial, military tribunals, and federal courts. We have discussed the first two topics at some modest length. However, we have also been discussing the role of the federal courts in relation to the military justice system both as it affects our own personnel and the terrorist detainee. The reasons should be apparent after some consideration by the reader of the import of these two chapters. The basic concept is that we are a nation bound together by the rule of law as a fundamental organizing principle. We believe in a supreme law of uniform application to all citizens and persons under the jurisdiction of our courts. We call that law our Constitution, and all jurisprudence in this country must be consistent with its precepts. We know from the reading that the Founders intended the Supreme Court to decide and mete out the law independent from influence from the political branches of Congress and the executive. Military law, like all our other laws, must be no different. With the UCMJ, military law now is in line with constitutional principles.

Throughout this chapter's discussion, we have seen how deeply intertwined the federal courts are with every aspect of military law as it relates to the trial and detention of our wartime enemies. We have studied a number of cases, past and present, the decisions of which shape the contours of the applicable law. We are seeing the development of this body of law right before our eyes. A separate discussion of the role of the federal courts here would be largely redundant, for their involvement has been an inseparable part of the ontogeny of this once obscure but now ever-increasingly relevant realm of jurisprudence. The courts, in every sense, say what the law is,[112] and it follows that they say what the law is regarding military courts and trials. Any attempt to depart from this tried and true methodology is to begin to court the abuses feared by the Founders.

What abuses are referred to? Recall that the Founders feared abuses either by the dictator or the mob. An all-powerful executive who could detain and try people with whom it was displeased without limitation by an impartial court is the classic scenario of despotism. Such a system puts people completely at the mercy of the dictator, whether styled king, president, or chancellor, and was the very antithesis of the freedom the Founders strove to forge. Mob rule by an unrestrained majority oppressing all the minority voices and rights is no better. Our courts are the great levelers and the principles we have created and continue to develop are what set our nation apart. Over the last 230 years, we have developed firm notions of what "full and fair"[113] trials look like. During that time, we have developed a strong concept of due process, an understanding that any judicial process will have mutually agreeable hallmark indicia of fundamental fairness. As Americans,

we claim to value fair play. Insisting on due process standards is one of the ways we prove we are serious about fairness. Abiding by the decisions of our courts regarding whether or not due process has been honored is another.

Our analysis of the military trial is largely based on the cases leading up to the present, framed by the Bush MO of November 13, 2001. This order, fairly read, provides a number of important due process protections as we have seen. The order is the most prudent response under wartime circumstances to a demonstrably dangerous and resourceful enemy. Even though not required to by the treaty, the Order even includes many of the basic Geneva Convention treatment standards be extended to all War on Terror detainees.[114] Detainees must be treated "humanely" without "adverse distinction" based on race, creed, religion, color, gender, birth, or even wealth.[115] The Order also mandates adequate food, water, shelter, clothing, and medical treatment as well as permitting the free exercise of religion consistent with the requirements of detention.[116] Once again, fairly read, it is hard to see what the critics are howling about. It is clear we are giving these people far more than we would receive in like circumstance and that we are taking real pains to honor our values by taking the trouble to write down all the process and privileges the detainees are entitled to, thereby codifying them for the entire world to read. Strange behavior for an executive who is trying to hide something.

The only problematic passages in the Order are those that purport to take away the process of review from the courts.[117] No one disputes the importance of the intelligence value of captured terrorists and the necessity of interrogating them.[118] We have established, or rather the courts have, that such detainees are not POWs and are not entitled to Geneva protections. The Order itself mandates basic human needs be met and provides ample due process for the trials themselves. By arrogating unto itself the sole right to both try and review all terrorist cases and to specifically preclude detainees from all review, the administration arguably risks going too far by usurping a basic court function.[119] We note detainees already have the right to challenge the legality of their detention with the Great Writ. It is a small step from there to have some basic level of appellate review in the military terrorist trials just as we do in courts-martial. It is a small price to pay to honor the fairness we are known for and, perhaps just as important in this media-conscious world, for the perception of fair treatment that review by a neutral tribunal affords. This writer predicts that this will be the ultimate complexion of the military tribunal process, and courts are already signaling this likely requirement. This review seems the most inherently fair way to balance the exigencies of wartime with cherished, intrinsic values. Moreover, by doing so, we quickly deflate the arguments of critics who accuse us of hypocrisy.[120]

There is already a precedent for review of court cases involving sensitive intelligence information. The Foreign Intelligence Surveillance Court (FISC) and the various other courts set up under the Foreign Intelligence Surveillance

Act (FISA) of 1978 (see Chapter 12) already have procedures in place for dealing with the sensitive information military trials of terrorists will likely involve. It should be a relatively simple step for Congress to authorize courts to review military tribunals either under FISC or some other existing court or to create one dedicated solely to tribunal review.[121] This is arguably a wise course not only to silence critics, but also as a way to more fully develop and utilize sensitive information. Because of the well-developed precedents already upholding the right of the military to try enemies of the nation, the establishment of civilian review simply completes a robust and workable structure for prosecuting terrorist crimes in the War on Terror. Far from being viewed as an obstacle or layer of bureaucracy, the federal courts are the best insurance for a fair adjudication of accused terrorists. Even if one's visceral reaction to terrorists is to lock them up and throw away the key, this writer argues the cause of the U.S. is advanced inexorably by having them prosecuted in a "full and fair" system. By sweeping terrorists from the battlefield, we show the might and efficiency of our military and our resolve to win. By fairly treating and prosecuting them, we show the superiority of our constitutional system of checks and balances. Our federal courts are, and must be, essential players in the War on Terror. All three branches are essential if we are to win, for that is our system, one that has permitted us to survive and thrive to this day.

Concluding Remarks

We are at war. It is an unfortunate comment on humanity that mortal conflict is so commonplace. The War on Terror is not one of our choosing, but it is one we must choose to win. After September 11, 2001 we had to quickly react and defend ourselves. That reaction provoked an accounting of previous approaches to a problem we were largely isolated against. We knew about terrorism, but it was mainly the tragic problem of other countries. Then we learned what those other nations already knew, that there are not any "other" countries when it comes to the palpable dangers of global terrorism. Anyone and any nation can be a target. The new warfare less and less consists of massed uniformed armies crossing borders in vast theaters of war and more and more of small groups of stateless individuals launching attacks of mass destruction against nonstrategic and innocent civilians. It is a new war with new faces and techniques, one which calls for new countermeasures, and the only thing that is not new is the casualties. You are just as dead whether you are shot by an invading soldier as when you are sitting in your high-rise office when it is struck by a hijacked aircraft full of jet fuel.

Even though this is a new war, there are useful lessons from the past. Every new war exhibits advances and changes from the one that preceded it. We have begun to re-examine our approaches to the terrorism problem and

are assessing what is effective and what is not. Because of the urgent nature of the risk, largely to civilians, we have had to adopt measures permitting a rapid and efficient response to the threats posed. We have moved away from perceiving terrorism as a purely criminal problem toward one of it as a military problem. This perception shift is paradigmatic and doing so unleashes the world's best trained, equipped, and effective military machine against the terrorist strongholds. The effect was immediate. Our successes generated large volumes of captured terrorists that had to be processed.

The physical success on the battlefield led in turn to battle in the courtrooms. Despite our great and righteous anger, we held fast to the rule of law and sought legal and fair ways to deal with our captives. We searched our souls and our history for the right course of action. In this effort, as in all others, we are ultimately guided by our bedrock Constitutional principles. Our respect for the rule of law is universal, but the benefits of our citizenship and our constitutional rights cannot be disseminated universally to all who would seek such shelter and least of all to our enemies. To extend the Bill of Rights to the very people who seek to destroy us and our law, to let them use it against us, is to court disaster and ignore the most basic legal duty of government, that of preserving and safeguarding the nation.

Rather, what we do provide is our values in the form of due process of law, even unto our most dedicated enemies, even when we are defending ourselves from death and destruction. The most reliable sign of the greatness of a nation is the quality of its justice. By steadfastly maintaining our principles, we do justice by our own citizens, the victims of terrorism, and the terrorists themselves. The work of the War on Terror has not caused us to forget what makes this nation great. Struggling to find a way to do what is right with debate from all viewpoints about what should be done affords us the intellectual raw materials to determine what must be done. Doing what is right is seldom easy or expedient, but it is American. By requiring our government to consistently do the right thing, we remain the innovative engine of evolving freedom.

References

1. U.S. Const., Amends. IV, V, VI, and VIII made applicable to the states by Amend. XIV.
2. Speech by President George W. Bush at West Point Military Academy, June 1, 2002; National Security Strategy of the United States, September 2002.
3. Ibid.
4. *See* Geneva Conventions of 1949 and 1977, Convention III.
5. Tibetan Foundation Newsletter, No. 32, 2001, available at: <http://www.tibet-foundation.org/nl/nl32.pdf>

6. See generally Shanor, C.A. and Lynn Hogue, L., *National Security and Military Law*, Thomson/West, Eagan, MN, 2003, chaps. 5–6.
7. Id. at p. 230.
8. Ibid.
9. Ibid.
10. *Parker v. Levy*, 417 U.S. 733, 1974.
11. 10 U.S.C. §§ 801–946.
12. U.S. Const., Art. I, § 8, Art. II, § 2, see also Chapter 12 of this text.
13. For example: desertion, aid and comfort to the enemy, cowardice under fire, dereliction of duty, absent without leave, disrespect to or disobedience to officers, etc. These are but a few examples of military crimes lacking civilian cognates.
14. 10 U.S.C., § 836.
15. Two significant changes were wrought in 1968 and 1983. These changes enhanced the role of the trial judge and required that licensed attorneys be appointed as defense counselors for accused at courts-martial.
16. The MRE mirror the Federal Rules of Evidence (FRE) in use in the federal court system.
17. O'Connor, T., Military Law and Military Justice, Lecture Notes, North Carolina Wesleyan University, Sept. 16, 2005.
18. Ibid.
19. Due process is many things, but basically it is characterized by fair proceedings for involved or accused parties with notice of charges or complaints, opportunity to respond and defend, opportunity to defend oneself, opportunity to confront witnesses and evidence against one, opportunity to produce favorable or exculpatory evidence, a right to advice of counsel, a right to a fair and impartial tribunal, and a right to appeal. Due process varies according to the situation, the value of the rights involved to the individual, the administrative burden, and the value of procedural safeguards. *Mathews v. Eldridge*, 424 U.S. 319 (1976) requires weighing of due process to balance three factors: (1) the interest of the individual in the life, liberty, or property right and the risk of deprivation from the government action; (2) administrative cost/burden and government interest in efficient administration; and (3) risk of error under the current process against the value of additional procedures.
20. This is said to be the "convening authority" or that of a commander to convene a court-martial.
21. MCM, Part III, RCM 303.
22. O'Connor, T., Military Law and Military Justice, Lecture Notes, North Carolina Wesleyan University, Sept. 16, 2005.
23. UCMJ, Art. 31.
24. UCMJ, Art. 32. This may be likened to a grand jury investigation.

25. See Dressler, J., Cases and material on criminal law, 2nd ed., West Publishing, 1999, pp. 131–141.
26. See generally International Military trials Nuremberg: Nazi Conspiracy and Aggression, Opinion and Judgment, and Office of United States Chief Counsel for Prosecution of Axis Criminality (United States Govt. Printing Off. 1947). The ancient German city of Nürnberg (often styled in English as Nuremberg) was the site of the famous torchlight Nazi party rallies of the 1930s. It was also spared heavy Allied bombing and the combination of the intact infrastructure and its value as a Nazi symbol made it the ideal Allied choice for the war crimes trials.
27. Ibid.
28. Ibid.
29. Id. at pp. 3–4.
30. Id. at p. 3.
31. Id. at p. 4.
32. Ibid.
33. Since the terrorists organizations are stateless and nonsignatories of the treaty, they technically do not qualify. Nor do they seem to meet the definitions of combatants since they are irregular forces who fight without recognizable uniforms or command structures. The Conventions apply to the uniformed armed forces of nations or similar colorable entities.
34. See generally Cheh, M., Should lawyers participate in rigged systems? The case of the military commissions, *J. Nat. Secur. Law Policy,* 1, 375, 2005.
35. Shanor, C.A. and Hogue, L.L., *National Security and Military Law*, pp. 41–42.
36. Id. at pp. 40–41.
37. Id. at pp. 40–41. See also U.S. Const., Art. I, § 9.
38. U.S. Const., Art. I, § 9.
39. Message to Congress (Jul. 4, 1861), in Roy P. Basler, Ed., IV Collected Works of Abraham Lincoln, 1953–1955, pp. 429–430.
40. *U.S. v. Rahman,* 189 F.3d 88, 2d. Cir., 1999.
41. Shanor, C.A. and Hogue, L.L., *National Security and Military Law*, p. 45.
42. Ibid.
43. *Ex Parte Quirin*, 317 U.S. 1, 1942.
44. Presidential Proclamation 2561, 7 Fed. Reg. 5101, 1942.
45. *Ex Parte Quirin*, 317 U.S. 1, pp. 30–31.
46. Id. at pp. 37–38.
47. Congressional Research Service Report for Congress, Terrorism and the Law of War: Trying Terrorists as War Criminals before Military Commissions, Dec. 11, 2001, p. 6.
48. Id. at pp. 6–10.

49. Geneva Convention III, Art. 4.
50. Geneva Convention V.
51. Geneva Convention III, Art. 4. Article 4 defines the POW status, numerous other articles mandate POWs be provided habitable shelter, food, water, clothing, not be tortured or be subject to harsh prolonged interrogation, have a right to practice religion, permitted to send or receive mail (subject to certain restrictions), suffer no harsh detention or cruel punishments, and ultimately be repatriated after hostilities cease. Thus, lawful combatants are persons committing belligerent acts, but who qualify as prisoners of war, whereas unlawful combatants commit belligerent acts, but do not qualify for protected POW status.
52. 18 U.S.C. § 2331(1).
53. 8 U.S.C. §1182(a)(3)(iii). The section goes on to include assassinations and the use or threatened use of weapons of mass destruction.
54. 22 U.S.C. 2656f.
55. 18 U.S.C. § 2331(5).
56. Military Order of Nov. 13, 2001, Detention, Treatment, and Trial of Certain Noncitizens in the War Against Terrorism, 66 Fed. Reg. 57833, Nov. 16, 2001 (hereinafter Military Order).
57. All About Jose Padilla, available at: http://www.crimelibrary.com/terrorists_spies/terrorists/jose_padilla/4.html.
58. Ibid.
59. *Padilla v. Rumsfeld*, 352 F.3d. 695, 2003, reversed and remanded for lack of jurisdiction.
60. Ibid.
61. *Padilla v. Hanft*, 389 F. Supp. 2d 678, 2005.
62. *Hanft v. Padilla*, 126 S.Ct. 978, 2006.
63. *Hamdi v. Rumsfeld*, 542 U.S. 507, 2004.
64. Ibid.
65. Ibid.
66. *U.S. v. Lindh*, 212 F. Supp. 2d 541, 2002; see also John Walker Lindh article, available at: http://en.wikipedia.org/wiki/John_Walker_Lindh#Trial.
67. *Supra* note 66.
68. 339 U.S. 763, 1950.
69. Id. at p. 777.
70. Id. at p. 771.
71. Id. at p. 785, stating unequivocally: "We hold that the Constitution does not confer a right of personal security or an immunity from military trial and punishment upon an alien enemy engaged in the hostile service of a government at war with the United States."
72. Id.at p. 775.

73. U.S. Const. Art. I, §8.
74. *Hamdan v. Rumsfeld*, 415 F. 3d 33, 2005, "In the joint resolution, passed in response to the attacks of September 11, 2001, Congress authorized the president "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided" the attacks and recognized the president's "authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." Authorization for Use of Military Force, Pub. L. No. 107–40, 115 Stat. 224, 224 (2001)."
75. *Eisentrager*, *supra*, note 68, at p. 786.
76. O'Connor, T., National Security Law and Terrorism, Lecture Notes, North Carolina Wesleyan University, Sept. 16, 2005.
77. Ibid.
78. Ibid.
79. *Hamdan v. Rumsfeld*, 344 F. Supp. 2d 152, 2004. Recall that under Geneva Convention III, Art. 5, a combatant status review tribunal is supposed to be held by all member nations to establish if the detained person is lawful/unlawful.
80. Ibid; see also: Article on Salim Ahmed Hamdan, available at: http://en.wikipedia.org/ wiki/Hamdan.
81. 415 U.S. 33, *supra* note 74.
82. Ibid. at pp. 37, 38, and 42.
83. Ibid.; Lecture Notes, *supra* note 76.
84. Lecture Notes, *supra* note 76.
85. *Hamdan v. Rumsfeld*, 126 S.Ct. 622, 2005.
86. Report for Congress, *supra*, note 47 at p. 27.
87. Presidential Proclamation 2561, Denying Certain Enemies Access to the Courts of the United States, July 2, 1942. This order was the one at issue, and upheld, in the *Quirin* case discussed earlier.
88. 50 U.S.C. §21, The Alien Enemy Act
89. Ibid.
90. Military Order, *supra* note 56, §1(e).
91. Id. §§ 2(a)(1)(i)–(iii).
92. Id. § 1(f).
93. Id. §§ 4(c)(1)–(4) and (6)–(7).
94. Id. § 4(c)(5).
95. Id. § 7(b)(2).
96. Cheh, M., Should lawyers participate, *supra* note 34, at p. 377.
97. Id. at p. 378.
98. Id. at p. 379.
99. Ibid.

100. *Hamdan v. Rumsfeld*, 344 F. Supp 2d 152, 166, D.D.C., 2004.
101. Id. § 4(c)(3)(b).
102. Cheh, M., Should lawyers participate, *supra* note 34, at pp. 391–392.
103. Id. at p. 377.
104. Military Order, *supra* note 56, §4(A)(1) & (2)–(4).
105. Cheh, M., Should lawyers participate, *supra* note 34, at p. 381.
106. See *supra* note 99 and accompanying text.
107. Cheh, *supra* note 34, at pp. 381–382. Also, the Military Order, *supra* note 56, at §7(a)(1) forbids the disclosure of state secrets to any person not otherwise authorized to have access to them.
108. Military Order, *supra* note 56, § 6(B)(3).
109. Id. § 6(D)(5)(b).
110. Report for Congress, *supra*, note 47 at pp. 37–38.
111. International Military Trial, *supra* note 26, frontispiece. Justice Jackson was the author of the brilliant concurrence in the *Youngstown* case, which articulated the test for assessing and curbing executive branch actions.
112. *Marbury v. Madison*, 5 U.S. (1 Cranch.) 137, 1803. The reader may recall this is the foundational case for all constitutional law, where the court, in an opinion by Chief Justice Marshall, declares its "province" to be the final word on the meaning of laws.
113. Military Order, *supra* note 56, §4(c)(2).
114. Id. § 3.
115. Id. § 3(a)–(b).
116. Id. § 3(c)–(d).
117. Id. § 7.
118. Congressional Research Service Report for Congress, Treatment of "Battlefield Detainees" in the War on Terror, April 11, 2002, p. 32.
119. Id. § 7(b)(2). This upsets the constitutional principle of separation of powers essential to federalism.
120. Cheh, M., Should lawyers participate, *supra* note 34, at pp. 379–380.
121. U.S. Const. Art. I, §8 gives Congress the power to constitute such inferior courts (to the Supreme Court) as necessary.

14 National Nuclear Security Administration Laboratories: Emerging Role in Homeland Security

RICHARD A. NEISER

Contents

Introduction

The U.S. Department of Energy (DOE) operates an extensive system of national laboratories. These world-class facilities are staffed by some of the best scientists and engineers in the nation. These laboratories provide a broad gamut of technical services ranging from basic research and development to highly applied national security work. The national labs were created to serve a variety of purposes. Los Alamos National Laboratory (LANL), Lawrence Livermore National Laboratory (LLNL), and the Sandia National Laboratories (SNL) are primarily responsible for the military use of nuclear energy. These three laboratories are administered by DOE's National Nuclear Security Administration (NNSA). Idaho National Laboratory was created to develop nuclear reactor technology, particularly for naval applications. Ten other laboratories are

overseen by DOE's Office of Science. These laboratories conduct studies across an astonishing range of science and technology including, for example, biological and genome research, chemistry and materials science, climatology, computing, energy, environmental sciences, geoscience, high-energy physics, nanotechnology, and nuclear medicine and physics. Still other national labs are focused on specific aspects of energy research and environmental restoration. The location of each national lab and its administrative office within DOE is shown in Figure 14.1.

The purpose of this chapter is to introduce the reader to the DOE national laboratory system and its history and then to focus on the three NNSA laboratories and their emerging role in national security, particularly with respect to homeland security. There is, of course, a rich literature describing the national labs, especially for the Manhattan Project and the development of the atomic bomb.[1,2] The decades of work performed by tens of thousands of men and women cannot be covered here, except in the most cursory way. The emphasis rather will be in helping the reader understand the roles and capabilities of the NNSA labs and describe how their national security responsibilities are evolving. The events of September 11, 2001 and the subsequent Global War on Terror continue to have a profound influence on the national security structure of the U.S. The NNSA laboratories are intimately caught up in the current of changes sweeping our government. It will not be apparent for several years yet what the lasting impact will be on the missions of our national laboratories.

DOE's National Laboratories

The national laboratory system was created in the years following World War II and sprang out of the Manhattan Project. Many of today's national labs played key roles in the development of the atomic bomb. For example, Oak Ridge was the site used to enrich uranium. Argonne (University of Chicago) demonstrated the first sustained nuclear chain reaction leading to the reactor at Hanford for synthesizing plutonium, which is where Pacific Northwest National Laboratory is located today. Lawrence Berkley National Lab was originally the University of California Radiation Lab (UCRL), where Ernest O. Lawrence built the first cyclotron particle accelerator and where many important contributions to the Manhattan project were made. Ames Laboratory in Iowa was founded in 1942 to develop casting and purification technologies for uranium metal. And, of course, Los Alamos was created in 1943 to design and build the uranium and plutonium bombs that ended the war.

Shortly after the war, other major facilities were established. Brookhaven National Lab on Long Island was created in 1946 by the Atomic Energy Commission (AEC) in collaboration with nine universities to promote basic

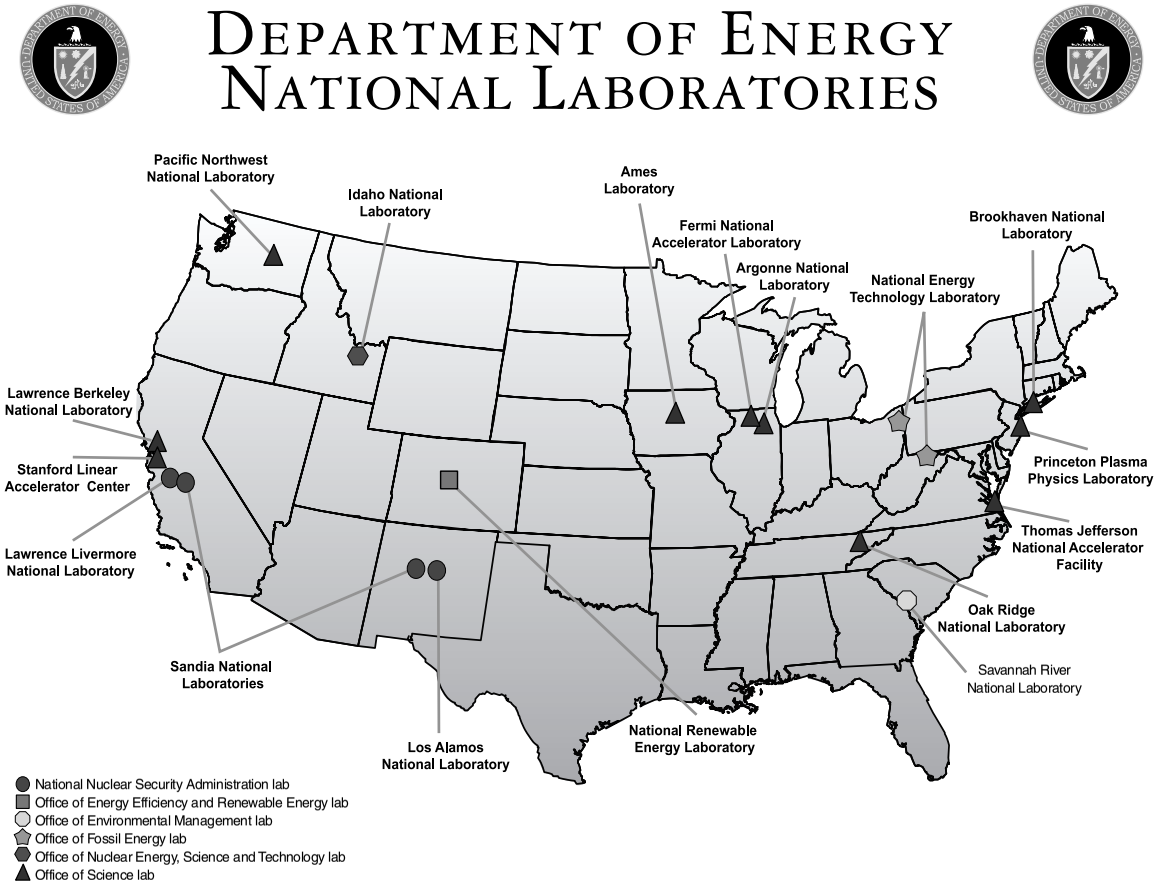


Figure 14.1 The DOE's national laboratory system.

research into peaceful uses of atomic science. SNL was originally the Z-Division of Los Alamos and was responsible for the engineering aspects of nuclear weapons prior to becoming a separate entity in 1949. Idaho National Lab was also founded in 1949 as the National Reactor Testing Station, which focused on harnessing the atom for power generation and propulsion. In 1952, Ernest Lawrence and Edward Teller established a new nuclear weapons design facility to compete with Los Alamos. A second UCRL campus was built in Livermore and eventually became LLNL. Shortly thereafter, in 1956, Sandia opened a second facility next door to Livermore to provide engineering design services for the new lab; hence, the plural in SNL. Thus, bit by bit, the current national lab structure arose.

In the 1970s, the AEC was replaced by the Energy Research and Development Agency and finally by the DOE, a new cabinet-level position within the U.S. government. In the decades following World War II, the laboratories' mission space increased dramatically and they evolved accordingly. New facilities, such as the Stanford Linear Accelerator, Fermilab, and the National Renewable Energy Laboratory among others, were created as DOE's scope broadened. Today the DOE is responsible not only for nuclear weaponry and reactor technology, but also for the overall energy policy of the U.S., domestic energy production, and it sponsors more basic and applied research in the physical sciences than any other federal entity. All of the major national labs are multi-programmatic and figure prominently in helping DOE accomplish its mission.

An important aspect to understand about the labs is that they are government owned and contractor operated (GOCO). Unlike other federal labs, such as the Department of Defense (DoD) military service labs, which are government owned and government operated (GOGO), national lab employees are not civil servants; rather they are employees of the contractor that manages the facility. For example, Lawrence Livermore workers are employed by the University of California and Sandians by Lockheed Martin. All of the equipment and facilities at a national laboratory belong to the federal government and the tasking is federally directed. This arrangement arose at the end of World War II when atomic weapons were transferred from military to civilian control. There were several reasons for choosing the GOCO model. It was difficult to attract and retain the top scientists and engineers needed by the national labs with the reduced pay scales and stricter career advancement opportunities associated with civil service. There was also an appreciation that academic and industrial entities were better at running complex technical research facilities than a governmental entity with its attendant bureaucracy. Although DOE exerts an ever-increasing level of oversight and control on the national labs, the original characteristics that were sought of civilian control of nuclear energy and world-class capabilities and people persist to this day.

The three NNSA laboratories (Los Alamos, Livermore, and Sandia) have historically focused on nuclear weapons and their associated safety, reliability,

and security. By comparison, the Office of Science laboratories have concentrated on basic science and unclassified work. The remainder of this chapter will discuss the role of the nuclear weapons labs in national and homeland security. This is not to say that the other national laboratories cannot or do not make important contributions to national security because they do; it is more a recognition that these three laboratories' major mission, nuclear weapons, is diminishing and their roles in our national security infrastructure are shifting.

Cold War Role of the Nuclear Weapons Labs

At the close of World War II, the U.S. was in sole possession of nuclear weapons. As Communism took over in Eastern Europe, China and the Far East and the U.S. and its allies established policies to contain its spread. During the resulting Cold War, nuclear weaponry was vital to deterring Communism and Soviet expansion.

A number of important decisions and events in the immediate postwar years determined the U.S. nuclear weapons posture and drove the activities of Los Alamos, at that time the only nuclear weapon laboratory. As soon as the war ended, the U.S. demobilized a large portion of its armed forces. With its monopoly on atomic energy and its historical predisposition to maintain a modest peacetime military, it was not surprising that by 1947 atomic bombs had assumed a central role in the U.S. defense posture. To support this stance, tests had to be conducted to understand the military effects of atomic detonations. Another problem to address was the fact that the original Fat Man plutonium implosion design was very conservative. Lighter-weight designs that could be carried by smaller aircraft, consumed less fissionable material, and had higher yields were urgently needed.

In the background to these activities, a debate raged within the AEC and at the highest levels of government regarding the development of a "hydrogen" or "thermonuclear" bomb. Initially scientists were unsure if one could even be built; however, studies at Los Alamos and elsewhere overcame the technical barriers. Two camps emerged to argue the military utility of such a device and whether it was morally responsible to build one. Unlike a fission bomb, which has an upper limit on its destructive force, a thermonuclear bomb's output is limited only by the amount of fuel present. It quickly became apparent that the usefulness of a thermonuclear bomb would be in its strategic deterrent value and not as a tactical weapon. The detonation of the Soviet's first fission bomb in 1949 was a shock because it happened many years sooner than was believed possible and removed American hegemony in nuclear power. President Truman and his advisers came to the conclusion that it would be an unacceptable national security risk if the U.S. chose not

to develop a thermonuclear weapon and the Soviets did. Work was continued, and the first thermonuclear device codenamed "Mike" was detonated in the Pacific in 1952. Work to create a deployable hydrogen bomb rapidly ensued.

During this time, major changes overtook the nuclear weapons activities of the U.S. Large numbers of bombs were required to meet an ever-increasing range of military needs. New designs of physics packages, the nuclear device itself, were required. These designs had to be "weaponized," which meant they had to be packaged into militarily useful assemblies. Parachutes, arming-fusing-and-firing systems, and control panels inside aircraft are but a few examples of items that had to be designed and built. Los Alamos' capacity for performing all these activities was quickly exceeded; thus, the birth of Sandia, Lawrence Livermore, and nuclear weapons production facilities across the nation.

Through the 1950s and 1960s, Soviet and American stockpiles grew. Eventually each nation could destroy the other many times over. The resulting stalemate was pithily called mutually assured destruction (MAD). In 1957, the Soviet launch of Sputnik ushered in the space age. Missile technology matured rapidly. The Americans and the Soviets pursued miniaturized thermonuclear weapons that could be mounted to land- and submarine-based ballistic missiles. A nuclear triad of bombers, submarines, and intercontinental ballistic missiles was created to provide the crucial second strike capability to prevent an overwhelming first strike from succeeding.

The frightening power of thermonuclear weaponry raised many safety and security questions. Missile technology shortened the response time to attack and necessitated the transfer of control of nuclear weapons back to the military. The Cuban Missile Crisis in 1962 profoundly demonstrated the possibility of a nuclear Armageddon and brought the question of civilian control to a head. Broken Arrow accidents, such as the Palomares and Thule crashes of B-52 bombers with nuclear weapons on board, highlighted the safety risks associated with actively deploying large numbers of weapons.

These developments stimulated activities at the nuclear weapons labs in an ever-increasing range of technical areas. Improved command and control systems to prevent use of nuclear weapons without presidential authorization were required. Safety systems to prevent the detonation of weapons exposed to fire, lightning, or other accident conditions became vitally important. Security systems to prevent nuclear weapons from falling into the wrong hands were also needed. Secure vaults, perimeter control systems, and safe and secure transportation capabilities are examples of new technologies that had to be developed.

Another major factor that dictated activities at the national labs were the various international treaties limiting the testing, numbers, and types of nuclear armaments. For example, extensive underground test facilities had to be built and instrumented as a result of the Partial Test Ban Treaty (PTBT)

of 1963 that prohibited further above-ground testing. Treaty verification technologies involving space-based and ground-based sensors were also developed at the nuclear weapons labs. The successful Vela satellite program for monitoring compliance with the PTBT and the Nuclear Nonproliferation Treaty of 1968 is a good example of how the national labs teamed with the DoD and U.S. industry to meet an important national need. The national laboratories have also provided technical support on behalf of the U.S. to the International Atomic Energy Agency (IAEA) since its inception in 1957.

The last phase of the Cold War was dominated by President Reagan's Strategic Defense Initiative (SDI), more commonly known as "Star Wars." At the root of SDI was Reagan's desire to replace the suicidal MAD doctrine, which was based on an offensive nuclear capability, with a defensive capability for destroying incoming ballistic missiles using ground and space systems. Though never deployed, the national labs developed and tested the sensors needed to detect an attack and investigated numerous systems for destroying incoming warheads. This work continues to this day as part of the U.S. theater defense program.

Impact of the End of the Cold War

In 1985, Mikhail Gorbachev ascended to the leadership of the Soviet Union. Summits with President Reagan led to the Strategic Arms Reduction Treaty (START I) and eased decades-long Cold War tensions. Gorbachev's attempts to reform the Soviet economy and the end of the supremacy of the Communist Party in the Soviet Union riveted world attention. In November 1989, the world watched in amazement as the Berlin Wall came down. Two short years later, the Cold War ended with the collapse of the Soviet Union. Accompanying these world-changing events was a reevaluation of the international strategic situation. People talked about a "new world order" that included nuclear disarmament, expanded power and influence for the United Nations, and worldwide progress on human rights. In the U.S. and, especially in Western Europe, military spending was sharply curtailed in the "peace dividend" that accompanied the end of the Cold War.

The U.S. nuclear weapon program was, of course, significantly impacted by these events. The last major warheads designed at the national labs were the W87 and W88 in the early to mid-1980s. The last two numbered warheads, the W89 and W91, were cancelled in the early 1990s (number designators are given to designs formally intended to become weapons). At the same time, the U.S. declared a moratorium on underground testing and conducted its last test in 1992. Although not ratified by the Senate, the U.S. adheres to the conditions of the Comprehensive Test Ban Treaty of 1996, which bans all nuclear explosions.

National Nuclear Security Administration

Nine years after the end of the Cold War, the NNSA was formed as a semi-autonomous entity within the DOE. Its creation followed the publication of two reports: the Cox Committee report released in May 1999, which discussed security lapses that allegedly allowed the Chinese to acquire U.S. nuclear weapons technology, and the Rudman report entitled, "Science at its best, security at its worst," which was issued by the president's Foreign Intelligence Advisory Board in June 1999. One of the root causes for creating NNSA was the concern that DOE's mission had become so broad that its focus on the vital nuclear security mission had suffered.

As an aside, it is interesting to note that the DOE was created in 1977 by merging 40 different government agencies and organizations in response to the Energy Crisis of the 1970s. Energy work was spread across the U.S. government in a noncentralized, *ad hoc* arrangement that prevented a coherent U.S. energy policy from emerging. The parallel to the formation of the Department of Homeland Security (DHS) in response to the terrorist attacks of September 11, 2001 with the goal of creating a coherent homeland security policy by assembling disparate organizations from across the government is striking.

NNSA's mission is to enhance national security through the military application of nuclear energy. It is to maintain the safety, reliability, and performance of the nuclear weapons stockpile, to provide the U.S. Navy with effective nuclear propulsion plants, to promote nuclear nonproliferation and reduce the global danger from weapons of mass destruction (WMD), and support U.S. leadership in science and technology.

With no testing, no new designs, and no production, the main focus of the nuclear weapons program since the early 1990s has become Stockpile Stewardship. The goal of this program is to maintain the safety, security, and reliability of the enduring stockpile in the absence of underground testing for the indefinite future. As part of the program, important capabilities, such as underground test facilities and the manufacturing infrastructure, are to be kept up to date and ready for use if so directed by the president.

U.S. nuclear weapons were not specifically built for a long lifespan; typically, they were designed to meet performance criteria, such as large yield combined with low weight. Aging systems may fail or act unpredictably for a variety of reasons. Understanding how the various materials and components within these complex systems age and developing methods for extending the life of the weapons lie at the heart of the Stockpile Stewardship program. The program includes within it a Life Extension Program for refurbishing aging warheads. A limited capability and capacity to manufacture pits, the plutonium shells inside the fission components of modern nuclear weapons, is another important task.

NNSA and the nuclear weapons labs have proposed the Reliable Replacement Warhead (RRW) Program as the path forward for creating a smaller, more flexible nuclear stockpile that meets U.S. national security needs. As weapons are refurbished and their lifespan extended, concerns inevitably arise about the ability to indefinitely assure the reliability and safety of the stockpile absent underground testing. The RRWs are intended to be replacements for legacy warheads that are easier to manufacture and maintain and are safer and more secure. The RRW program is politically fragile and it is far from certain that the nation will choose to pursue it.

In the area of nuclear nonproliferation, the NNSA and the national labs have a strong program. At the end of the Cold War, serious concerns about the security of nuclear weapons and materials in the Former Soviet Union (FSU) arose. There were additional worries about who the unemployed scientists and engineers from nuclear facilities might work for. Could they be lured to work for a country aspiring to possess nuclear weapons or for a terrorist organization? NNSA and the national labs have programs specifically geared to secure nuclear materials at potentially vulnerable sites in the FSU, to blend-down hundreds of tons of excess highly enriched uranium for commercial power use, and to help downsize the nuclear weapons infrastructure of the FSU by finding alternate, nonmilitary activities for the staff to work on at these facilities.

Other major nonproliferation activities are carried out at the national labs. The mitigation of safety and security concerns at nuclear reactors around the world in collaboration with the IAEA is a typical example. Better space-based and land-based sensors for detecting nuclear explosions in violation of international agreements are being developed. The labs also assist in developing export control policies to prevent the further spread of nuclear weapons technology. Border security technologies are being developed and deployed worldwide to halt nuclear smuggling and nuclear terrorism through the use of nuclear detection equipment at border crossings, airports, and seaports. These nonproliferation activities of the national labs have strong connections and parallels to homeland security and defense work being conducted within the U.S.

Diversifying the Work of the National Laboratories

In tackling the extraordinarily challenging problems of the Cold War, the nuclear weapons labs built a workforce and facilities second to none. Technical capabilities in physics, chemistry, materials science, electronics, explosives, aerodynamics, mathematics, computational science, and a host of others were essential if the labs were to succeed. Managing the cradle-to-grave

responsibility for nuclear weapons required a vertically integrated, agile infrastructure capable of tackling the most complex national security problems in a time-critical fashion. Although the national laboratories are contractor operated, they are part of the government with appropriate access to government information and, of course, have the ability to perform classified work. For all these reasons, the national labs are an attractive resource to government agencies in solving their most difficult technical problems.

A major diversification of activities came in the 1970s when the national labs became heavily involved in energy research as a result of the oil embargo crisis of 1973. Many activities in solar, wind, geothermal, photovoltaics, and other areas were initiated. The labs also became involved in establishing the Strategic Petroleum Reserve and supported initiatives in drilling and oil recovery. Significant tasking in renewable energy, conserving critical resources, such as fossil fuels and water, and teaming with international partners to explore the possibilities of fusion energy are ongoing and represent an important component of the laboratories' missions. Like nuclear weapon work, funding for energy research at the national labs is supplied by DOE.

The early 1990s not only saw the end of the Cold War, but also a rise in concern about loss of U.S. competitiveness in world markets. The economic threat posed to the U.S. by other nations was significant. In 1989, Congress passed the National Competitiveness Technology Transfer Act, which made technology transfer a mission of the nation's GOCO laboratories. As a result of this legislation, the national labs began working with U.S. industry via Cooperative Research and Development Agreements (CRADAs). Over the next few years, hundreds of CRADAs with individual companies and consortia were signed in many industries including automobiles, microelectronics, metallurgy, and defense, to name a few.

Since the end of the Cold War, the amount of nuclear weapon funding at the NNSA laboratories has decreased. Today only about 50% of the work at Sandia is related to nuclear weapons. Similar trends are occurring at Livermore and Los Alamos. Within a decade, all three labs will probably receive less than half of their funding from nuclear weapon sources.

Creating a Role for the National Laboratories

Previous chapters in this book have highlighted the concerns associated with terrorism, WMD, cyber security, and nuclear proliferation. As the sole superpower, the U.S. has become the primary focal point for envy, hatred, and distrust for extremist organizations and their sponsors around the globe. The easy movement of people and goods into the U.S. is important for economic

and political reasons. However, it must be counterbalanced against the threat that can be posed by even a small group of individuals, as was so dramatically demonstrated by the terrorist attacks of September 11, 2001.

Horrific concerns about a biological, nuclear, chemical, or radiological attack being conducted against the U.S. rightly receive center stage consideration by the DHS and by many other organizations in the federal government. However, devastating attacks that cripple our information or public and industrial infrastructure could also be mounted and do not even require, in the case of a cyber attack, for anyone to cross our borders.

New technologies of all sorts will be essential in addressing the homeland security challenge. The executive branch agencies and Congress recognize this need. Congress emphasized the importance of the national laboratories in supporting DHS in the Homeland Security Act of 2002 that founded the department. In it, Congress authorized the DHS secretary to utilize the DOE national labs and put DHS assignments on an equal footing with the nuclear weapon mission of the labs. Historically, the national labs have been assigned multiple missions; however, the nuclear weapon mission has always held preeminence and other work is conducted on the basis that it does not interfere with this primary mission. Congress sent the clear message that it wanted DHS to have unfettered access to the DOE labs and that no mission was more important than DHS's. The legislation further authorized the secretary of DHS to employ the national labs through a variety of methods. DHS could jointly sponsor a national lab with the DOE, it could contract directly with a national laboratory for services or it could use more traditional work for others (WFO) agreements that contract for a national laboratory's services through DOE. This authority was granted to give the DHS maximum flexibility in tapping into the technical capabilities of the labs.

The National Strategy for Homeland Security issued by the Office of Homeland Security in 2002 called for the establishment of a national laboratory for homeland security patterned after the DOE laboratories. While it is unlikely at this time that a dedicated DHS laboratory will be created, the need for a powerful, governmentally based, technology center to support the homeland security mission was clearly identified in the document.

In December 2003, Homeland Security Presidential Directive 7 (HSPD-7) was released. This directive identified and prioritized the infrastructural assets of the nation that needed to be protected and directed DHS to put together a plan for protecting these assets. The DHS secretary in coordination with the director of the Office of Science and Technology Policy must prepare on an annual basis a federal research and development plan to develop the technologies needed for homeland security. In response, the nation's first National Critical Infrastructure Protection Research and Development Plan (NCIP R&D Plan) was released in 2004. This R&D plan covers a 2-year time frame. The two goals to be accomplished are to: (1) catalog the major

R&D efforts already going on within the various federal agencies and (2) articulate a vision of the future R&D needs of DHS. This plan was crafted with the participation of numerous members taken from the national labs community.

The Directorate for Science and Technology (S&T) is the primary research and development arm of DHS. Four offices exist within the S&T Directorate. One of these, the Office of Research and Development is specifically focused on interactions with the national and federal labs and U.S. universities. Many of the national labs, including all three of the NNSA labs, have been identified as strategic partners of the S&T Directorate. Another office within the directorate, the Homeland Security Advanced Research Projects Agency (HSARPA) is patterned after the widely known Defense Advanced Research Projects Agency (DARPA) and focuses on more revolutionary technology solutions to DHS problems.

The National Laboratories and Homeland Security — Present and Future

The effort to harness the technological might of the nation in solving dauntingly complex homeland security problems is in its infancy. At the time of this writing, the DHS is little more than 3 years old. DHS is an amalgam of directorates and offices, some of which are new whereas others were transplanted largely intact from their previous organizations. At the present time, each of these elements reports directly to the secretary. Technological capabilities, such as those represented by the national laboratories, could benefit the missions of many of these department elements.

However, DHS has not existed long enough for the directorate of S&T to serve as the national labs' primary point of contact for the entire department. It is not surprising that many organizations — national laboratories, other federal laboratories, industry, and universities — have offered their services to DHS. As a result, projects have sprung up across DHS with a wide range of partners. Establishing a coordinated and integrated plan for homeland security was a primary reason for the creation of DHS, so it seems reasonable to expect that in coming years some level of overall coordination of the science and technology activities of the department will occur and that some strategic partnerships will emerge.

The DOE's national laboratories are logical choices as strategic partners of DHS for a variety of reasons. Their technical breadth and depth is unexcelled anywhere in the world. They are part of the U.S. government and have cleared personnel and facilities for handling large volumes of classified work. The national labs have a well established and ongoing heritage of responding

to the largest and most complex technical problems of national and international scope. In addition, the specific technology needs of DHS are very similar in nature to some of those that have been worked on for years at the national labs.

The national laboratories can have a strong impact on homeland security, particularly if they are given a mission to solve as opposed to a set of tasks to accomplish. The national labs have been extremely successful in their nuclear weapons mission because they have had cradle-to-grave responsibilities for the systems, have nurtured investments in core capabilities and new technologies over many years, and have participated in policy debates at the highest levels of government. It is also important to note that many of the technological capabilities in people and facilities needed for homeland security already exist at the labs. The DHS can leverage existing capacity within the laboratories in a shorter time and with less expense than trying to create such an infrastructure from scratch elsewhere.

The national labs are already working on numerous DHS projects, and these are likely to grow both in number and size. The range of activities covers all of the key technology areas laid out in the NCIP R&D plan. In addition, the labs are making additional investments in homeland security technologies using internal research and development funds. DHS and two of the national labs, Los Alamos and Sandia, have set up the National Infrastructure Simulation and Analysis Center (NISAC). NISAC provides advanced modeling and simulation capabilities for analyzing critical infrastructures, their interdependencies, and their vulnerabilities. This Center is important for several reasons: it is proactively focused on identifying potential issues before they become problems, it represents a systems-based approach to homeland security, and it is the first instance in which DHS has actually purchased and set up a substantial facility at an NNSA site. NISAC could serve as a prototype for establishing other DHS capabilities at the national laboratories. There are undoubtedly significant challenges to be overcome before the national labs can have the kind of impact on homeland security that is possible; however, progress is being made and many people at DHS, DOE, and the national laboratories are dedicated to its success.

Acknowledgment

The author would like to thank Billy Marshall, Jr. of Sandia National Laboratories for his helpful discussions regarding the role of the national laboratories in homeland security.

References

1. In addition to an extensive literature in book form, the Internet has many good sources covering the history of atomic energy and the national laboratories. The DOE, NNSA, and each of the national laboratories provide overviews of their history and missions. Many of the websites containing historical information regarding these institutions can be found at: http://www.nnsa.doe.gov/links.htm
2. A thorough overview of the history of Sandia National Laboratories can be found in, "Sandia National Laboratories: A History of Exceptional Service in the National Interest" by Leland Johnson, Sandia National Laboratories Report SAND97-1029, 1997.

An All-Hazards National Response Plan: Concluding Remarks

15

THOMAS A. JOHNSON

Contents

Our nation's focus on the prevention of any terrorist attack that utilizes weapons based on chemical, biological, radiological, nuclear, or explosives has been expanded to include any hazard that could cause damage or threaten lives, which may be caused by other forces of nature. The creation of our nation's National Response Plan is a direct result of Homeland Security Presidential Directive-5 which establishes a single comprehensive approach to domestic incident management to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The National Response Plan is an all-hazards plan built on the template of the National Incident Management System (NIMS).

The NIMS provides a consistent doctrinal framework for incident management at all jurisdictional levels regardless of the cause, size, or complexity of the incident. The National Response Plan (NRP), using the NIMS, provides the structure and mechanisms for national-level policy and operational direction for domestic incident management. The NRP can be partially or fully implemented in the context of a threat, anticipation of a significant event, or in response to an incident requiring a coordinated federal response. This includes events with potential national or long-term

implications, such as a public health emergency or a cyber incident. Selective implementation through the activation of one or more of the NRP elements allows maximum flexibility to meet the unique operational and information-sharing requirements of any situation and enables effective interaction among various federal, state, local, tribal, private sector, and other nongovernmental entities.

The NRP is applicable to all federal departments and agencies that have primary jurisdiction for or participate in operations requiring a coordinated federal response. The NRP also applies to the American Red Cross, which functions as an emergency support function (ESF) primary organization in coordinating the use of mass care resources.[1]

The question of what constitutes an incident of national significance (INS) that would activate our NRP is answered by the fact that our NRP is always in effect, it is only a matter of flexibility and scalability depending on the needs of the situation and the level of response required as to whether local, state, or federal agencies would be required to participate. The contingency plans of agencies at each level of government or private sector agencies would be invoked on a "need for" basis as enumerated in our National Response base plan.

An INS is an actual or potential high-impact event that requires robust coordination of the federal response in order to save lives and minimize damage and provides the basis for long-term community and economic recovery. The Secretary of Homeland Security, in consultation with other departments and agencies, and the White House, as appropriate, declares incidents of national significance. There are no automatic triggers for an INS. The Secretary of Homeland Security will consider the HSPD-5 criteria of the NRP when making the determination to declare an INS, but will also evaluate other factors in making a determination as to whether to declare an incident an INS. The Secretary of Homeland Security will manage the federal government's response following the declaration of an INS.[2]

As a result of the terrorist attacks on the U.S. on September 11, 2001, President George W. Bush has issued numerous Homeland Security Presidential Directives to address and manage these crises. HSPD-5, which articulates a NRP, was also severely tested by Hurricane Katrina in which FEMA, as a member agency of the U.S. Department of Homeland Security, was to play a major role in responding to this disastrous level-five hurricane. Therefore, irrespective as to the cause of the attack or nature of the disaster, our NRP is to guide our local, state, and federal agencies in responding to the incident in question. A brief outline of how this NRP is activated is described below.

The Incident Command Post

When an incident occurs, the appropriate jurisdictional authority (federal, state, or local) designates a single incident commander with overall incident management responsibility. Most jurisdictions predesignate their incident commanders in preparedness plans. The incident commander directs operations from the Incident Command Post (ICP).

The National Incident Management System/Incident Command System Unified Command

In many incidents (for example, during the response to a bombing that may have counterterrorism nexus), more than one federal, state, or local agency will have jurisdiction. As a team effort, the agency incident commanders form a Unified Command that overcomes much of the inefficiency and duplication of effort that can occur when agencies from different functional and geographic jurisdictions, or agencies at different levels of government, operate without a common system or organizational framework.

At the ICP, the Unified Command develops the NIMS incident command organizational structure in a top-down, modular fashion based on:

- Size and complexity of the incident
- Specifics of the hazard environment created by the incident

As federal, state, and local responders deploy, they must, regardless of agency affiliation, report to the ICP to receive an assignment in accordance with the procedures established by the Unified Command. At this juncture, they are under the tactical control of the Unified Command. Agencies with jurisdictional responsibility join the Unified Command, whereas agencies that lack jurisdictional responsibility, but are heavily involved in the incident:

- Are defined as supporting agencies
- Are represented in the command structure
- Effect coordination on behalf of their parent agency through a liaison officer attached to the Unified Command

Emergency Operations Center

Immediately on receiving notification of a significant incident or potential incident, the Unified Command will notify appropriate federal, state, and local emergency operations centers (EOCs). The EOCs coordinate support functions and provide resource support. Specific functions include:

- Multiagency coordination
- Communications
- Resource dispatch and tracking
- Information collection, analysis, and dissemination

National Operations Center

On receipt of a threat or incident notification, the National Operations Center (NOC) assesses the overall situation and makes an initial determination to initiate the coordination of federal information sharing and incident management activities.

Implementation of NRP coordination mechanisms is flexible and scalable. Actions range in scope from ongoing situational reporting and analysis, through the implementation of NRP Incident Annexes and other supplemental federal contingency plans, to full implementation of all relevant NRP coordination mechanisms outlined in the NRP base plan.

During incidents or potential incidents of lesser severity than an INS, the secretary may receive (through the NOC) requests for the activation of any NRP coordination mechanism.

Secretary of Homeland Security

Where the threat or incident is or may evolve into an INS, the NOC reports to the Secretary of Homeland Security and/or senior staff as delegated by the secretary, who then determines the need to implement components of the NRP to conduct further assessment of the situation, initiate interagency coordination, share information with affected jurisdictions and the private sector, and/or initiate deployment of resources. Concurrently, the secretary also makes a determination of whether an event should be designated as an INS.

> The NRP distinguishes between incidents that require the Secretary of Homeland Security to manage the Federal Response, termed Incidents of National Significance, and the majority of incidents occurring each year that are handled by responsible jurisdictions or agencies through other established authorities and existing plans executed in coordination with the NRP's comprehensive framework of Incident Annexes. When the Secretary of Homeland Security declares an Incident of National Significance, the Secretary will manage the Federal response.[3]

The manner in which our NRP and our NIMS can effectively coordinate local, state, and federal agencies response to a range of incidents from a minor level to an extreme national security threat level is fundamental to our nation's security. The NRP and NIMS are companion documents designed to improve the nation's incident management capabilities and overall efficiency.

The NIMS provides a template for incident management regardless of size, scope, or cause. Use of this template enables federal, state, local, and tribal governments and private sector and nongovernmental organizations to work together effectively and efficiently to prevent, prepare for, respond to, and recover from actual or potential domestic incidents regardless of cause, size, or complexity. Together, the NRP and NIMS integrate the capabilities and resources of various governmental jurisdictions, incident management, and emergency response disciplines with private sector organizations into a cohesive, coordinated, and seamless national framework for domestic incident management.[4] This theoretical blueprint for engaging multiple agencies into our NRP will require a substantial evaluation component, particularly since this effort is exploring new reactive responses to extraordinarily difficult challenges. The ability of our NRP to guide our agencies in protecting our nation from attacks in which chemical, biological, radiological, nuclear, or explosives might be utilized will be dependent on how effective our intelligence agencies will be in the collection and analysis of information in support of agencies response to incidents involving these weapons.

For almost 50 years after the passage of the National Security Act of 1947, the intelligence community's resources were overwhelmingly trained on a single threat — the Soviet Union, its nuclear arsenal, its massive conventional forces, and its activities around the world. By comparison, today's priority intelligence targets are greater in number (there are dozens of entities that could strike a devastating blow against the U.S.) and are often more diffuse in character (they include not only states, but also nebulous transnational terror and proliferation networks). What is more, some of the weapons that would be most dangerous in the hands of terrorists or rogue nations are difficult to detect. Much of the technology, equipment, and materials necessary to develop biological and chemical weapons, for example, also have legitimate commercial applications. Biological weapons themselves can be built in small-scale facilities that are easy to conceal and weapons-grade uranium can be effectively shielded from traditional detection techniques. At the same time, advances in technology have made the job of technical intelligence collection exceedingly difficult.

The demands of this new environment can only be met by broad and deep change in the intelligence community. The intelligence community we have today is buried beneath an avalanche of demands for "current intelligence" — the pressing need to meet the tactical requirements of the day. Current intelligence in support of military and other action is necessary, of course, but we also need an intelligence community with strategic capabilities. It must be equipped to develop long-term plans for penetrating today's difficult targets and to identify political and social trends shaping the threats that lie over the horizon. We can imagine no threat that demands greater strategic focus from the intelligence community than that posed by nuclear, biological, and chemical weapons.[5]

Some of the recommendations for improving our intelligence agencies abilities to more effectively perform their duties were noted by the Commission on the Intelligence Capabilities of the U.S. as follows:

- Create a new intelligence community process for managing collection as an "integrated enterprise"
- Create strategies for focusing collection on priority targets utilizing more sophisticated technical collection systems
- Create a new Human Intelligence Directorate
- Establish a National Counter Proliferation Center
- Establish an "innovation center" to develop new innovative human intelligence techniques
- Create an open source directorate within the CIA and utilize it as a primary test bed for new information technology
- Analytic expertise must be deepened, intelligence gaps reduced, and existing information made more usable
- Improve the rigor and "tradecraft" of analysis by increasing analyst training, and standardizing good tradecraft practices through the use of a National Intelligence University[6]

Regarding the issue of proliferation that our intelligence community must continue to make improvements, the Commission offers sound advice. The intelligence community also needs to change the way it approaches two of the greatest threats — biological weapons and new forms of nuclear proliferation.

Biological Weapons

The 2001 anthrax attacks on the U.S. killed five people, crippled mail delivery in several cities for a year, and imposed more than a billion dollars in decontamination costs. For all that, we were fortunate our loss of life was not greater than what we experienced. Since biological weapons are less expensive and easier to acquire than nuclear weapons and because genetic modification techniques will allow the creation of even worse biological weapons, the dangers we will confront in the future will expand as scientific knowledge increases. Most of the traditional intelligence community collection tools are of little or no use in tracking biological weapons. The intelligence community, and the government as a whole, needs to approach the problem with a new urgency and new strategies.

- *Work with the biological sciences community.* The intelligence community simply does not have the in-depth technical knowledge about biological weapons that it has about nuclear weapons. To close the expertise gap, the community cannot rely on hiring biologists, whose knowledge and skills are extremely important, but whose depth and timelines of expertise

begins eroding as soon as they move from the laboratory to the intelligence profession. Instead, the Director of National Intelligence (DNI) should create a community biodefense initiative to institutionalize outreach to technical experts inside and outside of government.

- *Make targeted collection of biological weapons intelligence a priority within the intelligence community.* The intelligence community's collection woes starkly illustrate the need for more aggressive, targeted approaches to collection on biological threats. We recommend that the DNI create a deputy within the National Counter Proliferation Center who is specifically responsible for biological weapons; this deputy would ensure the implementation of a comprehensive biological weapons targeting strategy, which would entail gaining real-time access to nontraditional sources of information, filtering open source data, and devising specific collection initiatives directed at the resulting targets.
- *Leverage regulation for biological weapons intelligence.* The U.S. should look outside of intelligence channels for enforcement mechanisms that can provide new avenues of international cooperation and resulting opportunities for intelligence collection on biological threats. We recommend encouraging foreign criminalization of biological weapons development and establishing biosafety and biosecurity regulations under United Nations Security Council Resolution 1540. We also propose extending biosecurity and biosafety regulations to foreign institutions with commercial ties to the U.S.[7]

Nuclear Weapons

The intelligence challenge posed by nuclear weapons continues to evolve. The intelligence community must continue to monitor established nuclear states such as Russia and China and at the same time, face newer and potentially more daunting challenges like terrorist use of a nuclear weapon. But the focus of the U.S. intelligence community has historically been on the capabilities of large nation–states. When applied to the problem of terrorist organizations and smaller states, many of our intelligence capabilities are inadequate.

The challenges posed by the new environment are well illustrated by two aspects of nuclear proliferation. The first is the continuing challenge of monitoring insecure nuclear weapons and materials, or "loose nukes" — mainly in the former Soviet Union, but also potentially in other nations. The second aspect is the appearance of nonstate nuclear "brokers," such as the private proliferation network run by the Pakistani scientist A. Q. Khan. In Khan's case, innovative human intelligence efforts gave the U.S. access to this proliferation web. However, not only does the full scope of Khan's work remain unknown, but senior officials readily acknowledge that the intelligence community must

know more about the private networks that support proliferation. The intelligence community must adapt to the changing threat.[8]

The linkage of our intelligence capabilities to our NRP is critical to providing our agencies with the information they will require to provide the level of prevention, protection, and response in the event of any incident manifesting itself.

The Intelligence Reform and Terrorism Prevention Act of 2004 provided a new management structure for the intelligence community, since it was the conclusion of Congress that our intelligence community needed substantial reorganization. The position of DNI was created to serve as the administrator of our intelligence community and also as the principal advisor to the president on intelligence matters related to national security. In addition, the Intelligence Reform and Terrorism Prevention Act also established for the first time an Office of the DNI (ODNI) with the following sections within the DNI Office:

The National Counterterrorism Center serves as the primary organization in the U.S. government for analyzing and integrating all intelligence possessed or acquired by the U.S. government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism. The National Counterterrorism Center (NCTC) also conducts strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies. Other national centers that may be created in addition to NCTC (for example, a new *National Counter Proliferation Center*) would also be part of the ODNI.

The National Intelligence Council is responsible for producing National Intelligence Estimates (NIEs) for the U.S. government and evaluating community-wide collection and production of intelligence by the intelligence community.

The National Counterintelligence Executive is responsible for improving the performance of the counterintelligence community in assessing, prioritizing, and countering intelligence threats to the U.S. and providing integration of counterintelligence activities of the U.S. government.

The Director for Science and Technology is to act as the chief representative of the DNI for science and technology and to assist the DNI in formulating a long-term strategy for scientific advances in the field of intelligence.

A Civil Liberties Protection Officer will ensure that the protection of civil liberties and privacy is appropriately incorporated into the policies and procedures developed by the ODNI.

A General Counsel will serve as the chief legal officer for the ODNI.
The statute also establishes the *Joint Intelligence Community Council*, which consists of the heads of each department that contains a component of the intelligence community (e.g., Secretary of Defense), and which will assist the DNI in developing and implementing a joint, unified national intelligence effort to protect national security.[9]

As a result of the Intelligence Reform and Terrorism Prevention Act of 2004, we now find our nations intelligence resources grouped within three major categories:

1. The National Intelligence Program (NIP)
2. The Joint Military Intelligence Program (JMIP)
3. Tactical Intelligence and Related Activities (TIARA)

The NIP provides the DNI with the full authority to develop the budget and allocate resources within the NIP. The agencies and organizations, which are included consist of the Central Intelligence Agency, National Security Agency, Defense Investigative Agency, National Geospatial Agency, National Reconnaissance Office, and the Intelligence Bureaus within the Department of State, Department of Justice, Department of Energy, and the Department of the Treasury.[10]

The JMIP includes military intelligence activities that support Department of Defense objectives, as opposed to individual military branch intelligence departments and offices. The JMIP remains under the full authority of the Secretary of Defense, with the Deputy Secretary of Defense responsible for supervision of daily activities and the Under Secretary of Defense for Intelligence Services serving as the JMIP program executive responsible for policy and program activities.[11]

The TIARA Program also is under the command of the Secretary of Defense and includes special activities and intelligence operations funded by each of the military services and the Special Operations Command. The DNI will participate in the budget development of both the JMIP and the TIARA Program; however, the DNI will not have authority over these areas as they will remain within the Department of Defense.[12]

The complexity of the reorganization of our intelligence community not only creates new offices, but provides for authority in 4 major cabinet level departments and includes 15 federal agencies. Also, the consultative relationship with the Department of Defense suggests the level of diplomacy required to successfully manage the NIP. It is also worth noting the levels of bureaucratic resistance endemic to such a massive reorganization that may complicate our nation's ability to develop programs that will cooperate and coordinate these activities. Indeed, our recent experience with the massive

reorganization of 22 federal agencies and their reassignment to a new Department of Homeland Security is documentation as to major levels of resistance and difficult organizational redeployments. Finally, our NRP that attempts to provide an integrated response to any national hazard or terrorist threat, while at the same time allocating responsibilities to all federal agencies, is clearly a most optimistic and aggressive plan.

The national security issues that confront our nation require a thoughtful and creative plan of action. The National Security Strategy and the Homeland Security Presidential Directives included in Appendix A and Appendix B provide evidence of the collective efforts of our nation's leaders in formulating a strategy to protect our citizens. The NRP, which engages all levels of government, as well as private sector agencies, requires cooperation and a level of commitment to excellence that will be required of all of our citizens.

Finally, the numerous national security challenges our nation will confront in the coming years will require a greater commitment from our universities. We must prepare the next generation of leaders who will assume responsible positions within our national security entities; our intelligence community; and the local, state, and federal agencies with the educational skills and insights to manage and creatively provide strategies to protect our nation and its citizens.

References

1. U.S. Department of Homeland Security, Quick Reference Guide for the National Response Plan, May 22, 2006, 11, Version 4.0, p. 1. This Quick Reference Guide does not supersede the NRP, as modified by the notice of change. If language in the Guide conflicts with the NRP as modified by the notice, the structures and mechanisms of the NRP take precedence.
2. Ibid., p. 2.
3. Ibid., pp. 21–22.
4. Ibid., p. 5.
5. Report to the President of the United States, The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Mar. 31, 2005, pp. 4–5.
6. Ibid., pp. 19–26.
7. Ibid., pp. 34–35.
8. Ibid., pp. 35–36.
9. Ibid., pp. 585–586.
10. Ibid., p. 587.
11. Ibid., p. 588
12. Ibid., p. 588

Appendices

Introduction

Appendix A includes the National Security Strategy of the United States of America as issued March 16, 2006. This is the second such strategy issued by President George W. Bush, the first being issued in 2002 during his first term in office and after the September 11, 2001 attack against the U.S. The current 2006 National Security Strategy builds on the previous 2002 National Security Strategy, which emphasized strengthening our nation's alliances with other countries in our effort to defeat global terrorism. This National Security Strategy focuses more attention as to our need to transform our national security institutions to meet the challenges our nation will confront in the 21st century.

It is unusual for any nation to so publicly proclaim its National Security Strategy and President George W. Bush has more than any other U.S. president, articulated our nations National Security Strategy to the entire community of nations and the world. There obviously exist more defined and classified policies and presidential decision directions, but it is important to appreciate how the broader framework of our National Security Strategy may provide the basis on which subsequent national security decisions may be shaped and contoured to future challenges.

The creation of our National Security Strategy requires extensive consultation and input from those agencies each responsible for other respective areas of national security. This implies not only agency-level directors, but also Cabinet-level secretaries and under-secretaries. The role of the National Security Council in this process will also be critical as it prepares white papers, drafts policies, and presents national security initiatives to the president for presidential action.

The National Security Act of 1947 created for the first time in our nation a National Security Council, under the chairmanship of the president and with the Secretaries of State and Defense as its key members to coordinate both

foreign policy and defense policy. Over the ensuing 59 years, modifications as to the membership of this Council and how large it would be, has actually been shaped by each new incoming president. In fact, the National Security Council has been so important that the last five presidents have issued Executive Orders (EOs) regarding its composition and functioning membership on the day of their inaugurations.

The function of the National Security Council as first outlined in the National Security Act of 1947 was to advise the president on the integration of domestic, foreign, and military policies related to national security and to facilitate interagency cooperation.[1]

Each new president has shaped the direction of the National Security Council by the appointments of not only its members, but also its committee structure and reporting policy. The important point is whether the National Security Council will be used for policy review, shaping national security policies and programs, or managing crisis in foreign policy. Presidents Kennedy, Johnson, Nixon, Ford, Carter, Reagan, George H. W. Bush, Clinton, and now George W. Bush have each used the National Security Council in each of the above described fashions. The key variable appears to be how close the National Security Advisor is to the president and the level of continuing access the National Security Advisor has to the president. The closer the relationship of the National Security Advisor to the president, the greater the likelihood that a strained relationship will emerge between the advisor and the Secretary of State, who has principal responsibility for foreign affairs and international matters, simply due to the fact that lines of authority and responsibility may become blurred. Therefore, the creation of a National Security Strategy that will receive the input and recommendations of Cabinet-level secretaries, military chiefs, agency-level directors, and Congressional advice and counsel is extremely difficult to formulate.

Another important part of our National Security Strategy is found in the process by which presidents use the National Security Council to review and assist in framing the policies, which will eventually be issued as a Presidential Directive or Executive Order.

Appendix B provides Executive Summaries of Homeland Security Presidential Directives 1 to 3; 5 to 14; all issued by President George W. Bush. Homeland Security Presidential Directive-4 remains classified. The flowing Homeland Security Presidential Directives by both subject matter and date of issue will be included in Appendix B to assist the reader in doing further research in the respective area covered by the Presidential Directive. For purposes of clarification: HS signifies Homeland Security and NS signifies National Security.

Presidential Directives Issued by President George W. Bush

National Security Instrument	Subject	Date
HSPD-1	Organization and Operation of the Homeland Security Council	10/29/01
HSPD-2	Combating Terrorism through Immigration Policies	10/29/01
HSPD-3	Homeland Security Advisory System	03/11/02
NSPD-17	National Strategy to Combat Weapons of Mass Destruction	12/2002
HSPD-4	Unclassified Version of NSPD-17	12/2002
HSPD-5	Management of Domestic Incidents	02/28/03
HSPD-6	Integration and Use of Screening Information	09/16/03
HSPD-7	Critical Infrastructure Identification Prioritization and Protection	12/17/03
HSPD-8	National Preparedness	12/17/03
HSPD-9	Defense of the United States Agriculture and Food	01/30/04
HSPD-10	Unclassified Version: Bio-Defense for the 21st Century	04/28/04
HSPD-11	Comprehensive Terrorist-Related Screening Procedures	08/27/04
HSPD-12	Policy for a Common Identification Standard for Federal Employees and Contractors	08/27/04
HSPD-13	Maritime Security Policy	12/21/04
NSPD-41	Maritime Security Policy	12/21/04
HSPD-14	Domestic Nuclear Detection	04/15/05
NSPD-43	Domestic Nuclear Detection	04/15/05

Every president since George Washington has issued at one time or another proclamations, announcements, executive orders, military orders, or presidential directives. These instruments of governance have come to be known by various names and each has prescribed forms and purposes. Executive orders and proclamations are the most common and well-known type and are published in the Federal Register and the Code of Federal Regulations (CFR).[2] Other forms are not as well known to the public partly because they become classified or remain less visibly published.

Presidential directives establish policy and have the force of law; executive orders are one of the oldest types of presidential directives and generally are issued concerning emergency situations and rely on the constitutional authority of powers granted to the president through our constitution. The numbering of executive orders began in President Lincoln's administration in 1862.[3]

National Security Instruments have only been available since the creation of the National Security Council in 1947, and they consist of the following:

All Presidents through George W. Bush	National Security Policy Papers
Presidents Kennedy and Johnson	• National Security Action Memoranda
Presidents Nixon and Ford	• National Security Study Memoranda and National Security Decision Memoranda
President Carter	• Presidential Review Memoranda and Presidential Directives
President Reagan	• National Security Study Memoranda and National Security Decision Directives
President George H. W. Bush	• National Security Reviews and National Security Directives
President Clinton	• Presidential Review Directives and Presidential Decision Directives
President George W. Bush	• National Security Presidential Directives and Homeland Security Presidential Directives[4]

In researching presidential directives, one can quickly observe that our last 10 presidents each used different processes to arrive at the issuance of presidential directives that addressed national security matters. Furthermore, in each of these administrations the use of the National Security Council occupied a critical role in the creation, review, and preparation of national security matters that eventually were expressed as presidential directives.

References

1. Office of the Historian, Bureau of Public Affairs, United States Department of State, "History of the National Security Council 1947–1997," August 1997, p. 3.
2. Harold C. Relyea, "Presidential Directives: Background and Overview," Congressional Research Service Report for Congress, The Library of Congress, January 7, 2005, p. 2.
3. Ibid., pp. 5–6.
4. Ibid., pp. 9-12.

Appendix A

National Security Strategy Summary

The National Security Strategy of the United States of America

MARCH 2006

The White House, Washington

My fellow Americans,

America is at war. This is a wartime national security strategy required by the grave challenge we face — the rise of terrorism fueled by an aggressive ideology of hatred and murder, fully revealed to the American people on September 11, 2001. This strategy reflects our most solemn obligation: to protect the security of the American people.

America also has an unprecedented opportunity to lay the foundations for future peace. The ideals that have inspired our history — freedom, democracy, and human dignity — are increasingly inspiring individuals and nations throughout the world. And because free nations tend toward peace, the advance of liberty will make America more secure.

These inseparable priorities — fighting and winning the war on terror and promoting freedom as the alternative to tyranny and despair — have now guided American policy for more than 4 years.

We have kept on the offensive against terrorist networks, leaving our enemy weakened, but not yet defeated.

We have joined with the Afghan people to bring down the Taliban regime — the protectors of the al-Qaida network — and aided a new, democratic government to rise in its place.

We have focused the attention of the world on the proliferation of dangerous weapons — although great challenges in this area remain.

We have stood for the spread of democracy in the broader Middle East — meeting challenges yet seeing progress few would have predicted or expected.

We have cultivated stable and cooperative relations with all the major powers of the world.

We have dramatically expanded our efforts to encourage economic development and the hope it brings — and focused these efforts on the promotion of reform and achievement of results.

We led an international coalition to topple the dictator of Iraq, who had brutalized his own people, terrorized his region, defied the international community, and sought and used weapons of mass destruction.

And we are fighting alongside Iraqis to secure a united, stable, and democratic Iraq — a new ally in the war on terror in the heart of the Middle East.

We have seen great accomplishments, confronted new challenges, and refined our approach as conditions changed. We have also found that the defense of freedom brings us loss and sorrow because freedom has determined enemies. We have always known that the war on terror would require great sacrifice — and in this war, we have said farewell to some very good men and women. The terrorists have used dramatic acts of murder — from the streets of Fallujah to the subways of London — in an attempt to undermine our will. The struggle against this enemy — an enemy that targets the innocent without conscience or hesitation — has been difficult. And our work is far from over.

America now faces a choice between the path of fear and the path of confidence. The path of fear — isolationism and protectionism, retreat and retrenchment — appeals to those who find our challenges too great and fail to see our opportunities. Yet history teaches that every time American leaders have taken this path, the challenges have only increased and the missed opportunities have left future generations less secure.

This Administration has chosen the path of confidence. We choose leadership over isolationism, and the pursuit of free and fair trade and open markets over protectionism. We choose to deal with challenges now rather than leaving them for future generations. We fight our enemies abroad instead of waiting for them to arrive in our country. We seek to shape the world, not merely be shaped by it; to influence events for the better instead of being at their mercy.

The path we have chosen is consistent with the great tradition of American foreign policy. Like the policies of Harry Truman and Ronald Reagan, our approach is idealistic about our national goals, and realistic about the means to achieve them.

To follow this path, we must maintain and expand our national strength so we can deal with threats and challenges before they can damage our people or our interests. We must maintain a military without peer — yet our strength is not founded on force of arms alone. It also rests on economic prosperity and a vibrant democracy. And it rests on strong alliances, friendships, and international institutions, which enable us to promote freedom, prosperity, and peace in common purpose with others.

Our national security strategy is founded upon two pillars:

The first pillar is promoting freedom, justice, and human dignity — working to end tyranny, to promote effective democracies, and to extend prosperity through free and fair trade and wise development policies. Free governments are accountable to their people, govern

their territory effectively, and pursue economic and political policies that benefit their citizens. Free governments do not oppress their people or attack other free nations. Peace and international stability are most reliably built on a foundation of freedom.

The second pillar of our strategy is confronting the challenges of our time by leading a growing community of democracies. Many of the problems we face — from the threat of pandemic disease, to proliferation of weapons of mass destruction, to terrorism, to human trafficking, to natural disasters — reach across borders. Effective multinational efforts are essential to solve these problems. Yet history has shown that only when we do our part will others do theirs. America must continue to lead.

George W. Bush
The White House
March 16, 2006

National Security Strategy: March 2006

Table of Contents

I. Overview of America's National Security Strategy

It is the policy of the United States to seek and support democratic movements and institutions in every nation and culture, with the ultimate goal of ending tyranny in our world. In the world today, the fundamental character of regimes matters as much as the distribution of power among them. The goal of our statecraft is to help create a world of democratic, well-governed states that can meet the needs of their citizens and conduct themselves responsibly in the international system. This is the best way to provide enduring security for the American people.

Achieving this goal is the work of generations. The United States is in the early years of a long struggle, similar to what our country faced in the early years of the Cold War. The 20th century witnessed the triumph of freedom over the threats of fascism and communism. Yet a new totalitarian ideology now threatens, an ideology grounded not in secular philosophy but in the perversion of a proud religion. Its content may be different from the ideologies of the last century, but its means are similar: intolerance, murder, terror, enslavement, and repression.

Like those who came before us, we must lay the foundations and build the institutions that our country needs to meet the challenges we face. The chapters that follow will focus on several essential tasks. The United States must:

- Champion aspirations for human dignity;
- Strengthen alliances to defeat global terrorism and work to prevent attacks against us and our friends;
- Work with others to defuse regional conflicts;
- Prevent our enemies from threatening us, our allies, and our friends with weapons of mass destruction (WMD);
- Ignite a new era of global economic growth through free markets and free trade;
- Expand the circle of development by opening societies and building the infrastructure of democracy;
- Develop agendas for cooperative action with other main centers of global power;
- Transform America's national security institutions to meet the challenges and opportunities of the 21st century; and
- Engage the opportunities and confront the challenges of globalization.

II. Champion Aspirations for Human Dignity

A. Summary of National Security Strategy 2002

The United States must defend liberty and justice because these principles are right and true for all people everywhere. These nonnegotiable demands of

human dignity are protected most securely in democracies. The United States Government will work to advance human dignity in word and deed, speaking out for freedom and against violations of human rights and allocating appropriate resources to advance these ideals.

B. Successes and Challenges Since 2002

Since 2002, the world has seen extraordinary progress in the expansion of freedom, democracy, and human dignity:

- The peoples of Afghanistan and Iraq have replaced tyrannies with democracies.
  - In Afghanistan, the tyranny of the Taliban has been replaced by a freely-elected government; Afghans have written and ratified a constitution guaranteeing rights and freedoms unprecedented in their history; and an elected legislature gives the people a regular voice in their government.
  - In Iraq, a tyrant has been toppled; over 8 million Iraqis voted in the nation's first free and fair election; a freely negotiated constitution was passed by a referendum in which almost 10 million Iraqis participated; and, for the first time in their history, nearly 12 million Iraqis have elected a permanent government under a popularly determined constitution.
- The people of Lebanon have rejected the heavy hand of foreign rule. The people of Egypt have experienced more open but still flawed elections. Saudi Arabia has taken some preliminary steps to give its citizens more of a voice in their government. Jordan has made progress in opening its political process. Kuwait and Morocco are pursuing agendas of political reform.
- The "color revolutions" in Georgia, Ukraine, and Kyrgyzstan have brought new hope for freedom across the Eurasian landmass.
- Democracy has made further advances in Africa, Latin America, and Asia, with peaceful transfers of power; growth in independent judiciaries and the rule of law; improved election practices; and expanding political and economic rights.

The human desire for freedom is universal, but the growth of freedom is not inevitable. Without support from free nations, freedom's spread could be hampered by the challenges we face:

- Many governments are at fragile stages of political development and need to consolidate democratic institutions — and leaders that have won democratic elections need to uphold the principles of democracy;

- Some governments have regressed, eroding the democratic freedoms their peoples enjoy;
- Some governments have not delivered the benefits of effective democracy and prosperity to their citizens, leaving them susceptible to or taken over by demagogues peddling an anti-free market authoritarianism;
- Some regimes seek to separate economic liberty from political liberty, pursuing prosperity while denying their people basic rights and freedoms; and Tyranny persists in its harshest form in a number of nations.

C. The Way Ahead

The United States has long championed freedom because doing so reflects our values and advances our interests. It reflects our values because we believe the desire for freedom lives in every human heart and the imperative of human dignity transcends all nations and cultures.

Championing freedom advances our interests because the survival of liberty at home increasingly depends on the success of liberty abroad. Governments that honor their citizens' dignity and desire for freedom tend to uphold responsible conduct toward other nations, while governments that brutalize their people also threaten the peace and stability of other nations. Because democracies are the most responsible members of the international system, promoting democracy is the most effective long-term measure for strengthening international stability; reducing regional conflicts; countering terrorism and terror-supporting extremism; and extending peace and prosperity.

To protect our Nation and honor our values, the United States seeks to extend freedom across the globe by leading an international effort to end tyranny and to promote effective democracy.

1. Explaining the Goal: Ending Tyranny

Tyranny is the combination of brutality, poverty, instability, corruption, and suffering, forged under the rule of despots and despotic systems. People living in nations such as the Democratic People's Republic of Korea (DPRK), Iran, Syria, Cuba, Belarus, Burma, and Zimbabwe know firsthand the meaning of tyranny; it is the bleak reality they endure every day. And the nations they border know the consequences of tyranny as well, for the misrule of tyrants at home leads to instability abroad. All tyrannies threaten the world's interest in freedom's expansion, and some tyrannies, in their pursuit of WMD or sponsorship of terrorism, threaten our immediate security interests as well.

Tyranny is not inevitable, and recent history reveals the arc of the tyrant's fate. The 20th century has been called the "Democracy Century," as tyrannies fell one by one and democracies rose in their stead. At mid-century about two dozen of the world's governments were democratic; 50 years later this

number was over 120. The democratic revolution has embraced all cultures and all continents.

Though tyranny has few advocates, it needs more adversaries. In today's world, no tyrant's rule can survive without the support or at least the tolerance of other nations. To end tyranny we must summon the collective outrage of the free world against the oppression, abuse, and impoverishment that tyrannical regimes inflict on their people — and summon their collective action against the dangers tyrants pose to the security of the world.

An end to tyranny will not mark an end to all global ills. Disputes, disease, disorder, poverty, and injustice will outlast tyranny, confronting democracies long after the last tyrant has fallen. Yet tyranny must not be tolerated — it is a crime of man, not a fact of nature.

2. Explaining the Goal: Promoting Effective Democracies

As tyrannies give way, we must help newly free nations build effective democracies: states that are respectful of human dignity, accountable to their citizens, and responsible towards their neighbors. Effective democracies:

- Honor and uphold basic human rights, including freedom of religion, conscience, speech, assembly, association, and press;
- Are responsive to their citizens, submitting to the will of the people, especially when people vote to change their government;
- Exercise effective sovereignty and maintain order within their own borders, protect independent and impartial systems of justice, punish crime, embrace the rule of law, and resist corruption; and
- Limit the reach of government, protecting the institutions of civil society, including the family, religious communities, voluntary associations, private property, independent business, and a market economy.

In effective democracies, freedom is indivisible. Political, religious, and economic liberty advance together and reinforce each other. Some regimes have opened their economies while trying to restrict political or religious freedoms. This will not work. Over time, as people gain control over their economic lives, they will insist on more control over their political and personal lives as well. Yet political progress can be jeopardized if economic progress does not keep pace. We will harness the tools of economic assistance, development aid, trade, and good governance to help ensure that new democracies are not burdened with economic stagnation or endemic corruption.

Elections are the most visible sign of a free society and can play a critical role in advancing effective democracy. But elections alone are not enough — they must be reinforced by other values, rights, and institutions to bring about lasting freedom. Our goal is human liberty protected by democratic institutions.

Participation in elections by individuals or parties must include their commitment to the equality of all citizens, minority rights, civil liberties, voluntary and peaceful transfer of power, and the peaceful resolution of differences. Effective democracy also requires institutions that can protect individual liberty and ensure that the government is responsive and accountable to its citizens. There must be an independent media to inform the public and facilitate the free exchange of ideas. There must be political associations and political parties that can freely compete. Rule of law must be reinforced by an independent judiciary, a professional legal establishment, and an honest and competent police force.

These principles are tested by the victory of Hamas candidates in the recent elections in the Palestinian territories. The Palestinian people voted in a process that was free, fair, and inclusive.

The Palestinian people having made their choice at the polls, the burden now shifts to those whom they have elected to take the steps necessary to advance peace, prosperity, and statehood for the Palestinian people. Hamas has been designated as a terrorist organization by the United States and European Union (EU) because it has embraced terrorism and deliberately killed innocent civilians. The international community has made clear that there is a fundamental contradiction between armed group and militia activities and the building of a democratic state. The international community has also made clear that a two-state solution to the conflict requires all participants in the democratic process to renounce violence and terror, accept Israel's right to exist, and disarm as outlined in the Roadmap. These requirements are clear, firm, and of long standing. The opportunity for peace and statehood — a consistent goal of this Administration — is open if Hamas will abandon its terrorist roots and change its relationship with Israel.

The elected Hamas representatives also have an opportunity and a responsibility to uphold the principles of democratic government, including protection of minority rights and basic freedoms and a commitment to a recurring, free, and fair electoral process. By respecting these principles, the new Palestinian leaders can demonstrate their own commitment to freedom and help bring a lasting democracy to the Palestinian territories. But any elected government that refuses to honor these principles cannot be considered fully democratic, however it may have taken office.

3. How We Will Advance Freedom: Principled in Goals and Pragmatic in Means

We have a responsibility to promote human freedom. Yet freedom cannot be imposed; it must be chosen. The form that freedom and democracy take in any land will reflect the history, culture, and habits unique to its people.

The United States will stand with and support advocates of freedom in every land. Though our principles are consistent, our tactics will vary. They will reflect, in part, where each government is on the path from tyranny to democracy. In some cases, we will take vocal and visible steps on behalf of immediate change. In other cases, we will lend more quiet support to lay the foundation for future reforms. As we consider which approaches to take, we will be guided by what will most effectively advance freedom's cause while we balance other interests that are also vital to the security and well-being of the American people.

In the cause of ending tyranny and promoting effective democracy, we will employ the full array of political, economic, diplomatic, and other tools at our disposal, including:

- Speaking out against abuses of human rights;
- Supporting publicly democratic reformers in repressive nations, including by holding high-level meetings with them at the White House, Department of State, and U.S. Embassies;
- Using foreign assistance to support the development of free and fair elections, rule of law, civil society, human rights, women's rights, free media, and religious freedom;
- Tailoring assistance and training of military forces to support civilian control of the military and military respect for human rights in a democratic society;
- Applying sanctions that designed to target those who rule oppressive regimes while sparing the people;
- Encouraging other nations not to support oppressive regimes;
- Partnering with other democratic nations to promote freedom, democracy, and human rights in specific countries and regions;
- Strengthening and building new initiatives such as the Broader Middle East and North Africa Initiative's Foundation for the Future, the Community of Democracies, and the United Nations Democracy Fund;
- Forming creative partnerships with nongovernmental organizations and other civil society voices to support and reinforce their work;
- Working with existing international institutions such as the United Nations and regional organizations such as the Organization for Security and Cooperation in Europe, the African Union (AU), and the Organization of American States (OAS) to help implement their democratic commitments, and helping establish democracy charters in regions that lack them;
- Supporting condemnation in multilateral institutions of egregious violations of human rights and freedoms;
- Encouraging foreign direct investment in and foreign assistance to countries where there is a commitment to the rule of law, fighting corruption, and democratic accountability; and

- Concluding free trade agreements (FTAs) that encourage countries to enhance the rule of law, fight corruption, and further democratic accountability.

These tools must be used vigorously to protect the freedoms that face particular peril around the world: religious freedom, women's rights, and freedom for men, women, and children caught in the cruel network of human trafficking.

- Against a terrorist enemy that is defined by religious intolerance, we defend the First Freedom: the right of people to believe and worship according to the dictates of their own conscience, free from the coercion of the state, the coercion of the majority, or the coercion of a minority that wants to dictate what others must believe.
- No nation can be free if half its population is oppressed and denied fundamental rights. We affirm the inherent dignity and worth of women, and support vigorously their full participation in all aspects of society.
- Trafficking in persons is a form of modern-day slavery, and we strive for its total abolition. Future generations will not excuse those who turn a blind eye to it.

Our commitment to the promotion of freedom is a commitment to walk alongside governments and their people as they make the difficult transition to effective democracies. We will not abandon them before the transition is secure because immature democracies can be prone to conflict and vulnerable to exploitation by terrorists. We will not let the challenges of democratic transitions frighten us into clinging to the illusory stability of the authoritarian.

America's closest alliances and friendships are with countries with whom we share common values and principles. The more countries demonstrate that they treat their own citizens with respect and are committed to democratic principles, the closer and stronger their relationship with America is likely to be.

The United States will lead and calls on other nations to join us in a common international effort. All free nations have a responsibility to stand together for freedom because all free nations share an interest in freedom's advance.

III. Strengthen Alliances to Defeat Global Terrorism and Work to Prevent Attacks against Us and Our Friends

A. Summary of National Security Strategy 2002

Defeating terrorism requires a long-term strategy and a break with old patterns. We are fighting a new enemy with global reach. The United States can no longer simply rely on deterrence to keep the terrorists at bay or defensive

measures to thwart them at the last moment. The fight must be taken to the enemy, to keep them on the run. To succeed in our own efforts, we need the support and concerted action of friends and allies. We must join with others to deny the terrorists what they need to survive: safe haven, financial support, and the support and protection that certain nation-states historically have given them.

B. Current Context: Successes and Challenges

The war against terror is not over. America is safer, but not yet safe. As the enemy adjusts to our successes, so too must we adjust. The successes are many:

- Al-Qaida has lost its safe haven in Afghanistan.
- A multinational coalition joined by the Iraqis is aggressively prosecuting the war against the terrorists in Iraq.
- The al-Qaida network has been significantly degraded. Most of those in the al-Qaida network responsible for the September 11 attacks, including the plot's mastermind Khalid Shaykh Muhammad, have been captured or killed.
- There is a broad and growing global consensus that the deliberate killing of innocents is never justified by any calling or cause.
- Many nations have rallied to fight terrorism, with unprecedented cooperation on law enforcement, intelligence, military, and diplomatic activity.
- Numerous countries that were part of the problem before September 11 are now increasingly becoming part of the solution — and this transformation has occurred without destabilizing friendly regimes in key regions.
- The Administration has worked with Congress to adopt and implement key reforms like the Patriot Act, which promote our security while also protecting our fundamental liberties.

The enemy is determined, however, and we face some old and new challenges:

- Terrorist networks today are more dispersed and less centralized. They are more reliant on smaller cells inspired by a common ideology and less directed by a central command structure.
- While the United States Government and its allies have thwarted many attacks, we have not been able to stop them all. The terrorists have struck in many places, including Afghanistan, Egypt, Indonesia, Iraq, Israel, Jordan, Morocco, Pakistan, Russia, Saudi Arabia, Spain, and the United Kingdom. And they continue to seek WMD in order to inflict even more catastrophic attacks on us and our friends and allies.

- The ongoing fight in Iraq has been twisted by terrorist propaganda as a rallying cry.
- Some states, such as Syria and Iran, continue to harbor terrorists at home and sponsor terrorist activity abroad.

C. The Way Ahead

From the beginning, the War on Terror has been both a battle of arms and a battle of ideas — a fight against the terrorists and against their murderous ideology. In the short run, the fight involves using military force and other instruments of national power to kill or capture the terrorists, deny them safe haven or control of any nation; prevent them from gaining access to WMD; and cut off their sources of support. In the long run, winning the war on terror means winning the battle of ideas, for it is ideas that can turn the disenchanted into murderers willing to kill innocent victims.

While the War on Terror is a battle of ideas, it is not a battle of religions. The transnational terrorists confronting us today exploit the proud religion of Islam to serve a violent political vision: the establishment, by terrorism and subversion, of a totalitarian empire that denies all political and religious freedom. These terrorists distort the idea of jihad into a call for murder against those they regard as apostates or unbelievers — including Christians, Jews, Hindus, other religious traditions, and all Muslims who disagree with them. Indeed, most of the terrorist attacks since September 11 have occurred in Muslim countries — and most of the victims have been Muslims.

To wage this battle of ideas effectively, we must be clear-eyed about what does and does not give rise to terrorism:

- Terrorism is not the inevitable by-product of poverty. Many of the September 11 hijackers were from middle-class backgrounds, and many terrorist leaders, like bin Laden, are from privileged upbringings.
- Terrorism is not simply a result of hostility to U.S. policy in Iraq. The United States was attacked on September 11 and earlier, well before we toppled the Saddam Hussein regime. Moreover, countries that stayed out of the Iraq war have not been spared from terror attack.
- Terrorism is not simply a result of Israeli-Palestinian issues. Al-Qaida plotting for the September 11 attacks began in the 1990s, during an active period in the peace process.
- Terrorism is not simply a response to our efforts to prevent terror attacks. The al-Qaida network targeted the United States long before the United States targeted al-Qaida. Indeed, the terrorists are emboldened more by perceptions of weakness than by demonstrations of resolve. Terrorists lure recruits by telling them that we are decadent and easily intimidated and will retreat if attacked.

The terrorism we confront today springs from:

- Political alienation. Transnational terrorists are recruited from people who have no voice in their own government and see no legitimate way to promote change in their own country. Without a stake in the existing order, they are vulnerable to manipulation by those who advocate a perverse vision based on violence and destruction.
- Grievances that can be blamed on others. The failures the terrorists feel and see are blamed on others, and on perceived injustices from the recent or sometimes distant past. The terrorists' rhetoric keeps wounds associated with this past fresh and raw, a potent motivation for revenge and terror.
- Sub-cultures of conspiracy and misinformation. Terrorists recruit more effectively from populations whose information about the world is contaminated by falsehoods and corrupted by conspiracy theories. The distortions keep alive grievances and filter out facts that would challenge popular prejudices and self-serving propaganda.
- An ideology that justifies murder. Terrorism ultimately depends upon the appeal of an ideology that excuses or even glorifies the deliberate killing of innocents. A proud religion — the religion of Islam — has been twisted and made to serve an evil end, as in other times and places other religions have been similarly abused.

Defeating terrorism in the long run requires that each of these factors be addressed. The genius of democracy is that it provides a counter to each.

- In place of alienation, democracy offers an ownership stake in society, a chance to shape one's own future.
- In place of festering grievances, democracy offers the rule of law, the peaceful resolution of disputes, and the habits of advancing interests through compromise.
- In place of a culture of conspiracy and misinformation, democracy offers freedom of speech, independent media, and the marketplace of ideas, which can expose and discredit falsehoods, prejudices, and dishonest propaganda.
- In place of an ideology that justifies murder, democracy offers a respect for human dignity that abhors the deliberate targeting of innocent civilians.

Democracy is the opposite of terrorist tyranny, which is why the terrorists denounce it and are willing to kill the innocent to stop it. Democracy is based on empowerment, while the terrorists' ideology is based on enslavement. Democracies expand the freedom of their citizens, while the terrorists seek to impose a single set of narrow beliefs. Democracy sees individuals as equal in worth and dignity, having an inherent potential to create and to govern

themselves. The terrorists see individuals as objects to be exploited, and then to be ruled and oppressed.

Democracies are not immune to terrorism. In some democracies, some ethnic or religious groups are unable or unwilling to grasp the benefits of freedom otherwise available in the society. Such groups can evidence the same alienation and despair that the transnational terrorists exploit in undemocratic states. This accounts for the emergence in democratic societies of homegrown terrorists such as were responsible for the bombings in London in July 2005 and for the violence in some other nations. Even in these cases, the long-term solution remains deepening the reach of democracy so that all citizens enjoy its benefits.

The strategy to counter the lies behind the terrorists' ideology is to empower the very people the terrorists most want to exploit: the faithful followers of Islam. We will continue to support political reforms that empower peaceful Muslims to practice and interpret their faith. The most vital work will be done within the Islamic world itself, and Jordan, Morocco, and Indonesia have begun to make important strides in this effort. Responsible Islamic leaders need to denounce an ideology that distorts and exploits Islam for destructive ends and defiles a proud religion.

Many of the Muslim faith are already making this commitment at great personal risk. They realize they are a target of this ideology of terror. Everywhere we have joined in the fight against terrorism, Muslim allies have stood beside us, becoming partners in this vital cause. Pakistan and Saudi Arabia have launched effective efforts to capture or kill the leadership of the al-Qaida network. Afghan troops are in combat against Taliban remnants. Iraqi soldiers are sacrificing to defeat al-Qaida in their own country. These brave citizens know the stakes — the survival of their own liberty, the future of their own region, the justice and humanity of their own traditions — and the United States is proud to stand beside them.

The advance of freedom and human dignity through democracy is the long-term solution to the transnational terrorism of today. To create the space and time for that long-term solution to take root, there are four steps we will take in the short term.

- **Prevent attacks by terrorist networks before they occur**. A government has no higher obligation than to protect the lives and livelihoods of its citizens. The hard core of the terrorists cannot be deterred or reformed; they must be tracked down, killed, or captured. They must be cut off from the network of individuals and institutions on which they depend for support. That network must in turn be deterred, disrupted, and disabled by using a broad range of tools.
- **Deny WMD to rogue states and to terrorist allies who would use them without hesitation**. Terrorists have a perverse moral code that glorifies deliberately targeting innocent civilians. Terrorists try to

inflict as many casualties as possible and seek WMD to this end. Denying terrorists WMD will require new tools and new international approaches. We are working with partner nations to improve security at vulnerable nuclear sites worldwide and bolster the ability of states to detect, disrupt, and respond to terrorist activity involving WMD.

- **Deny terrorist groups the support and sanctuary of rogue states**. The United States and its allies in the War on Terror make no distinction between those who commit acts of terror and those who support and harbor them because they are equally guilty of murder. Any government that chooses to be an ally of terror, such as Syria or Iran, has chosen to be an enemy of freedom, justice, and peace. The world must hold those regimes to account.
- **Deny the terrorists control of any nation that they would use as a base and launching pad for terror**. The terrorists' goal is to overthrow a rising democracy; claim a strategic country as a haven for terror; destabilize the Middle East; and strike America and other free nations with ever-increasing violence. This we can never allow. This is why success in Afghanistan and Iraq is vital, and why we must prevent terrorists from exploiting ungoverned areas.

America will lead in this fight, and we will continue to partner with allies and will recruit new friends to join the battle.

Afghanistan and Iraq: The Front Lines in the War on Terror

Winning the War on Terror requires winning the battles in Afghanistan and Iraq.

In Afghanistan, the successes already won must be consolidated. A few years ago, Afghanistan was condemned to a pre-modern nightmare. Now it has held two successful free elections and is a staunch ally in the war on terror. Much work remains, however, and the Afghan people deserve the support of the United States and the entire international community.

The terrorists today see Iraq as the central front of their fight against the United States. They want to defeat America in Iraq and force us to abandon our allies before a stable democratic government has been established that can provide for its own security. The terrorists believe they would then have proven that the United States is a waning power and an unreliable friend. In the chaos of a broken Iraq the terrorists believe they would be able to establish a safe haven like they had in Afghanistan, only this time in the heart of a geopolitically vital region. Surrendering to the .

terrorists would likewise hand them a powerful recruiting tool: the perception that they are the vanguard of history

When the Iraqi Government, supported by the Coalition, defeats the terrorists, terrorism will be dealt a critical blow. We will have broken one of al-Qaida's most formidable factions — the network headed by Zarqawi — and denied him the safe haven he seeks in Iraq. And the success of democracy in Iraq will be a launching pad for freedom's success throughout a region that for decades has been a source of instability and stagnation.

The Administration has explained in some detail the strategy for helping the Iraqi people defeat the terrorists and neutralize the insurgency in Iraq. This requires supporting the Iraqi people in integrating activity along three broad tracks:

Political: Work with Iraqis to:

- **Isolate** hardened enemy elements who are unwilling to accept a peaceful political process;
- **Engage** those outside the political process who are willing to turn away from violence and invite them into that process; and
- **Build** stable, pluralistic, and effective national institutions that can protect the interests of all Iraqis.

Security: Work with Iraqi Security Forces to:

- **Clear** areas of enemy control by remaining on the offensive, killing and capturing enemy fighters, and denying them safe haven;
- **Hold** areas freed from enemy control with an adequate Iraqi security force presence that ensures these areas remain under the control of a peaceful Iraqi Government; and
- **Build** Iraqi Security Forces and the capacity of local institutions to deliver services, advance the rule of law, and nurture civil society.

Economic: Work with the Iraqi Government to:

- **Restore** Iraq's neglected infrastructure so that Iraqis can meet increasing demand and the needs of a growing economy;
- **Reform** Iraq's economy so that it can be self-sustaining based on market principles; and
- **Build** the capacity of Iraqi institutions to maintain their infrastructure, rejoin the international economic community, and improve the general welfare and prosperity of all Iraqis.

IV. Work with Others to Defuse Regional Conflicts

A. Summary of National Security Strategy 2002

Regional conflicts are a bitter legacy from previous decades that continue to affect our national security interests today. Regional conflicts do not stay isolated for long and often spread or devolve into humanitarian tragedy or anarchy. Outside parties can exploit them to further other ends, much as al-Qaida exploited the civil war in Afghanistan. This means that even if the United States does not have a direct stake in a particular conflict, our interests are likely to be affected over time. Outsiders generally cannot impose solutions on parties that are not ready to embrace them, but outsiders can sometimes help create the conditions under which the parties themselves can take effective action.

B. Current Context: Successes and Challenges

The world has seen remarkable progress on a number of the most difficult regional conflicts that destroyed millions of lives over decades.

- In Sudan, the United States led international negotiations that peacefully resolved the 20-year conflict between the Government of Sudan and the Sudanese Peoples Liberation Movement.
- In Liberia, the United States led international efforts to restore peace and bolster stability after vicious internal conflict.
- Israeli forces have withdrawn from the Gaza Strip and the northern West Bank, creating the prospect for transforming Israeli-Palestinian relations and underscoring the need for the Palestinian Authority to stand up an effective, responsible government.
- Relations between India and Pakistan have improved, with an exchange of high-level visits and a new spirit of cooperation in the dispute over Kashmir — a cooperation made more tangible by humanitarian actions undertaken following a destructive earthquake.
- The cooperative approach to the relief effort following the tsunami that hit Indonesia resulted in political shifts that helped make possible a peaceful settlement in the bitter separatist conflict in Aceh.
- In Northern Ireland, the implementation of key parts of the Good Friday Agreement, including the decommissioning of weapons, marked a substantial milestone in ending that long-standing civil conflict.

Numerous remaining regional challenges demand the world's attention:

- In Darfur, the people of an impoverished region are the victims of genocide arising from a civil war that pits a murderous militia, backed by the Sudanese Government, against a collection of rebel groups.

- In Colombia, a democratic ally is fighting the persistent assaults of Marxist terrorists and drug-traffickers.
- In Venezuela, a demagogue awash in oil money is undermining democracy and seeking to destabilize the region.
- In Cuba, an anti-American dictator continues to oppress his people and seeks to subvert freedom in the region.
- In Uganda, a barbaric rebel cult — the Lord's Resistance Army — is exploiting a regional conflict and terrorizing a vulnerable population.
- In Ethiopia and Eritrea, a festering border dispute threatens to erupt yet again into open war.
- In Nepal, a vicious Maoist insurgency continues to terrorize the population while the government retreats from democracy.

C. The Way Ahead

Regional conflicts can arise from a wide variety of causes, including poor governance, external aggression, competing claims, internal revolt, tribal rivalries, and ethnic or religious hatreds. If left unaddressed, however, these different causes lead to the same ends: failed states, humanitarian disasters, and ungoverned areas that can become safe havens for terrorists.

The Administration's strategy for addressing regional conflicts includes three levels of engagement: conflict prevention and resolution; conflict intervention; and post-conflict stabilization and reconstruction.

Effective international cooperation on these efforts is dependent on capable partners. To this end, Congress has enacted new authorities that will permit the United States to train and equip our foreign partners in a more timely and effective manner. Working with Congress, we will continue to pursue foreign assistance reforms that allow the President to draw on the skills of agencies across the United States Government.

1. Conflict Prevention and Resolution

The most effective long-term measure for conflict prevention and resolution is the promotion of democracy. Effective democracies may still have disputes, but they are equipped to resolve their differences peacefully, either bilaterally or by working with other regional states or international institutions.

In the short term, however, a timely offer by free nations of "good offices" or outside assistance can sometimes prevent conflict or help resolve conflict once started. Such early measures can prevent problems from becoming crises and crises from becoming wars. The United States is ready to play this role when appropriate. Even with outside help, however, there is no substitute for bold and effective local leadership.

Progress in the short term may also depend upon the stances of key regional actors. The most effective way to address a problem within one

country may be by addressing the wider regional context. This regional approach has particular application to Israeli-Palestinian issues, the conflicts in the Great Lakes region of Africa, and the conflict within Nepal.

2. Conflict Intervention

Some conflicts pose such a grave threat to our broader interests and values that conflict intervention may be needed to restore peace and stability. Recent experience has underscored that the international community does not have enough high-quality military forces trained and capable of performing these peace operations. The Administration has recognized this need and is working with the North Atlantic Treaty Organization (NATO) to improve the capacity of states to intervene in conflict situations. We launched the Global Peace Operations Initiative at the 2004 G-8 Summit to train peacekeepers for duty in Africa. We are also supporting United Nations (U.N.) reform to improve its ability to carry out peacekeeping missions with enhanced accountability, oversight, and results-based management practices.

3. Post-Conflict Stabilization and Reconstruction

Once peace has been restored, the hard work of post-conflict stabilization and reconstruction must begin. Military involvement may be necessary to stop a bloody conflict, but peace and stability will last only if follow-on efforts to restore order and rebuild are successful. The world has found through bitter experience that success often depends on the early establishment of strong local institutions such as effective police forces and a functioning justice and penal system. This governance capacity is critical to establishing the rule of law and a free market economy, which provide long-term stability and prosperity.

To develop these capabilities, the Administration established a new office in the Department of State, the Office of the Coordinator for Reconstruction and Stabilization, to plan and execute civilian stabilization and reconstruction efforts. The office draws on all agencies of the government and integrates its activities with our military's efforts. The office will also coordinate United States Government efforts with other governments building similar capabilities (such as the United Kingdom, Canada, the EU, and others), as well as with new international efforts such as the U.N. Peacebuilding Commission.

4. Genocide

Patient efforts to end conflicts should not be mistaken for tolerance of the intolerable. Genocide is the intent to destroy in whole or in part a national, ethnic, racial, or religious group. The world needs to start honoring a principle that many believe has lost its force in parts of the international community in recent years: genocide must not be tolerated.

It is a moral imperative that states take action to prevent and punish genocide. History teaches that sometimes other states will not act unless America does its part. We must refine United States Government efforts — economic, diplomatic, and law-enforcement — so that they target those individuals responsible for genocide and not the innocent citizens they rule. Where perpetrators of mass killing defy all attempts at peaceful intervention, armed intervention may be required, preferably by the forces of several nations working together under appropriate regional or international auspices.

We must not allow the legal debate over the technical definition of "genocide" to excuse inaction. The world must act in cases of mass atrocities and mass killing that will eventually lead to genocide even if the local parties are not prepared for peace.

V. Prevent Our Enemies from Threatening Us, Our Allies, and Our Friends with Weapons of Mass Destruction

A. Summary of National Security Strategy 2002

The security environment confronting the United States today is radically different from what we have faced before. Yet the first duty of the United States Government remains what it always has been: to protect the American people and American interests. It is an enduring American principle that this duty obligates the government to anticipate and counter threats, using all elements of national power, before the threats can do grave damage. The greater the threat, the greater is the risk of inaction — and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack. There are few greater threats than a terrorist attack with WMD.

To forestall or prevent such hostile acts by our adversaries, the United States will, if necessary, act preemptively in exercising our inherent right of self-defense. The United States will not resort to force in all cases to preempt emerging threats. Our preference is that nonmilitary actions succeed. And no country should ever use preemption as a pretext for aggression.

Countering proliferation of WMD requires a comprehensive strategy involving strengthened nonproliferation efforts to deny these weapons of terror and related expertise to those seeking them; proactive counterproliferation efforts to defend against and defeat WMD and missile threats before they are unleashed; and improved protection to mitigate the consequences of WMD use. We aim to convince our adversaries that they cannot achieve their goals with WMD, and thus deter and dissuade them from attempting to use or even acquire these weapons in the first place.

B. Current Context: Successes and Challenges

We have worked hard to protect our citizens and our security. The United States has worked extensively with the international community and key partners to achieve common objectives.

- The United States has begun fielding ballistic missile defenses to deter and protect the United States from missile attacks by rogue states armed with WMD. The fielding of such missile defenses was made possible by the United States' withdrawal from the 1972 Anti-Ballistic Missile Treaty, which was done in accordance with the treaty's provisions.
- In May 2003, the Administration launched the Proliferation Security Initiative (PSI), a global effort that aims to stop shipments of WMD, their delivery systems, and related material. More than 70 countries have expressed support for this initiative, and it has enjoyed several successes in impeding WMD trafficking.
- United States leadership in extensive law enforcement and intelligence cooperation involving several countries led to the roll-up of the A.Q. Khan nuclear network.
- Libya voluntarily agreed to eliminate its WMD programs shortly after a PSI interdiction of a shipment of nuclear-related material from the A.Q. Khan network to Libya.
- The United States led in securing passage in April 2004 of United Nations Security Council (UNSC) Resolution 1540, requiring nations to criminalize WMD proliferation and institute effective export and financial controls.
- We have led the effort to strengthen the ability of the International Atomic Energy Agency (IAEA) to detect and respond to nuclear proliferation.
- The Administration has established a new comprehensive framework, *Biodefense for the 21st Century*, incorporating innovative initiatives to protect the United States against bioterrorism.

Nevertheless, serious challenges remain:

- Iran has violated its Non-Proliferation Treaty safeguards obligations and refuses to provide objective guarantees that its nuclear program is solely for peaceful purposes.
- The DPRK continues to destabilize its region and defy the international community, now boasting a small nuclear arsenal and an illicit nuclear program in violation of its international obligations.

- Terrorists, including those associated with the al-Qaida network, continue to pursue WMD.
- Some of the world's supply of weapons-grade fissile material — the necessary ingredient for making nuclear weapons — is not properly protected.
- Advances in biotechnology provide greater opportunities for state and non-state actors to obtain dangerous pathogens and equipment.

C. The Way Ahead

We are committed to keeping the world's most dangerous weapons out of the hands of the world's most dangerous people.

1. Nuclear Proliferation

The proliferation of nuclear weapons poses the greatest threat to our national security. Nuclear weapons are unique in their capacity to inflict instant loss of life on a massive scale. For this reason, nuclear weapons hold special appeal to rogue states and terrorists.

The best way to block aspiring nuclear states or nuclear terrorists is to deny them access to the essential ingredient of fissile material. It is much harder to deny states or terrorists other key components, for nuclear weapons represent a 60-year old technology and the knowledge is widespread. Therefore, our strategy focuses on controlling fissile material with two priority objectives: first, to keep states from acquiring the capability to produce fissile material suitable for making nuclear weapons; and second, to deter, interdict, or prevent any transfer of that material from states that have this capability to rogue states or to terrorists.

The first objective requires closing a loophole in the Non-Proliferation Treaty that permits regimes to produce fissile material that can be used to make nuclear weapons under cover of a civilian nuclear power program. To close this loophole, we have proposed that the world's leading nuclear exporters create a safe, orderly system that spreads nuclear energy without spreading nuclear weapons. Under this system, all states would have reliable access at reasonable cost to fuel for civilian nuclear power reactors. In return, those states would remain transparent and renounce the enrichment and reprocessing capabilities that can produce fissile material for nuclear weapons. In this way, enrichment and reprocessing will not be necessary for nations seeking to harness nuclear energy for strictly peaceful purposes.

The Administration has worked with the international community in confronting nuclear proliferation.

We may face no greater challenge from a single country than from Iran. For almost 20 years, the Iranian regime hid many of its key nuclear efforts from the international community. Yet the regime continues to claim that

it does not seek to develop nuclear weapons. The Iranian regime's true intentions are clearly revealed by the regime's refusal to negotiate in good faith; its refusal to come into compliance with its international obligations by providing the IAEA access to nuclear sites and resolving troubling questions; and the aggressive statements of its President calling for Israel to "be wiped off the face of the Earth." The United States has joined with our EU partners and Russia to pressure Iran to meet its international obligations and provide objective guarantees that its nuclear program is only for peaceful purposes. This diplomatic effort must succeed if confrontation is to be avoided.

As important as are these nuclear issues, the United States has broader concerns regarding Iran. The Iranian regime sponsors terrorism; threatens Israel; seeks to thwart Middle East peace; disrupts democracy in Iraq; and denies the aspirations of its people for freedom. The nuclear issue and our other concerns can ultimately be resolved only if the Iranian regime makes the strategic decision to change these policies, open up its political system, and afford freedom to its people. This is the ultimate goal of U.S. policy. In the interim, we will continue to take all necessary measures to protect our national and economic security against the adverse effects of their bad conduct. The problems lie with the illicit behavior and dangerous ambition of the Iranian regime, not the legitimate aspirations and interests of the Iranian people. Our strategy is to block the threats posed by the regime while expanding our engagement and outreach to the people the regime is oppressing.

The North Korean regime also poses a serious nuclear proliferation challenge. It presents a long and bleak record of duplicity and bad-faith negotiations. In the past, the regime has attempted to split the United States from its allies. This time, the United States has successfully forged a consensus among key regional partners — China, Japan, Russia, and the Republic of Korea (ROK) — that the DPRK must give up all of its existing nuclear programs. Regional cooperation offers the best hope for a peaceful, diplomatic resolution of this problem. In a joint statement signed on September 19, 2005, in the Six-Party Talks among these participants, the DPRK agreed to abandon its nuclear weapons and all existing nuclear programs. The joint statement also declared that the relevant parties would negotiate a permanent peace for the Korean peninsula and explore ways to promote security cooperation in Asia. Along with our partners in the Six-Party Talks, the United States will continue to press the DPRK to implement these commitments.

The United States has broader concerns regarding the DPRK as well. The DPRK counterfeits our currency; traffics in narcotics and engages in other illicit activities; threatens the ROK with its army and its neighbors with its missiles; and brutalizes and starves its people. The DPRK regime needs to change these policies, open up its political system, and afford freedom to its people. In the interim, we will continue to take all necessary measures to

protect our national and economic security against the adverse effects of their bad conduct.

The second nuclear proliferation objective is to keep fissile material out of the hands of rogue states and terrorists. To do this we must address the danger posed by inadequately safeguarded nuclear and radiological materials worldwide. The Administration is leading a global effort to reduce and secure such materials as quickly as possible through several initiatives including the Global Threat Reduction Initiative (GTRI). The GTRI locates, tracks, and reduces existing stockpiles of nuclear material. This new initiative also discourages trafficking in nuclear material by emplacing detection equipment at key transport nodes.

Building on the success of the PSI, the United States is also leading international efforts to shut down WMD trafficking by targeting key maritime and air transportation and transshipment routes, and by cutting off proliferators from financial resources that support their activities.

2. Biological Weapons

Biological weapons also pose a grave WMD threat because of the risks of contagion that would spread disease across large populations and around the globe. Unlike nuclear weapons, biological weapons do not require hard-to-acquire infrastructure or materials. This makes the challenge of controlling their spread even greater.

Countering the spread of biological weapons requires a strategy focused on improving our capacity to detect and respond to biological attacks, securing dangerous pathogens, and limiting the spread of materials useful for biological weapons. The United States is working with partner nations and institutions to strengthen global biosurveillance capabilities for early detection of suspicious outbreaks of disease. We have launched new initiatives at home to modernize our public health infrastructure and to encourage industry to speed the development of new classes of vaccines and medical countermeasures. This will also enhance our Nation's ability to respond to pandemic public health threats, such as avian influenza.

3. Chemical Weapons

Chemical weapons are a serious proliferation concern and are actively sought by terrorists, including al-Qaida. Much like biological weapons, the threat from chemical weapons increases with advances in technology, improvements in agent development, and ease in acquisition of materials and equipment.

To deter and defend against such threats, we work to identify and disrupt terrorist networks that seek chemical weapons capabilities, and seek to deny them access to materials needed to make these weapons. We are improving our detection and other chemical defense capabilities at home and abroad, including

ensuring that U.S. military forces and emergency responders are trained and equipped to manage the consequences of a chemical weapons attack.

4. The Need for Action

The new strategic environment requires new approaches to deterrence and defense. Our deterrence strategy no longer rests primarily on the grim premise of inflicting devastating consequences on potential foes. Both offenses and defenses are necessary to deter state and non-state actors, through denial of the objectives of their attacks and, if necessary, responding with overwhelming force.

Safe, credible, and reliable nuclear forces continue to play a critical role. We are strengthening deterrence by developing a New Triad composed of offensive strike systems (both nuclear and improved conventional capabilities); active and passive defenses, including missile defenses; and a responsive infrastructure, all bound together by enhanced command and control, planning, and intelligence systems. These capabilities will better deter some of the new threats we face, while also bolstering our security commitments to allies. Such security commitments have played a crucial role in convincing some countries to forgo their own nuclear weapons programs, thereby aiding our nonproliferation objectives.

Deterring potential foes and assuring friends and allies, however, is only part of a broader approach. Meeting WMD proliferation challenges also requires effective international action — and the international community is most engaged in such action when the United States leads.

Taking action need not involve military force. Our strong preference and common practice is to address proliferation concerns through international diplomacy, in concert with key allies and regional partners. If necessary, however, under long-standing principles of self defense, we do not rule out the use of force before attacks occur, even if uncertainty remains as to the time and place of the enemy's attack. When the consequences of an attack with WMD are potentially so devastating, we cannot afford to stand idly by as grave dangers materialize. This is the principle and logic of preemption. The place of preemption in our national security strategy remains the same. We will always proceed deliberately, weighing the consequences of our actions. The reasons for our actions will be clear, the force measured, and the cause just.

Iraq and Weapons of Mass Destruction

This Administration inherited an Iraq threat that was unresolved. In early 2001, the international support for U.N. sanctions and continued limits on the Iraqi regime's weapons-related activity was eroding, and key UNSC members were asking that they be lifted.

For America, the September 11 attacks underscored the danger of allowing threats to linger unresolved. Saddam Hussein's continued defiance of 16 UNSC resolutions over 12 years, combined with his record of

invading neighboring countries, supporting terrorists, tyrannizing his own people, and using chemical weapons, presented a threat we could no longer ignore.

The UNSC unanimously passed Resolution 1441 on November 8, 2002, calling for full and immediate compliance by the Iraqi regime with its disarmament obligations. Once again, Saddam defied the international community. According to the Iraq Survey Group, the team of inspectors that went into Iraq after Saddam Hussein was toppled and whose report provides the fullest accounting of the Iraqi regime's illicit activities:

Saddam continued to see the utility of WMD. He explained that he purposely gave an ambiguous impression about possession as a deterrent to Iran. He gave explicit direction to maintain the intellectual capabilities. As U.N. sanctions eroded there was a concomitant expansion of activities that could support full WMD reactivation. He directed that ballistic missile work continue that would support long-range missile development. Virtually no senior Iraqi believed that Saddam had forsaken WMD forever. Evidence suggests that, as resources became available and the constraints of sanctions decayed, there was a direct expansion of activity that would have the effect of supporting future WMD reconstitution.

With the elimination of Saddam's regime, this threat has been addressed, once and for all.

The Iraq Survey Group also found that pre-war intelligence estimates of Iraqi WMD stockpiles were wrong — a conclusion that has been confirmed by a bipartisan commission and congressional investigations. We must learn from this experience if we are to counter successfully the very real threat of proliferation.

First, our intelligence must improve. The President and the Congress have taken steps to reorganize and strengthen the U.S. intelligence community. A single, accountable leader of the intelligence community with authorities to match his responsibilities, and increased sharing of information and increased resources, are helping realize this objective.

Second, there will always be some uncertainty about the status of hidden programs. Since proliferators are often brutal regimes that go to great lengths to conceal their activities. Indeed, prior to the 1991 Gulf War, many intelligence analysts underestimated the WMD threat posed by the Iraqi regime. After that conflict, they were surprised to learn how far Iraq had progressed along various pathways to try to produce fissile material.

Third, Saddam's strategy of bluff, denial, and deception is a dangerous game that dictators play at their peril. The world offered Saddam a clear choice: effect full and immediate compliance with his disarmament obligations or face serious consequences. Saddam chose the latter course and is now facing judgment in an Iraqi court. It was Saddam's reckless behavior

that demanded the world's attention, and it was his refusal to remove the ambiguity that he created that forced the United States and its allies to act. We have no doubt that the world is a better place for the removal of this dangerous and unpredictable tyrant, and we have no doubt that the world is better off if tyrants know that they pursue WMD at their own peril.

VI. Ignite a New Era of Global Economic Growth through Free Markets and Free Trade

A. Summary of National Security Strategy 2002

Promoting free and fair trade has long been a bedrock tenet of American foreign policy. Greater economic freedom is ultimately inseparable from political liberty. Economic freedom empowers individuals, and empowered individuals increasingly demand greater political freedom. Greater economic freedom also leads to greater economic opportunity and prosperity for everyone. History has judged the market economy as the single most effective economic system and the greatest antidote to poverty. To expand economic liberty and prosperity, the United States promotes free and fair trade, open markets, a stable financial system, the integration of the global economy, and secure, clean energy development.

B. Current Context: Successes and Challenges

The global economy is more open and free, and many people around the world have seen their lives improve as prosperity and economic integration have increased. The Administration has accomplished much of the economic freedom agenda it set out in 2002:

Seizing the Global Initiative. We have worked to open markets and integrate the global economy through launching the Doha Development Agenda negotiations of the World Trade Organization (WTO). The United States put forward bold and historic proposals to reform global agricultural trade, to eliminate farm export subsidies and reduce trade-distorting support programs, to eliminate all tariffs on consumer and industrial goods, and to open global services markets. When negotiations stalled in 2003, the United States took the initiative to put Doha back on track, culminating in a successful framework agreement reached in Geneva in 2004. As talks proceed, the United States continues to lead the world in advancing bold proposals for economic freedom through open markets. We also have led the way in helping the accessions of new WTO members such as Armenia, Cambodia, Macedonia, and Saudi Arabia.

Pressing Regional and Bilateral Trade Initiatives. We have used FTAs to open markets, support economic reform and the rule of law, and create new opportunities for American farmers and workers. Since 2001, we have:

- Implemented or completed negotiations for FTAs with 14 countries on 5 continents, and are negotiating agreements with 11 additional countries;
- Partnered with Congress to pass the Central America Free Trade Agreement — Dominican Republic (CAFTA-DR), long sought by the leaders of El Salvador, Honduras, Guatemala, Nicaragua, Costa Rica, and Dominican Republic;
- Called in 2003 for the creation of a Middle East Free Trade Area (MEFTA) by 2013 to bring the Middle East into an expanding circle of opportunity;
- Negotiated FTAs with Bahrain, Jordan, Morocco, and Oman to provide a foundation for the MEFTA initiative;
- Launched in 2002 the Enterprise for ASEAN Initiative, which led to the completion of a free trade agreement with Singapore, and the launch of negotiations with Thailand and Malaysia;
- Concluded an FTA with Australia, one of America's strongest allies in the Asia-Pacific region and a major trading partner of the United States; and
- Continued to promote the opportunities of increased trade to sub-Saharan Africa through the African Growth and Opportunity Act (AGOA), and extended opportunity to many other developing countries through the Generalized System of Preferences.

Pressing for Open Markets, Financial Stability, and Deeper Integration of the World Economy. We have partnered with Europe, Japan, and other major economies to promote structural reforms that encourage growth, stability, and opportunity across the globe. The United States has:

- Gained agreement in the G-7 on the Agenda for Growth, which commits member states to take concrete steps to reform domestic economic systems;
- Worked with other nations that serve as regional and global engines of growth — such as India, China, the ROK, Brazil, and Russia — on reforms to open markets and ensure financial stability;
- Urged China to move to a market-based, flexible exchange rate regime — a step that would help both China and the global economy; and
- Pressed for reform of the International Financial Institutions to focus on results, fostering good governance and sound policies, and freeing poor countries from unpayable debts.

Enhancing Energy Security and Clean Development. The Administration has worked with trading partners and energy producers to expand the types and sources of energy, to open markets and strengthen the rule of law, and to foster private investment that can help develop the energy needed to meet global demand. In addition, we have:

- Worked with industrialized and emerging nations on hydrogen, clean coal, and advanced nuclear technologies; and
- Joined with Australia, China, India, Japan, and the ROK in forming the Asia-Pacific Partnership for Clean Development and Climate to accelerate deployment of clean technologies to enhance energy security, reduce poverty, and reduce pollution.

Several challenges remain:

- Protectionist impulses in many countries put at risk the benefits of open markets and impede the expansion of free and fair trade and economic growth.
- Nations that lack the rule of law are prone to corruption, lack of transparency, and poor governance. These nations frustrate the economic aspirations of their people by failing to promote entrepreneurship, protect intellectual property, or allow their citizens access to vital investment capital.
- Many countries are too dependent upon foreign oil, which is often imported from unstable parts of the world.
- Economic integration spreads wealth across the globe, but also makes local economies more subject to global market conditions.
- Some governments restrict the free flow of capital, subverting the vital role that wise investment can play in promoting economic growth. This denies investments, economic opportunity, and new jobs to the people who need them most.

C. The Way Ahead

Economic freedom is a moral imperative. The liberty to create and build or to buy, sell, and own property is fundamental to human nature and foundational to a free society. Economic freedom also reinforces political freedom. It creates diversified centers of power and authority that limit the reach of government. It expands the free flow of ideas; with increased trade and foreign investment comes exposure to new ways of thinking and living which give citizens more control over their own lives.

To continue extending liberty and prosperity, and to meet the challenges that remain, our strategy going forward involves:

1. Opening Markets and Integrating Developing Countries

While most of the world affirms in principle the appeal of economic liberty, in practice too many nations hold fast to the false comforts of subsidies and trade barriers. Such distortions of the market stifle growth in developed countries, and slow the escape from poverty in developing countries. Against

these short-sighted impulses, the United States promotes the enduring vision of a global economy that welcomes all participants and encourages the voluntary exchange of goods and services based on mutual benefit, not favoritism.

We will continue to advance this agenda through the WTO and through bilateral and regional FTAs.

- The United States will seek completion of the Doha Development Agenda negotiations. A successful Doha agreement will expand opportunities for Americans and for others around the world. Trade and open markets will empower citizens in developing countries to improve their lives, while reducing the opportunities for corruption that afflict state-controlled economies.
- We will continue to work with countries such as Russia, Ukraine, Kazakhstan, and Vietnam on the market reforms needed to join the WTO. Participation in the WTO brings opportunities as well as obligations — to strengthen the rule of law and honor the intellectual property rights that sustain the modern knowledge economy, and to remove tariffs, subsidies, and other trade barriers that distort global markets and harm the world's poor.
- We will advance MEFTA by completing and bringing into force FTAs for Bahrain, Oman, and the United Arab Emirates and through other initiatives to expand open trade with and among countries in the region.
- In Africa, we are pursuing an FTA with the countries of the Southern African Customs Union: Botswana, Lesotho, Namibia, South Africa, and Swaziland.
- In Asia, we are pursuing FTAs with Thailand, the ROK, and Malaysia. We will also continue to work closely with China to ensure it honors its WTO commitments and protects intellectual property.
- In our own hemisphere, we will advance the vision of a free trade area of the Americas by building on North American Free Trade Agreement, CAFTA-DR, and the FTA with Chile. We will complete and bring into force FTAs with Colombia, Peru, Ecuador, and Panama.

2. Opening, Integrating, and Diversifying Energy Markets to Ensure Energy Independence

Most of the energy that drives the global economy comes from fossil fuels, especially petroleum. The United States is the world's third largest oil producer, but we rely on international sources to supply more than 50 percent of our needs. Only a small number of countries make major contributions to the world's oil supply.

The world's dependence on these few suppliers is neither responsible nor sustainable over the long term. The key to ensuring our energy

security is diversity in the regions from which energy resources come and in the types of energy resources on which we rely.

- The Administration will work with resource-rich countries to increase their openness, transparency, and rule of law. This will promote effective democratic governance and attract the investment essential to developing their resources and expanding the range of energy suppliers.
- We will build the Global Nuclear Energy Partnership to work with other nations to develop and deploy advanced nuclear recycling and reactor technologies. This initiative will help provide reliable, emission-free energy with less of the waste burden of older technologies and without making available separated plutonium that could be used by rogue states or terrorists for nuclear weapons. These new technologies will make possible a dramatic expansion of safe, clean nuclear energy to help meet the growing global energy demand.
- We will work with international partners to develop other transformational technologies such as clean coal and hydrogen. Through projects like our FutureGen initiative, we seek to turn our abundant domestic coal into emissions-free sources of electricity and hydrogen, providing our economies increased power with decreased emissions.
- On the domestic front, we are investing in zero-emission coal-fired plants; revolutionary solar and wind technologies; clean, safe nuclear energy; and cutting-edge methods of producing ethanol.

Our comprehensive energy strategy puts a priority on reducing our reliance on foreign energy sources. Diversification of energy sources also will help alleviate the "petroleum curse" — the tendency for oil revenues to foster corruption and prevent economic growth and political reform in some oil-producing states. In too many such nations, ruling elites enrich themselves while denying the people the benefits of their countries' natural wealth. In the worst cases, oil revenues fund activities that destabilize their regions or advance violent ideologies. Diversifying the suppliers within and across regions reduces opportunities for corruption and diminishes the leverage of irresponsible rulers.

3. Reforming the International Financial System to Ensure Stability and Growth

In our interconnected world, stable and open financial markets are an essential feature of a prosperous global economy. We will work to improve the stability and openness of markets by:

- **Promoting Growth-Oriented Economic Policies Worldwide**. Sound policies in the United States have helped drive much international growth. We cannot be the only source of strength, however. We will work with the world's other major economies, including the EU and Japan, to promote structural reforms that open their markets and increase productivity in their nations and across the world.
- **Encouraging Adoption of Flexible Exchange Rates and Open Markets for Financial Services**. The United States will help emerging economies make the transition to the flexible exchange rates appropriate for major economies. In particular, we will continue to urge China to meet its own commitment to a market-based, flexible exchange rate regime. We will also promote more open financial service markets, which encourage stable and sound financial practices.
- **Strengthening International Financial Institutions**. At the dawn of a previous era 6 decades ago, the United States championed the creation of the World Bank and the International Monetary Fund (IMF). These institutions were instrumental in the development of the global economy and an expansion of prosperity unprecedented in world history. They remain vital today, but must adapt to new realities:
  - For the World Bank and regional development banks, we will encourage greater emphasis on investments in the private sector. We will urge more consideration of economic freedom, governance, and measurable results in allocating funds. We will promote an increased use of grants to relieve the burden of unsustainable debt.
  - For the IMF, we will seek to refocus it on its core mission: international financial stability. This means strengthening the IMF's ability to monitor the financial system to prevent crises before they happen. If crises occur, the IMF's response must reinforce each country's responsibility for its own economic choices. A refocused IMF will strengthen market institutions and market discipline over financial decisions, helping to promote a stable and prosperous global economy. By doing so, over time markets and the private sector can supplant the need for the IMF to perform in its current role.
- **Building Local Capital Markets and the Formal Economy in the Developing World**. The first place that small businesses in developing countries turn to for resources is their own domestic markets. Unfortunately, in too many countries these resources are unavailable due to weak financial systems, a lack of property rights, and the diversion of economic activity away from the formal economy into the black market. The United States will work with these

countries to develop and strengthen local capital markets and reduce the black market. This will provide more resources to helping the public sector govern effectively and the private sector grow and prosper.

- **Creating a More Transparent, Accountable, and Secure International Financial System**. The United States has worked with public and private partners to help secure the international financial system against abuse by criminals, terrorists, money launderers, and corrupt political leaders. We will continue to use international venues like the Financial Action Task Force to ensure that this global system is transparent and protected from abuse by tainted capital. We must also develop new tools that allow us to detect, disrupt, and isolate rogue financial players and gatekeepers.

VII. Expand the Circle of Development by Opening Societies and Building the Infrastructure of Democracy

A. Summary of National Security Strategy 2002

Helping the world's poor is a strategic priority and a moral imperative. Economic development, responsible governance, and individual liberty are intimately connected. Past foreign assistance to corrupt and ineffective governments failed to help the populations in greatest need. Instead, it often impeded democratic reform and encouraged corruption. The United States must promote development programs that achieve measurable results — rewarding reforms, encouraging transparency, and improving people's lives. Led by the United States, the international community has endorsed this approach in the Monterrey Consensus.

B. Current Context: Successes and Challenges

The United States has improved the lives of millions of people and transformed the practice of development by adopting more effective policies and programs.

- **Advancing Development and Reinforcing Reform**. The Administration pioneered a revolution in development strategy with the Millennium Challenge Account program, rewarding countries that govern justly, invest in their people, and foster economic freedom. The program is based on the principle that each nation bears the responsibility for its own development. It offers governments the opportunity and the means to undertake transformational change by designing their own reform and development programs, which are then funded through the Millennium Challenge Corporation (MCC). The MCC has

approved over $1.5 billion for compacts in eight countries, is working with over a dozen other countries on compacts, and has committed many smaller grants to other partner countries.

- **Turning the Tide against AIDS and Other Infectious Diseases**. The President's Emergency Plan for AIDS Relief is an unprecedented, 5-year, $15 billion effort. Building on the success of pioneering programs in Africa, we have launched a major initiative that will prevent 7 million new infections, provide treatment to 2 million infected individuals, and care for 10 million AIDS orphans and others affected by the disease. We have launched a $1.2 billion, 5-year initiative to reduce malaria deaths by 50 percent in at least 15 targeted countries. To mobilize other nations and the private sector, the United States pioneered the creation of the Global Fund to Fight HIV/AIDS, tuberculosis, and malaria. We are the largest donor to the Fund and have already contributed over $1.4 billion.
- **Promoting Debt Sustainability and a Path toward Private Capital Markets**. The administration has sought to break the burden of debt that traps many poor countries by encouraging international financial institutions to provide grants instead of loans to low-income nations. With the United Kingdom, we spearheaded the G-8 initiative to provide 100 percent multilateral debt relief to qualifying Heavily Indebted Poor Countries. Reducing debt to sustainable levels allows countries to focus on immediate development challenges. In the long run, reducing debt also opens access to private capital markets, which foster sound policies and long-term growth.
- **Addressing Urgent Needs and Investing in People**. The United States leads the world in providing food relief. We launched the Initiative to End Hunger in Africa, using science, technology, and market incentives to increase the productivity of African farmers. We launched a 3-year, $900 million initiative to provide clean water to the poor. We have tripled basic education assistance through programs such as the Africa Education Initiative, which will train teachers and administrators, build schools, buy textbooks, and expand opportunities inside and outside the classroom.
- **Unleashing the Power of the Private Sector**. The Administration has sought to multiply the impact of our development assistance through initiatives such as the Global Development Alliance, which forges partnerships with the private sector to advance development goals, and Volunteers for Prosperity, which enlists some of our Nation's most capable professionals to serve strategically in developing nations.
- **Fighting Corruption and Promoting Transparency**. Through multilateral efforts like the G-8 Transparency Initiative and our policy of

denying corrupt foreign officials entry into the United States, we are helping ensure that organized crime and parasitic rulers do not choke off the benefits of economic assistance and growth.

We have increased our overall development assistance spending by 97 percent since 2000. In all of these efforts, the United States has sought concrete measures of success. Funding is a means, not the end. We are giving more money to help the world's poor, and giving it more effectively.

Many challenges remain, including:

- Helping millions of people in the world who continue to suffer from poverty and disease;
- Ensuring that the delivery of assistance reinforces good governance and sound economic policies; and
- Building the capacity of poor countries to take ownership of their own development strategies.

C. The Way Ahead

America's national interests and moral values drive us in the same direction: to assist the world's poor citizens and least developed nations and help integrate them into the global economy. We have accomplished many of the goals laid out in the 2002 National Security Strategy. Many of the new initiatives we launched in the last 4 years are now fully operating to help the plight of the world's least fortunate. We will persevere on this path.

Development reinforces diplomacy and defense, reducing long-term threats to our national security by helping to build stable, prosperous, and peaceful societies. Improving the way we use foreign assistance will make it more effective in strengthening responsible governments, responding to suffering, and improving people's lives.

1. Transformational Diplomacy and Effective Democracy

Transformational diplomacy means working with our many international partners to build and sustain democratic, well-governed states that will respond to the needs of their citizens and conduct themselves responsibly in the international system. Long-term development must include encouraging governments to make wise choices and assisting them in implementing those choices. We will encourage and reward good behavior rather than reinforce negative behavior. Ultimately it is the countries themselves that must decide to take the necessary steps toward development, yet we will help advance this process by creating external incentives for governments to reform themselves.

Effective economic development advances our national security by helping promote responsible sovereignty, not permanent dependency. Weak and impoverished states and ungoverned areas are not only a threat to their people and a burden on regional economies, but are also susceptible to exploitation by terrorists, tyrants, and international criminals. We will work to bolster threatened states, provide relief in times of crisis, and build capacity in developing states to increase their progress.

2. Making Foreign Assistance More Effective

The Administration has created the new position of Director of Foreign Assistance (DFA) in the State Department. The DFA will serve concurrently as Administrator of U.S. Agency for International Development (US AID), a position that will continue to be at the level of Deputy Secretary, and will have, consistent with existing legal requirements, authority over all State Department and USAID foreign assistance. This reorganization will create a more unified and rational structure that will more fully align assistance programs in State and USAID, increase the effectiveness of these programs for recipient countries, and ensure that we are being the best possible stewards of taxpayer dollars. And it will focus our foreign assistance on promoting greater ownership and responsibility on the part of host nations and their citizens.

With this new authority, the DFA/Administrator will develop a coordinated foreign assistance strategy, including 5-year, country-specific assistance strategies and annual country-specific assistance operational plans. The DFA/Administrator also will provide guidance for the assistance delivered through other entities of the United States Government, including the MCC and the Office of the Global AIDS Coordinator.

To ensure the best stewardship of our foreign assistance, the United States will:

- Distinguish among the different challenges facing different nations and address those challenges with tools appropriate for each country's stage of development;
- Encourage and reward good government and economic reform, both bilaterally and through the multilateral institutions such as international financial institutions, the G-8, and the Asia-Pacific Economic Cooperation (APEC);
- Engage the private sector to help solve development problems;
- Promote graduation from economic aid dependency with the ultimate goal of ending assistance;
- Build trade capacity to enable the poorest countries to enter into the global trade system; and
- Empower local leaders to take responsibility for their country's development.

Our assistance efforts will also highlight and build on the lessons learned from successful examples of wise development and economic policy choices, such as the ROK, Taiwan, Ireland, Poland, Slovakia, Chile, and Botswana.

VIII. Develop Agendas for Cooperative Action with the Other Main Centers of Global Power

A. Summary of National Security Strategy 2002

Relations with the most powerful countries in the world are central to our national security strategy. Our priority is pursuing American interests within cooperative relationships, particularly with our oldest and closest friends and allies. At the same time, we must seize the opportunity — unusual in historical terms — of an absence of fundamental conflict between the great powers. Another priority, therefore, is preventing the reemergence of the great power rivalries that divided the world in previous eras. New times demand new approaches, flexible enough to permit effective action even when there are reasonable differences of opinions among friends, yet strong enough to confront the challenges the world faces.

B. Current Context: Successes and Challenges

The United States has enjoyed unprecedented levels of cooperation on many of its highest national security priorities:

- The global coalition against terror has grown and deepened, with extensive cooperation and common resolve. The nations that have partnered with us in Afghanistan and Iraq have developed capabilities that can be applied to other challenges.
- We have joined with other nations around the world as well as numerous multilateral organizations to improve the capability of all nations to defend their homelands against terrorists and transnational criminals.
- We have achieved extraordinary coordination among historic rivals in pressing the DPRK to abandon its nuclear program.
- We have partnered with European allies and international institutions to pressure Iran to honor its non-proliferation commitments.
- The North Atlantic Treaty Organization (NATO) is transforming itself to meet current threats and is playing a leading role in stabilizing the Balkans and Afghanistan, as well as training the Iraqi military leadership to address its security challenges.
- We have set aside decades of mistrust and put relations with India, the world's most populous democracy, on a new and fruitful path.

At the same time, America's relations with other nations have been strong enough to withstand differences and candid exchanges of views.

- Some of our oldest and closest friends disagreed with U.S. policy in Iraq. There are ongoing and serious debates with our allies about how best to address the unique and evolving nature of the global terrorist threat.
- We have disagreed on the steps to reduce agricultural subsidies and achieve success in the WTO Doha Round of trade negotiations. We have also faced challenges in forging consensus with other major nations on the most effective measures to protect the environment.

C. The Way Ahead

The struggle against militant Islamic radicalism is the great ideological conflict of the early years of the 21st century and finds the great powers all on the same side — opposing the terrorists. This circumstance differs profoundly from the ideological struggles of the 20th century, which saw the great powers divided by ideology as well as by national interest.

The potential for great power consensus presents the United States with an extraordinary opportunity. Yet certain challenges must be overcome. Some nations differ with us on the appropriate pace of change. Other nations provide rhetorical support for free markets and effective democracy but little action on freedom's behalf.

Five principles undergird our strategy for relations with the main centers of global power.

- First, these relations must be set in their proper context. Bilateral policies that ignore regional and global realities are unlikely to succeed.
- Second, these relations must be supported by appropriate institutions, regional and global, to make cooperation more permanent, effective, and wide-reaching. Where existing institutions can be reformed to meet new challenges, we, along with our partners, must reform them. Where appropriate institutions do not exist, we, along with our partners, must create them.
- Third, we cannot pretend that our interests are unaffected by states' treatment of their own citizens. America's interest in promoting effective democracies rests on an historical fact: states that are governed well are most inclined to behave well. We will encourage all our partners to expand liberty, and to respect the rule of law and the dignity of the individual, as the surest way to advance the welfare of their people and to cement close relations with the United States.
- Fourth, while we do not seek to dictate to other states the choices they make, we do seek to influence the calculations on which these

choices are based. We also must hedge appropriately in case states choose unwisely.

- Fifth, we must be prepared to act alone if necessary, while recognizing that there is little of lasting consequence that we can accomplish in the world without the sustained cooperation of our allies and partners.

1. The Western Hemisphere

These principles guide our relations within our own Hemisphere, the front-line of defense of American national security. Our goal remains a hemisphere fully democratic, bound together by good will, security cooperation, and the opportunity for all our citizens to prosper. Tyrants and those who would follow them belong to a different era and must not be allowed to reverse the progress of the last two decades. Countries in the Hemisphere must be helped to the path of sustained political and economic development. The deceptive appeal of anti-free market populism must not be allowed to erode political freedoms and trap the Hemisphere's poorest in cycles of poverty. If America's nearest neighbors are not secure and stable, then Americans will be less secure.

Our strategy for the Hemisphere begins with deepening key relationships with Canada and Mexico, a foundation of shared values and cooperative policies that can be extended throughout the region. We must continue to work with our neighbors in the Hemisphere to reduce illegal immigration and promote expanded economic opportunity for marginalized populations. We must also solidify strategic relationships with regional leaders in Central and South America and the Caribbean who are deepening their commitment to democratic values. And we must continue to work with regional partners to make multilateral institutions like the OAS and the Inter-American Development Bank more effective and better able to foster concerted action to address threats that may arise to the region's stability, security, prosperity, or democratic progress. Together, these partnerships can advance our four strategic priorities for the region: bolstering security, strengthening democratic institutions, promoting prosperity, and investing in people.

2. Africa

Africa holds growing geo-strategic importance and is a high priority of this Administration. It is a place of promise and opportunity, linked to the United States by history, culture, commerce, and strategic significance. Our goal is an African continent that knows liberty, peace, stability, and increasing prosperity.

Africa's potential has in the past been held hostage by the bitter legacy of colonial misrule and bad choices by some African leaders. The United States recognizes that our security depends upon partnering with Africans

to strengthen fragile and failing states and bring ungoverned areas under the control of effective democracies.

Overcoming the challenges Africa faces requires partnership, not paternalism. Our strategy is to promote economic development and the expansion of effective, democratic governance so that African states can take the lead in addressing African challenges. Through improved governance, reduced corruption, and market reforms, African nations can lift themselves toward a better future. We are committed to working with African nations to strengthen their domestic capabilities and the regional capacity of the AU to support post-conflict transformations, consolidate democratic transitions, and improve peacekeeping and disaster responses.

3. Middle East

The Broader Middle East continues to command the world's attention. For too long, too many nations of the Middle East have suffered from a freedom deficit. Repression has fostered corruption, imbalanced or stagnant economies, political resentments, regional conflicts, and religious extremism. These maladies were all cloaked by an illusion of stability. Yet the peoples of the Middle East share the same desires as people in the rest of the world: liberty, opportunity, justice, order, and peace. These desires are now being expressed in movements for reform. The United States is committed to supporting the efforts of reformers to realize a better life for themselves and their region.

We seek a Middle East of independent states, at peace with each other, and fully participating in an open global market of goods, services, and ideas. We are seeking to build a framework that will allow Israel and the Palestinian territories to live side by side in peace and security as two democratic states. In the wider region, we will continue to support efforts for reform and freedom in traditional allies such as Egypt and Saudi Arabia. Tyrannical regimes such as Iran and Syria that oppress at home and sponsor terrorism abroad know that we will continue to stand with their people against their misrule. And in Iraq, we will continue to support the Iraqi people and their historic march from tyranny to effective democracy. We will work with the freely elected, democratic government of Iraq — our new partner in the War on Terror — to consolidate and expand freedom, and to build security and lasting stability.

4. Europe

The North Atlantic Treaty Organization remains a vital pillar of U.S. foreign policy. The Alliance has been strengthened by expanding its membership and now acts beyond its borders as an instrument for peace and stability in many parts of the world. It has also established partnerships with other key European states, including Russia, Ukraine, and others, further extending NATO's

historic transformation. The internal reform of NATO structures, capabilities, and procedures must be accelerated to ensure that NATO is able to carry out its missions effectively. The Alliance's door will also remain open to those countries that aspire for membership and meet NATO standards. Further, NATO must deepen working relationships between and across institutions, as it is doing with the EU, and as it also could do with new institutions. Such relationships offer opportunities for enhancing the distinctive strengths and missions of each organization.

Europe is home to some of our oldest and closest allies. Our cooperative relations are built on a sure foundation of shared values and interests. This foundation is expanding and deepening with the ongoing spread of effective democracies in Europe, and must expand and deepen still further if we are to reach the goal of a Europe whole, free, and at peace. These democracies are effective partners, joining with us to promote global freedom and prosperity. Just as in the special relationship that binds us to the United Kingdom, these cooperative relationships forge deeper ties between our nations.

5. Russia

The United States seeks to work closely with Russia on strategic issues of common interest and to manage issues on which we have differing interests. By reason of geography and power, Russia has great influence not only in Europe and its own immediate neighborhood, but also in many other regions of vital interest to us: the broader Middle East, South and Central Asia, and East Asia. We must encourage Russia to respect the values of freedom and democracy at home and not to impede the cause of freedom and democracy in these regions. Strengthening our relationship will depend on the policies, foreign and domestic, that Russia adopts. Recent trends regrettably point toward a diminishing commitment to democratic freedoms and institutions. We will work to try to persuade the Russian Government to move forward, not backward, along freedom's path.

Stability and prosperity in Russia's neighborhood will help deepen our relations with Russia; but that stability will remain elusive as long as this region is not governed by effective democracies. We will seek to persuade Russia's government that democratic progress in Russia and its region benefits the peoples who live there and improves relationships with us, with other Western governments, and among themselves. Conversely, efforts to prevent democratic development at home and abroad will hamper the development of Russia's relations with the United States, Europe, and its neighbors.

6. South and Central Asia

South and Central Asia is a region of great strategic importance where American interests and values are engaged as never before. India is a great

democracy, and our shared values are the foundation of our good relations. We are eager to see Pakistan move along a stable, secure, and democratic path. Our goal is for the entire region of South and Central Asia to be democratic, prosperous, and at peace.

We have made great strides in transforming America's relationship with India, a major power that shares our commitment to freedom, democracy, and rule of law. In July 2005, we signed a bold agreement — a roadmap to realize the meaningful cooperation that had eluded our two nations for decades. India now is poised to shoulder global obligations in cooperation with the United States in a way befitting a major power.

Progress with India has been achieved even as the United States has improved its strategic relationship with Pakistan. For decades, outsiders acted as if good relations with India and Pakistan were mutually exclusive. This Administration has shown that improved relations with each are possible and can help India and Pakistan make strides toward a lasting peace between themselves. America's relationship with Pakistan will not be a mirror image of our relationship with India. Together, our relations with the nations of South Asia can serve as a foundation for deeper engagement throughout Central Asia. Increasingly, Afghanistan will assume its historical role as a land-bridge between South and Central Asia, connecting these two vital regions.

Central Asia is an enduring priority for our foreign policy. The five countries of Central Asia are distinct from one another and our relations with each, while important, will differ. In the region as a whole, the elements of our larger strategy meet, and we must pursue those elements simultaneously: promoting effective democracies and the expansion of free-market reforms, diversifying global sources of energy, and enhancing security and winning the War on Terror.

7. *East Asia*

East Asia is a region of great opportunities and lingering tensions. Over the past decade, it has been a source of extraordinary economic dynamism and also of economic turbulence. Few regional economies have more effectively harnessed the engines of future prosperity: technology and globalized trade. Yet few regions have had greater difficulty overcoming the suspicions of the past.

The United States is a Pacific nation, with extensive interests throughout East and Southeast Asia. The region's stability and prosperity depend on our sustained engagement: maintaining robust partnerships supported by a forward defense posture supporting economic integration through expanded trade and investment and promoting democracy and human rights.

Forging new international initiatives and institutions can assist in the spread of freedom, prosperity, and regional security. Existing institutions like the APEC forum and the Association of Southeast Asian Nations (ASEAN) Regional Forum, can play a vital role. New arrangements, such as the U.S.-

ASEAN Enhanced Partnership, or others that are focused on problem-solving and action, like the Six-Party Talks and the PSI, can likewise bring together Asian nations to address common challenges. And Asian nations that share our values can join us in partnership to strengthen new democracies and promote democratic reforms throughout the region. This institutional framework, however, must be built upon a foundation of sound bilateral relations with key states in the region.

With Japan, the United States enjoys the closest relations in a generation. As the world's two largest economies and aid donors, acting in concert multiplies each of our strengths and magnifies our combined contributions to global progress. Our shared commitment to democracy at home offers a sure foundation for cooperation abroad.

With Australia, our alliance is global in scope. From Iraq and Afghanistan to our historic FTA, we are working jointly to ensure security, prosperity, and expanded liberty.

With the ROK, we share a vision of a prosperous, democratic, and united Korean peninsula. We also share a commitment to democracy at home and progress abroad and are translating that common vision into joint action to sustain our alliance into the 21st century.

With Southeast Asia, we celebrate the dynamism of increased economic freedom and look to further extend political freedom to all the people in the region, including those suffering under the repressive regime in Burma. In promoting greater economic and political liberty, we will work closely with our allies and key friends, including Indonesia, Malaysia, the Philippines, Singapore, and Thailand.

China encapsulates Asia's dramatic economic successes, but China's transition remains incomplete. In one generation, China has gone from poverty and isolation to growing integration into the international economic system. China once opposed global institutions; today it is a permanent member of the UNSC and the WTO. As China becomes a global player, it must act as a responsible stakeholder that fulfills its obligations and works with the United States and others to advance the international system that has enabled its success: enforcing the international rules that have helped China lift itself out of a century of economic deprivation, embracing the economic and political standards that go along with that system of rules, and contributing to international stability and security by working with the United States and other major powers.

China's leaders proclaim that they have made a decision to walk the transformative path of peaceful development. If China keeps this commitment, the United States will welcome the emergence of a China that is peaceful and prosperous and that cooperates with us to address common challenges and mutual interests. China can make an important contribution to global prosperity and ensure its own prosperity for the longer term if it

will rely more on domestic demand and less on global trade imbalances to drive its economic growth. China shares our exposure to the challenges of globalization and other transnational concerns. Mutual interests can guide our cooperation on issues such as terrorism, proliferation, and energy security. We will work to increase our cooperation to combat disease pandemics and reverse environmental degradation.

The United States encourages China to continue down the road of reform and openness, because in this way China's leaders can meet the legitimate needs and aspirations of the Chinese people for liberty, stability, and prosperity. As economic growth continues, China will face a growing demand from its own people to follow the path of East Asia's many modern democracies, adding political freedom to economic freedom. Continuing along this path will contribute to regional and international security.

China's leaders must realize, however, that they cannot stay on this peaceful path while holding on to old ways of thinking and acting that exacerbate concerns throughout the region and the world. These old ways include:

- Continuing China's military expansion in a non-transparent way;
- Expanding trade, but acting as if they can somehow "lock up" energy supplies around the world or seek to direct markets rather than opening them up — as if they can follow a mercantilism borrowed from a discredited era; and
- Supporting resource-rich countries without regard to the misrule at home or misbehavior abroad of those regimes.

China and Taiwan must also resolve their differences peacefully, without coercion and without unilateral action by either China or Taiwan.

Ultimately, China's leaders must see that they cannot let their population increasingly experience the freedoms to buy, sell, and produce, while denying them the rights to assemble, speak, and worship. Only by allowing the Chinese people to enjoy these basic freedoms and universal rights can China honor its own constitution and international commitments and reach its full potential. Our strategy seeks to encourage China to make the right strategic choices for its people, while we hedge against other possibilities.

IX. Transform America's National Security Institutions to Meet the Challenges and Opportunities of the 21st Century

A. Summary of National Security Strategy 2002

The major institutions of American national security were designed in a different era to meet different challenges. They must be transformed.

B. Current Context: Successes and Challenges

In the last four years, we have made substantial progress in transforming key national security institutions.

- The establishment of the Department of Homeland Security brought under one authority 22 federal entities with vital roles to play in protecting our Nation and preventing terrorist attacks within the United States. The Department is focused on three national security priorities: preventing terrorist attacks within the United States; reducing America's vulnerability to terrorism; and minimizing the damage and facilitating the recovery from attacks that do occur.
- In 2004, the Intelligence Community launched its most significant reorganization since the 1947 National Security Act. The centerpiece is a new position, the Director of National Intelligence, endowed with expanded budgetary, acquisition, tasking, and personnel authorities to integrate more effectively the efforts of the Community into a more unified, coordinated, and effective whole. The transformation also includes a new National Counterterrorism Center and a new National Counterproliferation Center to manage and coordinate planning and activities in those critical areas. The transformation extends to the FBI, which has augmented its intelligence capabilities and is now more fully and effectively integrated with the Intelligence Community.
- The Department of Defense has completed the 2006 Quadrennial Defense Review, which details how the Department will continue to adapt and build to meet new challenges.
  - We are pursuing a future force that will provide tailored deterrence of both state and non-state threats (including WMD employment, terrorist attacks in the physical and information domains, and opportunistic aggression) while assuring allies and dissuading potential competitors. The Department of Defense also is expanding Special Operations Forces and investing in advanced conventional capabilities to help win the long war against terrorist extremists and to help dissuade any hostile military competitor from challenging the United States, its allies, and partners.
  - The Department is transforming itself to better balance its capabilities across four categories of challenges:
    - **Traditional** challenges posed by states employing conventional armies, navies, and air forces in well-established forms of military competition.
    - **Irregular** challenges from state and non-state actors employing methods such as terrorism and insurgency to counter our tradi-

tional military advantages, or engaging in criminal activity such as piracy and drug trafficking that threaten regional security.

- **Catastrophic** challenges involving the acquisition, possession, and use of WMD by state and non-state actors; and deadly pandemics and other natural disasters that produce WMD-like effects.
- **Disruptive** challenges from state and non-state actors who employ technologies and capabilities (such as biotechnology, cyber and space operations, or directed-energy weapons) in new ways to counter military advantages the United States currently enjoys.

C. The Way Ahead

We must extend and enhance the transformation of key institutions, both domestically and abroad.

At home, we will pursue three priorities:

- ***Sustaining the transformation already under way in the Departments of Defense, Homeland Security, and Justice; the Federal Bureau of Investigation; and the Intelligence Community.***
- ***Continuing to reorient the Department of State towards transformational diplomacy,*** which promotes effective democracy and responsible sovereignty. Our diplomats must be able to step outside their traditional role to become more involved with the challenges within other societies, helping them directly, channeling assistance, and learning from their experience. This effort will include:
  - Promoting the efforts of the new Director for Foreign. Assistance/Administrator to ensure that foreign assistance is used as effectively as possible to meet our broad foreign policy objectives. This new office will align more fully the foreign assistance activities carried out by the Department of State and USAID, demonstrating that we are responsible stewards of taxpayer dollars.
  - Improving our capability to plan for and respond to post-conflict and failed-state situations. The Office of Reconstruction and Stabilization will integrate all relevant United States Government resources and assets in conducting reconstruction and stabilization operations. This effort must focus on building the security and law enforcement structures that are often the prerequisite for restoring order and ensuring success.
  - Developing a civilian reserve corps, analogous to the military reserves. The civilian reserve corps would utilize, in a flexible and timely manner, the human resources of the American people for

skills and capacities needed for international disaster relief and post-conflict reconstruction.
    - Strengthening our public diplomacy, so that we advocate the policies and values of the United States in a clear, accurate, and persuasive way to a watching and listening world. This includes actively engaging foreign audiences, expanding educational opportunities for Americans to learn about foreign languages and cultures and for foreign students and scholars to study in the United States; empowering the voices of our citizen ambassadors as well as those foreigners who share our commitment to a safer, more compassionate world; enlisting the support of the private sector; increasing our channels for dialogue with Muslim leaders and citizens; and confronting propaganda quickly, before myths and distortions have time to take root in the hearts and minds of people across the world.
- ***Improving the capacity of agencies to plan, prepare, coordinate, integrate, and execute responses*** covering the full range of crisis contingencies and long-term challenges.
    - We need to strengthen the capacity of departments and agencies to do comprehensive, results-oriented planning.
    - Agencies that traditionally played only a domestic role increasingly have a role to play in our foreign and security policies. This requires us to better integrate interagency activity both at home and abroad.

Abroad, we will work with our allies on three priorities:

- ***Promoting meaningful reform of the U.N.***, including:
    - Creating structures to ensure financial accountability and administrative and organizational efficiency.
    - Enshrining the principle that membership and participation privileges are earned by responsible behavior and by reasonable burden-sharing of security and stability challenges.
    - Enhancing the capacity of the U.N. and associated regional organizations to stand up well-trained, rapidly deployable, sustainable military and gendarme units for peace operations.
    - Ensuring that the U.N. reflects today's geopolitical realities and is not shackled by obsolete structures.
    - Reinvigorating the U.N.'s commitment, reflected in the U.N. Charter, to the promotion of democracy and human rights.
- ***Enhancing the role of democracies and democracy promotion throughout international and multilateral institutions,*** including:
    - Strengthening and institutionalizing the Community of Democracies.

  - Fostering the creation of regional democracy-based institutions in Asia, the Middle East, Africa, and elsewhere.
  - Improving the capacity of the U.N. and other multilateral institutions to advance the freedom agenda through tools like the U.N. Democracy Fund.
  - Coordinating more effectively the unique contributions of international financial institutions and regional development banks.
- ***Establishing results-oriented partnerships*** on the model of the PSI ***to meet new challenges and opportunities***. These partnerships emphasize international cooperation, not international bureaucracy. They rely on voluntary adherence rather than binding treaties. They are oriented towards action and results rather than legislation or rulemaking.

X. Engage the Opportunities and Confront the Challenges of Globalization

In recent years, the world has witnessed the growing importance of a set of opportunities and challenges that were addressed indirectly in National Security Strategy 2002: the national security implications of globalization.

Globalization presents many opportunities. Much of the world's prosperity and improved living standards in recent years derive from the expansion of global trade, investment, information, and technology. The United States has been a leader in promoting these developments, and we believe they have improved significantly the quality of life of the American people and people the world over. Other nations have embraced these opportunities and have likewise benefited. Globalization has also helped the advance of democracy by extending the marketplace of ideas and the ideals of liberty.

These new flows of trade, investment, information, and technology are transforming national security. Globalization has exposed us to new challenges and changed the way old challenges touch our interests and values, while also greatly enhancing our capacity to respond. Examples include:

- ***Public health challenges like pandemics (HIV/AIDS, avian influenza) that recognize no borders***. The risks to social order are so great that traditional public health approaches may be inadequate, necessitating new strategies and responses.
- ***Illicit trade, whether in drugs, human beings, or sex, that exploits the modern era's greater ease of transport and exchange***. Such traffic

corrodes social order; bolsters crime and corruption; undermines effective governance; facilitates the illicit transfer of WMD and advanced conventional weapons technology; and compromises traditional security and law enforcement.

- ***Environmental destruction, whether caused by human behavior or cataclysmic mega-disasters such as floods, hurricanes, earthquakes, or tsunamis***. Problems of this scope may overwhelm the capacity of local authorities to respond, and may even overtax national militaries, requiring a larger international response.

These challenges are not traditional national security concerns, such as the conflict of arms or ideologies. But if left unaddressed they can threaten national security. We have learned that:

- Preparing for and managing these challenges requires the full exercise of national power, up to and including traditional security instruments. For example, the U.S. military provided critical logistical support in the response to the Southeast Asian tsunami and the South Asian earthquake until U.N. and civilian humanitarian responders could relieve the military of these vital duties.
- Technology can help, but the key to rapid and effective response lies in achieving unity of effort across a range of agencies. For example, our response to Hurricane Katrina and Hurricane Rita underscored the need for communications systems that remain operational and integrated during times of crisis. Even more vital, however, is improved coordination within the Federal government, with state and local partners, and with the private sector.
- Existing international institutions have a role to play, but in many cases coalitions of the willing may be able to respond more quickly and creatively, at least in the short term. For example, U.S. leadership in mobilizing the Regional Core Group to respond to the tsunami of 2004 galvanized the follow-on international response.
- The response and the new partnerships it creates can sometimes serve as a catalyst for changing existing political conditions to address other problems. For example, the response to the tsunami in Southeast Asia and the earthquake in Pakistan developed new lines of communication and cooperation at a local level, which opened the door to progress in reconciling long-standing regional conflicts in Aceh and the Kashmir.

Effective democracies are better able to deal with these challenges than are repressive or poorly governed states. Pandemics require robust and fully transparent public health systems, which weak governments and those that fear freedom are unable or unwilling to provide. Yet these challenges require effective democracies to come together in innovative ways.

The United States must lead the effort to reform existing institutions and create new ones — including forging new partnerships between governmental and nongovernmental actors, and with transnational and international organizations.

To confront illicit trade, for example, the Administration launched the Proliferation Security Initiative and the APEC Secure Trade in the APEC Region Initiative, both of which focus on tangible steps governments can take to combat illegal trade.

To combat the cultivation and trafficking of narcotics, the Administration devotes over $1 billion annually to comprehensive counternarcotics efforts, working with governments, particularly in Latin America and Asia, to eradicate crops, destroy production facilities, interdict shipments, and support developing alternative livelihoods.

To confront the threat of a possible pandemic, the Administration took the lead in creating the International Partnership on Avian and Pandemic Influenza, a new global partnership of states committed to effective surveillance and preparedness that will help to detect and respond quickly to any outbreaks of the disease.

XI. Conclusion

The challenges America faces are great, yet we have enormous power and influence to address those challenges. The times require an ambitious national security strategy, yet one recognizing the limits to what even a nation as powerful as the United States can achieve by itself. Our national security strategy is idealistic about goals, and realistic about means.

There was a time when two oceans seemed to provide protection from problems in other lands, leaving America to lead by example alone. That time has long since passed. America cannot know peace, security, and prosperity by retreating from the world. America must lead by deed as well as by example. This is how we plan to lead, and this is the legacy we will leave to those who follow.

Appendix B

Homeland Security Presidential Directives 1 to 14

Homeland Security Presidential Directive-1

OCTOBER 29, 2001

Subject: Organization and Operation of the Homeland Security Council

This is the first in a series of Homeland Security Presidential Directives that shall record and communicate presidential decisions about the homeland security policies of the United States.

A. Homeland Security Council

Securing Americans from terrorist threats or attacks is a critical national security function. It requires extensive coordination across a broad spectrum of Federal, State, and local agencies to reduce the potential for terrorist attacks and to mitigate damage should such an attack occur. The Homeland Security Council (HSC) shall ensure coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies.

B. The Homeland Security Council Principals Committee

The HSC Principals Committee (HSC/PC) shall be the senior interagency forum under the HSC for homeland security issues. The HSC/PC is composed of the following members: the Secretary of the Treasury; the Secretary of Defense; the Attorney General; the Secretary of Health and Human Services; the Secretary of Transportation; the Director of the Office of Management and Budget; the Assistant to the President for Homeland Security (who serves as Chairman); the Assistant to the President and Chief of Staff; the Director of Central Intelligence; the Director of the Federal Bureau of Investigation; the Director of the Federal Emergency Management Agency; and the Assistant to the President and Chief of Staff to the Vice President. The Assistant to the President for National Security Affairs shall be invited to attend all meetings of the HSC/PC. The following people shall be invited to HSC/PC meetings when issues pertaining to their responsibilities and

expertise are discussed: the Secretary of State; the Secretary of the Interior; the Secretary of Agriculture; the Secretary of Commerce; the Secretary of Labor; the Secretary of Energy; the Secretary of Veterans Affairs; the Administrator of the Environmental Protection Agency; and the Deputy National Security Advisor for Combating Terrorism. The Counsel to the President shall be consulted regarding the agenda of HSC/PC meetings and shall attend any meeting when, in consultation with the Assistant to the President for Homeland Security, the Counsel deems it appropriate. The Deputy Director of the Office of Homeland Security shall serve as Executive Secretary of the HSC/PC. Other heads of departments and agencies and senior officials shall be invited, when appropriate.

The HSC/PC shall meet at the call of the Assistant to the President for Homeland Security, in consultation with the regular attendees of the HSC/PC. The Assistant to the President for Homeland Security shall determine the agenda, in consultation with the regular attendees, and shall ensure that all necessary papers are prepared. When global terrorism with domestic implications is on the agenda of the HSC/PC, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall perform these tasks in concert.

C. Homeland Security Council Deputies Committee

The HSC Deputies Committee (HSC/DC) shall serve as the senior sub-Cabinet interagency forum for consideration of policy issues affecting homeland security. The HSC/DC can task and review the work of the HSC interagency groups discussed below. The HSC/DC shall help ensure that issues brought before the HSC/PC or the HSC have been properly analyzed and prepared for action. The HSC/DC shall have the following as its regular members: the Deputy Secretary of the Treasury; the Deputy Secretary of Defense; the Deputy Attorney General; the Deputy Secretary of Health and Human Services; the Deputy Secretary of Transportation; the Deputy Director of the Office of Homeland Security (who serves as Chairman); the Deputy Director of Central Intelligence; the Deputy Director of the Federal Bureau of Investigation; the Deputy Director of the Federal Emergency Management Agency; the Deputy Director of the Office of Management and Budget; and the Assistant to the President and Chief of Staff to the Vice President. The Assistant to the President and Deputy National Security Advisor shall be invited to attend all meetings of the HSC/DC. The following people shall be invited to attend when issues pertaining to their responsibilities and expertise are to be discussed: the Deputy Secretary of State; the Deputy Secretary of the Interior; the Deputy Secretary of Agriculture; the Deputy Secretary of Commerce; the Deputy Secretary of Labor; the Deputy Secretary of Energy; the Deputy Secretary of Veterans Affairs; the Deputy

Administrator of the Environmental Protection Agency; the Deputy National Security Advisor for Combating Terrorism; and the Special Advisor to the President for Cyber-space Security. The Executive Secretary of the Office of Homeland Security shall serve as Executive Secretary of the HSC/DC. Other senior officials shall be invited, when appropriate.

The HSC/DC shall meet at the call of its Chairman. Any regular member of the HSC/DC may request a meeting of the HSC/DC for prompt crisis management. For all meetings, the Chairman shall determine the agenda, in consultation with the regular members, and shall ensure that necessary papers are prepared.

D. Homeland Security Council Policy Coordination Committees

HSC Policy Coordination Committees (HSC/PCCs) shall coordinate the development and implementation of homeland security policies by multiple departments and agencies throughout the Federal government, and shall coordinate those policies with State and local government. The HSC/PCCs shall be the main day-to-day fora for interagency coordination of homeland security policy. They shall provide policy analysis for consideration by the more senior committees of the HSC system and ensure timely responses to decisions made by the President. Each HSC/PCC shall include representatives from the executive departments, offices, and agencies represented in the HSC/DC.

Eleven HSC/PCCs are hereby established for the following functional areas, each to be chaired by the designated Senior Director from the Office of Homeland Security:

1. Detection, Surveillance, and Intelligence (by the Senior Director, Intelligence and Detection);
2. Plans, Training, Exercises, and Evaluation (by the Senior Director, Policy and Plans);
3. Law Enforcement and Investigation (by the Senior Director, Intelligence and Detection);
4. Weapons of Mass Destruction (WMD) Consequence Management (by the Senior Director, Response and Recovery);
5. Key Asset, Border, Territorial Waters, and Airspace Security (by the Senior Director, Protection and Prevention);
6. Domestic Transportation Security (by the Senior Director, Protection and Prevention);
7. Research and Development (by the Senior Director, Research and Development);
8. Medical and Public Health Preparedness (by the Senior Director, Protection and Prevention);

9. Domestic Threat Response and Incident Management (by the Senior Director, Response and Recovery);
10. Economic Consequences (by the Senior Director, Response and Recovery); and
11. Public Affairs (by the Senior Director, Communications).

Each HSC/PCC shall also have an Executive Secretary to be designated by the Assistant to the President for Homeland Security (from the staff of the HSC). The Executive Secretary of each HSC/PCC shall assist his or her Chair in scheduling the meetings of the HSC/PCC, determining the agenda, recording the actions taken and tasks assigned, and ensuring timely responses to the central policy-making committees of the HSC system. The Chairman of each HSC/PCC, in consultation with its Executive Secretary, may invite representatives of other executive departments and agencies to attend meetings of the HSC/PCC, when appropriate.

The Assistant to the President for Homeland Security, at the direction of the President and in consultation with the Vice President, the Attorney General, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Transportation, and the Director of the Federal Emergency Management Agency, may establish additional HSC/PCCs, as appropriate.

The Chairman of each HSC/PCC, with the agreement of its Executive Secretary, may establish subordinate working groups to assist the PCC in the performance of its duties.

The Vice President may attend any and all meetings of any entity established by or under this directive.

This directive shall be construed in a manner consistent with Executive Order 13228.

George W. Bush

Homeland Security Presidential Directive-2

OCTOBER 29, 2001

Subject: Combating Terrorism Through Immigration Policies

A. National Policy

The United States has a long and valued tradition of welcoming immigrants and visitors. But the attacks of September 11, 2001, showed that some come to the United States to commit terrorist acts, to raise funds for illegal terrorist activities, or to provide other support for terrorist operations, here and abroad. It is the policy of the United States to work aggressively to prevent aliens who engage in or support terrorist activity from entering the United States and to detain, prosecute, or deport any such aliens who are within the United States.

1. Foreign Terrorist Tracking Task Force

By November 1, 2001, the Attorney General shall create the Foreign Terrorist Tracking Task Force (Task Force), with assistance from the Secretary of State, the Director of Central Intelligence and other officers of the government, as appropriate. The Task Force shall ensure that, to the maximum extent permitted by law, Federal agencies coordinate programs to accomplish the following: 1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and 2) locate, detain, prosecute, or deport any such aliens already present in the United States.

The Attorney General shall appoint a senior official as the full-time Director of the Task Force. The Director shall report to the Deputy Attorney General, serve as a Senior Advisor to the Assistant to the President for Homeland Security, and maintain direct liaison with the Commissioner of the Immigration and Naturalization Service (INS) on issues related to immigration and the foreign terrorist presence in the United States. The Director shall also consult with the Assistant Secretary of State for Consular Affairs on issues related to visa matters.

The Task Force shall be staffed by expert personnel from the Department of State, the INS, the Federal Bureau of Investigation, the Secret Service, the Customs

Service, the Intelligence Community, military support components, and other Federal agencies as appropriate to accomplish the Task Force's mission.

The Attorney General and the Director of Central Intelligence shall ensure, to the maximum extent permitted by law, that the Task Force has access to all available information necessary to perform its mission, and they shall request information from State and local governments, where appropriate.

With the concurrence of the Attorney General and the Director of Central Intelligence, foreign liaison officers from cooperating countries shall be invited to serve as liaisons to the Task Force, where appropriate, to expedite investigation and data sharing.

Other Federal entities, such as the Migrant Smuggling and Trafficking in Persons Coordination Center and the Foreign Leads Development Activity, shall provide the Task Force with any relevant information they possess concerning aliens suspected of engaging in or supporting terrorist activity.

2. Enhanced INS and Customs Enforcement Capability

The Attorney General and the Secretary of the Treasury, assisted by the Director of Central Intelligence, shall immediately develop and implement multi-year plans to enhance the investigative and intelligence analysis capabilities of the INS and the Customs Service. The goal of this enhancement is to increase significantly efforts to identify, locate, detain, prosecute or deport aliens associated with, suspected of being engaged in, or supporting terrorist activity within the United States.

The new multi-year plans should significantly increase the number of Customs and INS special agents assigned to Joint Terrorism Task Forces, as deemed appropriate by the Attorney General and the Secretary of the Treasury. These officers shall constitute new positions over and above the existing on-duty special agent forces of the two agencies.

3. Abuse of International Student Status

The United States benefits greatly from international students who study in our country. The United States Government shall continue to foster and support international students.

The Government shall implement measures to end the abuse of student visas and prohibit certain international students from receiving education and training in sensitive areas, including areas of study with direct application to the development and use of weapons of mass destruction. The Government shall also prohibit the education and training of foreign nationals who would use such training to harm the United States or its Allies.

The Secretary of State and the Attorney General, working in conjunction with the Secretary of Education, the Director of the Office of Science and

Technology Policy, the Secretary of Defense, the Secretary of Energy, and any other departments or entities they deem necessary, shall develop a program to accomplish this goal. The program shall identify sensitive courses of study, and shall include measures whereby the Department of State, the Department of Justice, and United States academic institutions, working together, can identify problematic applicants for student visas and deny their applications. The program shall provide for tracking the status of a foreign student who receives a visa (to include the proposed major course of study, the status of the individual as a full-time student, the classes in which the student enrolls, and the source of the funds supporting the student's education).

The program shall develop guidelines that may include control mechanisms, such as limited duration student immigration status, and may implement strict criteria for renewing such student immigration status. The program shall include guidelines for exempting students from countries or groups of countries from this set of requirements.

In developing this new program of control, the Secretary of State, the Attorney General, and the Secretary of Education shall consult with the academic community and other interested parties. This new program shall be presented through the Homeland Security Council to the President within 60 days.

The INS, in consultation with the Department of Education, shall conduct periodic reviews of all institutions certified to receive nonimmigrant students and exchange visitor program students. These reviews shall include checks for compliance with record keeping and reporting requirements. Failure of institutions to comply may result in the termination of the institution's approval to receive such students.

4. North American Complementary Immigration Policies

The Secretary of State, in coordination with the Secretary of the Treasury and the Attorney General, shall promptly initiate negotiations with Canada and Mexico to assure maximum possible compatibility of immigration, customs, and visa policies. The goal of the negotiations shall be to provide all involved countries the highest possible level of assurance that only individuals seeking entry for legitimate purposes enter any of the countries, while at the same time minimizing border restrictions that hinder legitimate trans-border commerce.

As part of this effort, the Secretaries of State and the Treasury and the Attorney General shall seek to substantially increase sharing of immigration and customs information. They shall also seek to establish a shared immigration and customs control data-base with both countries. The Secretary of State, the Secretary of the Treasury, and the Attorney General shall explore existing mechanisms to accomplish this goal and, to the maximum extent

possible, develop new methods to achieve optimal effectiveness and relative transparency. To the extent statutory provisions prevent such information sharing, the Attorney General and the Secretaries of State and the Treasury shall submit to the Director of the Office of Management and Budget proposed remedial legislation.

5. Use of Advanced Technologies for Data Sharing and Enforcement Efforts

The Director of the OSTP, in conjunction with the Attorney General and the Director of Central Intelligence, shall make recommendations about the use of advanced technology to help enforce United States immigration laws, to implement United States immigration programs, to facilitate the rapid identification of aliens who are suspected of engaging in or supporting terrorist activity, to deny them access to the United States, and to recommend ways in which existing government databases can be best utilized to maximize the ability of the government to detect, identify, locate, and apprehend potential terrorists in the United States. Databases from all appropriate Federal agencies, state and local governments, and commercial databases should be included in this review. The utility of advanced data mining software should also be addressed. To the extent that there may be legal barriers to such data sharing, the Director of the OSTP shall submit to the Director of the Office of Management and Budget proposed legislative remedies. The study also should make recommendations, propose timelines, and project budgetary requirements.

The Director of the OSTP shall make these recommendations to the President through the Homeland Security Council within 60 days.

6. Budgetary Support

The Office of Management and Budget shall work closely with the Attorney General, the Secretaries of State and of the Treasury, the Assistant to the President for Homeland Security, and all other appropriate agencies to review the budgetary support and identify changes in legislation necessary for the implementation of this directive and recommend appropriate support for a multi-year program to provide the United States a robust capability to prevent aliens who engage in or support terrorist activity from entering or remaining in the United States or the smuggling of implements of terrorism into the United States. The Director of the Office of Management and Budget shall make an interim report through the Homeland Security Council to the President on the recommended program within 30 days, and shall make a final report through the Homeland Security Council to the President on the recommended program within 60 days.

George W. Bush

Homeland Security Presidential Directive-3

MARCH 11, 2002

Purpose

The Nation requires a Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. Such a system would provide warnings in the form of a set of graduated "Threat Conditions" that would increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies would implement a corresponding set of "Protective Measures" to further reduce vulnerability or increase response capability during a period of heightened alert.

This system is intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work.

Homeland Security Advisory System

The Homeland Security Advisory System shall be binding on the executive branch and suggested, although voluntary, to other levels of government and the private sector. There are five Threat Conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

Low = Green;
Guarded = Blue;
Elevated = Yellow;
High = Orange;
Severe = Red.

The higher the Threat Condition, the greater the risk of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. Threat Conditions shall be assigned by the Attorney General in consultation with the Assistant to the President for Homeland Security. Except in exigent circumstances, the Attorney General shall seek the views of the appropriate Homeland Security Principals or their subordinates, and other parties as appropriate, on the Threat Condition to be assigned. Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. Assigned Threat Conditions shall be reviewed at regular intervals to determine whether adjustments are warranted.

For facilities, personnel, and operations inside the territorial United States, all Federal departments, agencies, and offices other than military facilities shall conform their existing threat advisory systems to this system and henceforth administer their systems consistent with the determination of the Attorney General with regard to the Threat Condition in effect.

The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures. Protective Measures are the specific steps an organization shall take to reduce its vulnerability or increase its ability to respond during a period of heightened alert. The authority to craft and implement Protective Measures rests with the Federal departments and agencies. It is recognized that departments and agencies may have several preplanned sets of responses to a particular Threat Condition to facilitate a rapid, appropriate, and tailored response. Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. Likewise, they retain the authority to respond, as necessary, to risks, threats, incidents, or events at facilities within the specific jurisdiction of their department or agency, and, as authorized by law, to direct agencies and industries to implement their own Protective Measures. They shall continue to be responsible for taking all appropriate proactive steps to reduce the vulnerability of their personnel and facilities to terrorist attack. Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition. Governors, mayors, and the leaders of other organizations are encouraged to conduct a similar review of their organizations' Protective Measures.

The decision whether to publicly announce Threat Conditions shall be made on a case-by-case basis by the Attorney General in consultation with the Assistant to the President for Homeland Security. Every effort shall be made to share as much information regarding the threat as possible, consistent

with the safety of the Nation. The Attorney General shall ensure, consistent with the safety of the Nation, that State and local government officials and law enforcement authorities are provided the most relevant and timely information. The Attorney General shall be responsible for identifying any other information developed in the threat assessment process that would be useful to State and local officials and others and conveying it to them as permitted consistent with the constraints of classification. The Attorney General shall establish a process and a system for conveying relevant information to Federal, State, and local government officials, law enforcement authorities, and the private sector expeditiously.

The Director of Central Intelligence and the Attorney General shall ensure that a continuous and timely flow of integrated threat assessments and reports is provided to the President, the Vice President, Assistant to the President and Chief of Staff, the Assistant to the President for Homeland Security, and the Assistant to the President for National Security Affairs. Whenever possible and practicable, these integrated threat assessments and reports shall be reviewed and commented upon by the wider interagency community.

A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that, at any given Threat Condition, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

1. To what degree is the threat information credible?
2. To what degree is the threat information corroborated?
3. To what degree is the threat specific and/or imminent?
4. How grave are the potential consequences of the threat?

Threat Conditions and Associated Protective Measures

The world has changed since September 11, 2001. We remain a Nation at risk to terrorist attacks and will remain at risk for the foreseeable future. At all Threat Conditions, we must remain vigilant, prepared, and ready to deter terrorist attacks. The following Threat Conditions each represent an increasing risk of terrorist attacks. Beneath each Threat Condition are some suggested Protective Measures, recognizing that the heads of Federal departments and agencies are responsible for developing and implementing appropriate agency-specific Protective Measures:

1. Low Condition (Green). This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement:
   a) Refining and exercising as appropriate preplanned Protective Measures;
   b) Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and
   c) Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.
2. Guarded Condition (Blue). This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
   a) Checking communications with designated emergency response or command locations;
   b) Reviewing and updating emergency response procedures; and
   c) Providing the public with any information that would strengthen its ability to act appropriately.
3. Elevated Condition (Yellow). An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement:
   a) Increasing surveillance of critical locations;
   b) Coordinating emergency plans as appropriate with nearby jurisdictions;
   c) Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and
   d) Implementing, as appropriate, contingency and emergency response plans.
4. High Condition (Orange). A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

a) Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
b) Taking additional precautions at public events and possibly considering alternative venues or even cancellation;
c) Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and
d) Restricting threatened facility access to essential personnel only.

5. Severe Condition (Red). A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
   a) Increasing or redirecting personnel to address critical emergency needs;
   b) Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;
   c) Monitoring, redirecting, or constraining transportation systems; and
   d) Closing public and government facilities.

Comment and Review Periods

The Attorney General, in consultation and coordination with the Assistant to the President for Homeland Security, shall, for 45 days from the date of this directive, seek the views of government officials at all levels and of public interest groups and the private sector on the proposed Homeland Security Advisory System.

One hundred thirty-five days from the date of this directive the Attorney General, after consultation and coordination with the Assistant to the President for Homeland Security, and having considered the views received during the comment period, shall recommend to the President in writing proposed refinements to the Homeland Security Advisory System.

George W. Bush

National Security Presidential/NSPD-17 Homeland Security Presidential/HSPD-4

(Unclassified Version)

The classified version of NSPD-17, as reported by the Washington Times on January 31, 2003, included this controversial sentence:

> "The United States will continue to make clear that it reserves the right to respond with overwhelming force — including potentially nuclear weapons — to the use of [weapons of mass destruction] against the United States, our forces abroad, and friends and allies."

December 2002

National Strategy to Combat Weapons of Mass Destruction

> "The gravest danger our Nation faces lies at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination. The United States will not allow these efforts to succeed. ... History will judge harshly those who saw this coming danger but failed to act. In the new world we have entered, the only path to peace and security is the path of action."
>
> ***President Bush***
> *The National Security Strategy of the United States of America*
> *September 17, 2002*

Introduction

Weapons of mass destruction (WMD) – nuclear, biological, and chemical – in the possession of hostile states and terrorists represent one of the greatest security challenges facing the United States. We must pursue a comprehensive strategy to counter this threat in all of its dimensions.

An effective strategy for countering WMD, including their use and further proliferation, is an integral component of the National Security Strategy of the United States of America. As with the war on terrorism, our strategy for homeland security, and our new concept of deterrence, the U.S. approach to combat WMD represents a fundamental change from the past. To succeed, we must take full advantage of today's opportunities, including the application of new technologies, increased emphasis on intelligence collection and analysis, the strengthening of alliance relationships, and the establishment of new partnerships with former adversaries.

Weapons of mass destruction could enable adversaries to inflict massive harm on the United States, our military forces at home and abroad, and our friends and allies. Some states, including several that have supported and continue to support terrorism, already possess WMD and are seeking even greater capabilities, as tools of coercion and intimidation. For them, these are not weapons of last resort, but militarily useful weapons of choice intended to overcome our nation's advantages in conventional forces and to deter us from responding to aggression against our friends and allies in regions of vital interest. In addition, terrorist groups are seeking to acquire WMD with the stated purpose of killing large numbers of our people and those of friends and allies — without compunction and without warning.

We will not permit the world's most dangerous regimes and terrorists to threaten us with the world's most destructive weapons. We must accord the highest priority to the protection of the United States, our forces, and our friends and allies from the existing and growing WMD threat.

Pillars of Our National Strategy

Our National Strategy to Combat Weapons of Mass Destruction has three principal pillars:

Counterproliferation to Combat WMD Use

The possession and increased likelihood of use of WMD by hostile states and terrorists are realities of the contemporary security environment. It is therefore critical that the U. S. military and appropriate civilian agencies be prepared to deter and defend against the full range of possible WMD employment scenarios. We will ensure that all needed capabilities to combat WMD are fully integrated into the emerging defense transformation plan and into our homeland security posture. Counterproliferation will also be fully integrated into the basic doctrine, training, and equipping of all forces, in order to ensure that they can sustain operations to decisively defeat WMD-armed adversaries.

Strengthened Nonproliferation to Combat WMD Proliferation

The United States, our friends and allies, and the broader international community must undertake every effort to prevent states and terrorists from acquiring WMD and missiles. We must enhance traditional measures – diplomacy, arms control, multilateral agreements, threat reduction assistance, and export controls — that seek to dissuade or impede proliferant states and terrorist networks, as well as to slow and make more costly their access to sensitive technologies, material, and expertise. We must ensure compliance with relevant international agreements, including the Nuclear Nonproliferation Treaty (NPT), the Chemical Weapons Convention (CWC), and the Biological Weapons Convention (BWC). The United States will continue to work with other states to improve their capability to prevent unauthorized transfers of WMD and missile technology, expertise, and material. We will identify and pursue new methods of prevention, such as national criminalization of proliferation activities and expanded safety and security measures.

Consequence Management to Respond to WMD Use

Finally, the United States must be prepared to respond to the use of WMD against our citizens, our military forces, and those of friends and allies. We will develop and maintain the capability to reduce to the extent possible the potentially horrific consequences of WMD attacks at home and abroad.

The three pillars of the U.S. national strategy to combat WMD are seamless elements of a comprehensive approach. Serving to integrate the pillars are four cross-cutting enabling functions that need to be pursued on a priority basis: intelligence collection and analysis on WMD, delivery systems, and related technologies; research and development to improve our ability to respond to evolving threats; bilateral and multilateral cooperation; and targeted strategies against hostile states and terrorists.

Counterproliferation

We know from experience that we cannot always be successful in preventing and containing the proliferation of WMD to hostile states and terrorists. Therefore, U.S. military and appropriate civilian agencies must possess the full range of operational capabilities to counter the threat and use of WMD by states and terrorists against the United States, our military forces, and friends and allies.

Interdiction

Effective interdiction is a critical part of the U.S. strategy to combat WMD and their delivery means. We must enhance the capabilities of our military,

intelligence, technical, and law enforcement communities to prevent the movement of WMD materials, technology, and expertise to hostile states and terrorist organizations.

Deterrence

Today's threats are far more diverse and less predictable than those of the past. States hostile to the United States and to our friends and allies have demonstrated their willingness to take high risks to achieve their goals, and are aggressively pursuing WMD and their means of delivery as critical tools in this effort. As a consequence, we require new methods of deterrence. A strong declaratory policy and effective military forces are essential elements of our contemporary deterrent posture, along with the full range of political tools to persuade potential adversaries not to seek or use WMD. The United States will continue to make clear that it reserves the right to respond with overwhelming force — including through resort to all of our options — to the use of WMD against the United States, our forces abroad, and friends and allies.

In addition to our conventional and nuclear response and defense capabilities, our overall deterrent posture against WMD threats is reinforced by effective intelligence, surveillance, interdiction, and domestic law enforcement capabilities. Such combined capabilities enhance deterrence both by devaluing an adversary's WMD and missiles, and by posing the prospect of an overwhelming response to any use of such weapons.

Defense and Mitigation

Because deterrence may not succeed, and because of the potentially devastating consequences of WMD use against our forces and civilian population, U.S. military forces and appropriate civilian agencies must have the capability to defend against WMD-armed adversaries, including in appropriate cases through preemptive measures. This requires capabilities to detect and destroy an adversary's WMD assets before these weapons are used. In addition, robust active and passive defenses and mitigation measures must be in place to enable U.S. military forces and appropriate civilian agencies to accomplish their missions, and to assist friends and allies when WMD are used.

Active defenses disrupt, disable, or destroy WMD en route to their targets. Active defenses include vigorous air defense and effective missile defenses against today's threats. Passive defenses must be tailored to the unique characteristics of the various forms of WMD. The United States must also have the ability rapidly and effectively to mitigate the effects of a WMD attack against our deployed forces.

Our approach to defend against biological threats has long been based on our approach to chemical threats, despite the fundamental differences

between these weapons. The United States is developing a new approach to provide us and our friends and allies with an effective defense against biological weapons.

Finally, U.S. military forces and domestic law enforcement agencies as appropriate must stand ready to respond against the source of any WMD attack. The primary objective of a response is to disrupt an imminent attack or an attack in progress, and eliminate the threat of future attacks. As with deterrence and prevention, an effective response requires rapid attribution and robust strike capability. We must accelerate efforts to field new capabilities to defeat WMD-related assets. The United States needs to be prepared to conduct post-conflict operations to destroy or dismantle any residual WMD capabilities of the hostile state or terrorist network. An effective U.S. response not only will eliminate the source of a WMD attack but will also have a powerful deterrent effect upon other adversaries that possess or seek WMD or missiles.

Nonproliferation

Active Nonproliferation Diplomacy

The United States will actively employ diplomatic approaches in bilateral and multilateral settings in pursuit of our nonproliferation goals. We must dissuade supplier states from cooperating with proliferant states and induce proliferant states to end their WMD and missile programs. We will hold countries responsible for complying with their commitments. In addition, we will continue to build coalitions to support our efforts, as well as to seek their increased support for nonproliferation and threat reduction cooperation programs. However, should our wide-ranging nonproliferation efforts fail, we must have available the full range of operational capabilities necessary to defend against the possible employment of WMD.

Multilateral Regimes

Existing nonproliferation and arms control regimes play an important role in our overall strategy. The United States will support those regimes that are currently in force, and work to improve the effectiveness of, and compliance with, those regimes. Consistent with other policy priorities, we will also promote new agreements and arrangements that serve our nonproliferation goals. Overall, we seek to cultivate an international environment that is more conducive to nonproliferation. Our efforts will include:

- Nuclear
  - Strengthening of the Nuclear Nonproliferation Treaty and International Atomic Energy Agency (IAEA), including through

ratification of an IAEA Additional Protocol by all NPT states parties, assurances that all states put in place full-scope IAEA safeguards agreements, and appropriate increases in funding for the Agency;
  - Negotiating a Fissile Material Cut-Off Treaty that advances U.S. security interests; and
  - Strengthening the Nuclear Suppliers Group and Zangger Committee.
- Chemical and Biological
  - Effective functioning of the Organization for the Prohibition of Chemical Weapons;
  - Identification and promotion of constructive and realistic measures to strengthen the BWC and thereby to help meet the biological weapons threat; and
  - Strengthening of the Australia Group.
- Missile
  - Strengthening the Missile Technology Control Regime (MTCR), including through support for universal adherence to the International Code of Conduct Against Ballistic Missile Proliferation.

Nonproliferation and Threat Reduction Cooperation

The United States pursues a wide range of programs, including the Nunn-Lugar program, designed to address the proliferation threat stemming from the large quantities of Soviet-legacy WMD and missile-related expertise and materials. Maintaining an extensive and efficient set of nonproliferation and threat reduction assistance programs to Russia and other former Soviet states is a high priority. We will also continue to encourage friends and allies to increase their contributions to these programs, particularly through the G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction. In addition, we will work with other states to improve the security of their WMD-related materials.

Controls on Nuclear Materials

In addition to programs with former Soviet states to reduce fissile material and improve the security of that which remains, the United States will continue to discourage the worldwide accumulation of separated plutonium and to minimize the use of highly-enriched uranium. As outlined in the National Energy Policy, the United States will work in collaboration with international partners to develop recycle and fuel treatment technologies that are cleaner, more efficient, less waste-intensive, and more proliferation-resistant.

U.S. Export Controls

We must ensure that the implementation of U.S. export controls furthers our nonproliferation and other national security goals, while recognizing the realities that American businesses face in the increasingly globalized marketplace.

We will work to update and strengthen export controls using existing authorities. We also seek new legislation to improve the ability of our export control system to give full weight to both nonproliferation objectives and commercial interests. Our overall goal is to focus our resources on truly sensitive exports to hostile states or those that engage in onward proliferation, while removing unnecessary barriers in the global marketplace.

Nonproliferation Sanctions

Sanctions can be a valuable component of our overall strategy against WMD proliferation. At times, however, sanctions have proven inflexible and ineffective. We will develop a comprehensive sanctions policy to better integrate sanctions into our overall strategy and work with Congress to consolidate and modify existing sanctions legislation.

WMD Consequence Management

Defending the American homeland is the most basic responsibility of our government. As part of our defense, the United States must be fully prepared to respond to the consequences of WMD use on our soil, whether by hostile states or by terrorists. We must also be prepared to respond to the effects of WMD use against our forces deployed abroad, and to assist friends and allies.

The National Strategy for Homeland Security discusses U.S. Government programs to deal with the consequences of the use of a chemical, biological, radiological, or nuclear weapon in the United States. A number of these programs offer training, planning, and assistance to state and local governments. To maximize their effectiveness, these efforts need to be integrated and comprehensive. Our first responders must have the full range of protective, medical, and remediation tools to identify, assess, and respond rapidly to a WMD event on our territory.

The White House Office of Homeland Security will coordinate all federal efforts to prepare for and mitigate the consequences of terrorist attacks within the United States, including those involving WMD. The Office of Homeland Security will also work closely with state and local governments to ensure their planning, training, and equipment requirements are addressed. These issues, including the roles of the Department of Homeland Security, are addressed in detail in the National Strategy for Homeland Security.

The National Security Council's Office of Combating Terrorism coordinates and helps improve U. S. efforts to respond to and manage the recovery from terrorist attacks outside the United States. In cooperation with the Office of Combating Terrorism, the Department of State coordinates interagency efforts to work with our friends and allies to develop their own emergency preparedness and consequence management capabilities.

Integrating the Pillars

Several critical enabling functions serve to integrate the three pillars — counterproliferation, nonproliferation, and consequence management — of the U.S. National Strategy to Combat WMD.

Improved Intelligence Collection and Analysis

A more accurate and complete understanding of the full range of WMD threats is, and will remain, among the highest U. S. intelligence priorities, to enable us to prevent proliferation, and to deter or defend against those who would use those capabilities against us. Improving our ability to obtain timely and accurate knowledge of adversaries' offensive and defensive capabilities, plans, and intentions is key to developing effective counter - and nonproliferation policies and capabilities. Particular emphasis must be accorded to improving: intelligence regarding WMD-related facilities and activities; interaction among U.S. intelligence, law enforcement, and military agencies; and intelligence cooperation with friends and allies.

Research and Development

The United States has a critical need for cutting-edge technology that can quickly and effectively detect, analyze, facilitate interdiction of, defend against, defeat, and mitigate the consequences of WMD. Numerous U.S. Government departments and agencies are currently engaged in the essential research and development to support our overall strategy against WMD proliferation.

The new Counterproliferation Technology Coordination Committee, consisting of senior representatives from all concerned agencies, will act to improve interagency coordination of U.S. Government counterproliferation research and development efforts. The Committee will assist in identifying priorities, gaps, and overlaps in existing programs and in examining options for future investment strategies.

Strengthened International Cooperation

WMD represent a threat not just to the United States, but also to our friends and allies and the broader international community. For this reason, it is

vital that we work closely with like-minded countries on all elements of our comprehensive proliferation strategy.

Targeted Strategies Against Proliferants

All elements of the overall U. S. strategy to combat WMD must be brought to bear in targeted strategies against supplier and recipient states of WMD proliferation concern, as well as against terrorist groups which seek to acquire WMD.

A few states are dedicated proliferators, whose leaders are determined to develop, maintain, and improve their WMD and delivery capabilities, which directly threaten the United States, U.S. forces overseas, and/or our friends and allies. Because each of these regimes is different, we will pursue country-specific strategies that best enable us and our friends and allies to prevent, deter, and defend against WMD and missile threats from each of them. These strategies must also take into account the growing cooperation among proliferant states — so-called secondary proliferation — which challenges us to think in new ways about specific country strategies.

One of the most difficult challenges we face is to prevent, deter, and defend against the acquisition and use of WMD by terrorist groups. The current and potential future linkages between terrorist groups and state sponsors of terrorism are particularly dangerous and require priority attention. The full range of counterproliferation, nonproliferation, and consequence management measures must be brought to bear against the WMD terrorist threat, just as they are against states of greatest proliferation concern.

End Note

Our National Strategy to Combat WMD requires much of all of us — the Executive Branch, the Congress, state and local governments, the American people, and our friends and allies. The requirements to prevent, deter, defend against, and respond to today's WMD threats are complex and challenging. But they are not daunting. We can and will succeed in the tasks laid out in this strategy; we have no other choice.

George W. Bush

Homeland Security Presidential Directive/HSPD-5

FEBRUARY 28, 2003

Subject: Management of Domestic Incidents

Purpose

(1) To enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.

Definitions

(2) In this directive:
(a) the term "Secretary" means the Secretary of Homeland Security.
(b) the term "Federal departments and agencies" means those executive departments enumerated in 5 U.S.C. 101, together with the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.
(c) the terms "State," "local," and the "United States" when it is used in a geographical sense, have the same meanings as used in the Homeland Security Act of 2002, Public Law 107–296.

Policy

(3) To prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management. The objective of the United States Government is to ensure that all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management. In these efforts, with regard to domestic incidents, the United States Government treats crisis management and consequence management as a single, integrated function, rather than as two separate functions.

(4) The Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The Secretary shall coordinate the Federal Government's resources utilized in response to or recovery from terrorist attacks, major disasters, or other emergencies if and when any one of the following four conditions applies: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of State and local authorities are overwhelmed and Federal assistance has been requested by the appropriate State and local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President.

(5) Nothing in this directive alters, or impedes the ability to carry out, the authorities of Federal departments and agencies to perform their responsibilities under law. All Federal departments and agencies shall cooperate with the Secretary in the Secretary's domestic incident management role.

(6) The Federal Government recognizes the roles and responsibilities of State and local authorities in domestic incident management. Initial responsibility for managing domestic incidents generally falls on State and local authorities. The Federal Government will assist State and local authorities when their resources are overwhelmed, or when Federal interests are involved. The Secretary will coordinate with State and local governments to ensure adequate planning, equipment, training, and exercise activities. The Secretary will also provide assistance to State and local governments to develop all-hazards plans and capabilities, including those of greatest importance to the security of the United States, and will ensure that State, local, and Federal plans are compatible.

(7) The Federal Government recognizes the role that the private and nongovernmental sectors play in preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies. The Secretary will coordinate with the private and nongovernmental sectors to ensure adequate planning, equipment, training, and exercise activities and to promote partnerships to address incident management capabilities.

(8) The Attorney General has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups

inside the United States, or directed at United States citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States, as well as for related intelligence collection activities within the United States, subject to the National Security Act of 1947 and other applicable law, Executive Order 12333, and Attorney General-approved procedures pursuant to that Executive Order. Generally acting through the Federal Bureau of Investigation, the Attorney General, in cooperation with other Federal departments and agencies engaged in activities to protect our national security, shall also coordinate the activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. Following a terrorist threat or an actual incident that falls within the criminal jurisdiction of the United States, the full capabilities of the United States shall be dedicated, consistent with United States law and with activities of other Federal departments and agencies to protect our national security, to assisting the Attorney General to identify the perpetrators and bring them to justice. The Attorney General and the Secretary shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments.

(9) Nothing in this directive impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures. The Secretary of Defense shall provide military support to civil authorities for domestic incidents as directed by the President or when consistent with military readiness and appropriate under the circumstances and the law. The Secretary of Defense shall retain command of military forces providing civil support. The Secretary of Defense and the Secretary shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments.

(10) The Secretary of State has the responsibility, consistent with other United States Government activities to protect our national security, to coordinate international activities related to the prevention, preparation, response, and recovery from a domestic incident, and for the protection of United States citizens and United States interests overseas. The Secretary of State and the Secretary shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments.

(11) The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall be responsible for interagency policy coordination on domestic and international incident management, respectively, as directed by the President. The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall work together to ensure that the United States domestic and international incident management efforts are seamlessly united.

(12) The Secretary shall ensure that, as appropriate, information related to domestic incidents is gathered and provided to the public, the private sector, State and local authorities, Federal departments and agencies, and, generally through the Assistant to the President for Homeland Security, to the President. The Secretary shall provide standardized, quantitative reports to the Assistant to the President for Homeland Security on the readiness and preparedness of the Nation — at all levels of government — to prevent, prepare for, respond to, and recover from domestic incidents.

(13) Nothing in this directive shall be construed to grant to any Assistant to the President any authority to issue orders to Federal departments and agencies, their officers, or their employees.

Tasking

(14) The heads of all Federal departments and agencies are directed to provide their full and prompt cooperation, resources, and support, as appropriate and consistent with their own responsibilities for protecting our national security, to the Secretary, the Attorney General, the Secretary of Defense, and the Secretary of State in the exercise of the individual leadership responsibilities and missions assigned in paragraphs (4), (8), (9), and (10), respectively, above.

(15) The Secretary shall develop, submit for review to the Homeland Security Council, and administer a National Incident Management System (NIMS). This system will provide a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources.

(16) The Secretary shall develop, submit for review to the Homeland Security Council, and administer a National Response Plan (NRP). The Secretary shall consult with appropriate Assistants to the President (including the Assistant to the President for Economic Policy) and the Director of the Office of Science and Technology Policy, and other such Federal officials as may be appropriate, in developing and implementing the NRP. This plan shall integrate Federal Government domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan. The NRP shall be unclassified. If certain operational aspects require classification, they shall be included in classified annexes to the NRP.

(a) The NRP, using the NIMS, shall, with regard to response to domestic incidents, provide the structure and mechanisms for national level policy and operational direction for Federal support to State and local incident managers and for exercising direct Federal authorities and responsibilities, as appropriate.

(b) The NRP will include protocols for operating under different threats or threat levels; incorporation of existing Federal emergency and incident management plans (with appropriate modifications and revisions) as either integrated components of the NRP or as supporting operational plans; and additional operational plans or annexes, as appropriate, including public affairs and intergovernmental communications.

(c) The NRP will include a consistent approach to reporting incidents, providing assessments, and making recommendations to the President, the Secretary, and the Homeland Security Council.

(d) The NRP will include rigorous requirements for continuous improvements from testing, exercising, experience with incidents, and new information and technologies.

(17) The Secretary shall:

(a) By April 1, 2003, (1) develop and publish an initial version of the NRP, in consultation with other Federal departments and agencies; and (2) provide the Assistant to the President for Homeland Security with a plan for full development and implementation of the NRP.

(b) By June 1, 2003, (1) in consultation with Federal departments and agencies and with State and local governments, develop a national system of standards, guidelines, and protocols to implement the NIMS; and (2) establish a mechanism for ensuring ongoing management and maintenance of the NIMS, including regular consultation with other Federal departments and agencies and with State and local governments.

(c) By September 1, 2003, in consultation with Federal departments and agencies and the Assistant to the President for Homeland Security, review existing authorities and regulations and prepare recommendations for the President on revisions necessary to implement fully the NRP.

(18) The heads of Federal departments and agencies shall adopt the NIMS within their departments and agencies and shall provide support and assistance to the Secretary in the development and maintenance of the NIMS. All Federal departments and agencies will use the NIMS in their domestic incident management and emergency prevention, preparedness, response, recovery, and mitigation activities, as well as those actions taken in support of State or local entities. The heads of Federal departments and agencies shall participate in the NRP, shall assist and support the Secretary in the development and maintenance of the NRP, and shall participate in and use domestic incident reporting systems and protocols established by the Secretary.

(19) The head of each Federal department and agency shall:

(a) By June 1, 2003, make initial revisions to existing plans in accordance with the initial version of the NRP.

(b) By August 1, 2003, submit a plan to adopt and implement the NIMS to the Secretary and the Assistant to the President for Homeland Security. The Assistant to the President for Homeland Security shall advise the President on whether such plans effectively implement the NIMS.

(20) Beginning in Fiscal Year 2005, Federal departments and agencies shall make adoption of the NIMS a requirement, to the extent permitted by law, for providing Federal preparedness assistance through grants, contracts, or other activities. The Secretary shall develop standards and guidelines for determining whether a State or local entity has adopted the NIMS.

Technical and Conforming Amendments to National Security Presidential Directive-1 (NSPD-1)

(21) NSPD-1 ("Organization of the National Security Council System") is amended by replacing the fifth sentence of the third paragraph on the first page with the following: "The Attorney General, the Secretary of Homeland Security, and the Director of the Office of Management and Budget shall be invited to attend meetings pertaining to their responsibilities."

Technical and Conforming Amendments to National Security Presidential Directive-8 (NSPD-8)

(22) NSPD-8 ("National Director and Deputy National Security Advisor for Combating Terrorism") is amended by striking "and the Office of Homeland Security," on page 4, and inserting "the Department of Homeland Security, and the Homeland Security Council" in lieu thereof.

Technical and Conforming Amendments to Homeland Security Presidential Directive-2 (HSPD-2)

(23) HSPD-2 ("Combating Terrorism Through Immigration Policies") is amended as follows:
(a) striking "the Commissioner of the Immigration and Naturalization Service (INS)" in the second sentence of the second paragraph in section 1, and inserting "the Secretary of Homeland Security" in lieu thereof ;
(b) striking "the INS," in the third paragraph in section 1, and inserting "the Department of Homeland Security" in lieu thereof;
(c) inserting ", the Secretary of Homeland Security," after "The Attorney General" in the fourth paragraph in section 1;
(d) inserting ", the Secretary of Homeland Security," after "the Attorney General" in the fifth paragraph in section 1;
(e) striking "the INS and the Customs Service" in the first sentence of the first paragraph of section 2, and inserting "the Department of Homeland Security" in lieu thereof;
(f) striking "Customs and INS" in the first sentence of the second paragraph of section 2, and inserting "the Department of Homeland Security" in lieu thereof;
(g) striking "the two agencies" in the second sentence of the second paragraph of section 2, and inserting "the Department of Homeland Security" in lieu thereof;
(h) striking "the Secretary of the Treasury" wherever it appears in section 2, and inserting "the Secretary of Homeland Security" in lieu thereof;
(i) inserting ", the Secretary of Homeland Security," after "The Secretary of State" wherever the latter appears in section 3;
(j) inserting ", the Department of Homeland Security," after "the Department of State," in the second sentence in the third paragraph in section 3;
(k) inserting "the Secretary of Homeland Security," after "the Secretary of State," in the first sentence of the fifth paragraph of section 3;
(l) striking "INS" in the first sentence of the sixth paragraph of section 3, and inserting "Department of Homeland Security" in lieu thereof;
(m) striking "the Treasury" wherever it appears in section 4 and inserting "Homeland Security" in lieu thereof;

(n) inserting ", the Secretary of Homeland Security," after "the Attorney General" in the first sentence in section 5; and
(o) inserting ", Homeland Security" after "State" in the first sentence of section 6.

Technical and Conforming Amendments to Homeland Security Presidential Directive-3 (HSPD-3)

(24) The Homeland Security Act of 2002 assigned the responsibility for administering the Homeland Security Advisory System to the Secretary of Homeland Security. Accordingly, HSPD-3 of March 11, 2002 ("Homeland Security Advisory System") is amended as follows:
(a) replacing the third sentence of the second paragraph entitled "Homeland Security Advisory System" with "Except in exigent circumstances, the Secretary of Homeland Security shall seek the views of the Attorney General, and any other federal agency heads the Secretary deems appropriate, including other members of the Homeland Security Council, on the Threat Condition to be assigned."
(b) inserting "At the request of the Secretary of Homeland Security, the Department of Justice shall permit and facilitate the use of delivery systems administered or managed by the Department of Justice for the purposes of delivering threat information pursuant to the Homeland Security Advisory System." as a new paragraph after the fifth paragraph of the section entitled "Homeland Security Advisory System."
(c) inserting ", the Secretary of Homeland Security" after "The Director of Central Intelligence" in the first sentence of the seventh paragraph of the section entitled "Homeland Security Advisory System".
(d) striking "Attorney General" wherever it appears (except in the sentences referred to in subsections (a) and (c) above), and inserting "the Secretary of Homeland Security" in lieu thereof; and
(e) striking the section entitled "Comment and Review Periods."

George W. Bush

Homeland Security Presidential Directive/HSPD-6

SEPTEMBER 16, 2003

Subject: Integration and Use of Screening Information

To protect against terrorism it is the policy of the United States to (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

This directive shall be implemented in a manner consistent with the provisions of the Constitution and applicable laws, including those protecting the rights of all Americans.

To further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism, and to the full extent permitted by law and consistent with the policy set forth above:

(1) The Attorney General shall establish an organization to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes.

(2) The heads of executive departments and agencies shall, to the extent permitted by law, provide to the Terrorist Threat Integration Center (TTIC) on an ongoing basis all appropriate Terrorist Information in their possession, custody, or control. The Attorney General, in coordination with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence shall implement appropriate procedures and safeguards with respect to all such information about United States persons. The TTIC will provide the organization referenced in paragraph (1) with access to all appropriate information or intelligence

in the TTIC's custody, possession, or control that the organization requires to perform its functions.

(3) The heads of executive departments and agencies shall conduct screening using such information at all appropriate opportunities, and shall report to the Attorney General not later than 90 days from the date of this directive, as to the opportunities at which such screening shall and shall not be conducted.

(4) The Secretary of Homeland Security shall develop guidelines to govern the use of such information to support State, local, territorial, and tribal screening processes, and private sector screening processes that have a substantial bearing on homeland security.

(5) The Secretary of State shall develop a proposal for my approval for enhancing cooperation with certain foreign governments, beginning with those countries for which the United States has waived visa requirements, to establish appropriate access to terrorism screening information of the participating governments.

This directive does not alter existing authorities or responsibilities of department and agency heads to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

The Attorney General, in consultation with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence, shall report to me through the Assistant to the President for Homeland Security not later than October 31, 2003, on progress made to implement this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

George W. Bush

Homeland Security Presidential Directive/HSPD-7

DECEMBER 17, 2003

Subject: Critical Infrastructure Identification, Prioritization, and Protection

Purpose

(1) This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

Background

(2) Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence.

(3) America's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. The majority of these are owned and operated by the private sector and State or local governments. These critical infrastructures and key resources are both physical and cyber-based and span all sectors of the economy.

(4) Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.

(5) While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.

Definitions

(6) In this directive:
- (a) The term "critical infrastructure" has the meaning given to that term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).
- (b) The term "key resources" has the meaning given that term in section 2(9) of the Homeland Security Act of 2002 (6 U.S.C. 101(9)).
- (c) The term "the Department" means the Department of Homeland Security.
- (d) The term "Federal departments and agencies" means those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.
- (e) The terms "State," and "local government," when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).
- (f) The term "the Secretary" means the Secretary of Homeland Security.
- (g) The term "Sector-Specific Agency" means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category. Sector-Specific Agencies will conduct their activities under this directive in accordance with guidance provided by the Secretary.
- (h) The terms "protect" and "secure" mean reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks.

Policy

(7) It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:
- (a) cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;

(b) impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
(c) undermine State and local government capacities to maintain order and to deliver minimum essential public services;
(d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
(e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or
(f) undermine the public's morale and confidence in our national economic and political institutions.

(8) Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective.

(9) Federal departments and agencies will ensure that homeland security programs do not diminish the overall economic security of the United States.

(10) Federal departments and agencies will appropriately protect information associated with carrying out this directive, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

(11) Federal departments and agencies shall implement this directive in a manner consistent with applicable provisions of law, including those protecting the rights of United States persons.

Roles and Responsibilities of the Secretary

(12) In carrying out the functions assigned in the Homeland Security Act of 2002, the Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.

(13) Consistent with this directive, the Secretary will identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass

casualties comparable to those from the use of a weapon of mass destruction.

(14) The Secretary will establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities.

(15) The Secretary shall coordinate protection activities for each of the following critical infrastructure sectors: information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping. The Department shall coordinate with appropriate departments and agencies to ensure the protection of other key resources including dams, government facilities, and commercial facilities. In addition, in its role as overall cross-sector coordinator, the Department shall also evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time, as appropriate.

(16) The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations. To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. The organization will support the Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law.

(17) The Secretary will work closely with other Federal departments and agencies, State and local governments, and the private sector in accomplishing the objectives of this directive.

Roles and Responsibilities of Sector-Specific Federal Agencies

(18) Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, there are designated Sector-Specific Agencies, including:

(a) Department of Agriculture — agriculture, food (meat, poultry, egg products);
(b) Health and Human Services — public health, healthcare, and food (other than meat, poultry, egg products);
(c) Environmental Protection Agency — drinking water and water treatment systems;
(d) Department of Energy — energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities;
(e) Department of the Treasury — banking and finance;
(f) Department of the Interior — national monuments and icons; and
(g) Department of Defense — defense industrial base.

(19) In accordance with guidance provided by the Secretary, Sector-Specific Agencies shall:
(a) collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;
(b) conduct or facilitate vulnerability assessments of the sector; and
(c) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

(20) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance.

(21) Federal departments and agencies shall cooperate with the Department in implementing this directive, consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

Roles and Responsibilities of Other Departments, Agencies, and Offices

(22) In addition to the responsibilities given the Department and Sector-Specific Agencies, there are special functions of various Federal departments and agencies and components of the Executive Office of the President related to critical infrastructure and key resources protection.
(a) The Department of State, in conjunction with the Department, and the Departments of Justice, Commerce, Defense, the Treasury and other appropriate agencies, will work with foreign countries and international organizations to strengthen the protection of United States critical infrastructure and key resources.
(b) The Department of Justice, including the Federal Bureau of Investigation, will reduce domestic terrorist threats, and investigate and

prosecute actual or attempted terrorist attacks on, sabotage of, or disruptions of critical infrastructure and key resources. The Attorney General and the Secretary shall use applicable statutory authority and attendant mechanisms for cooperation and coordination, including but not limited to those established by presidential directive.

(c) The Department of Commerce, in coordination with the Department, will work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act to assure the timely availability of industrial products, materials, and services to meet homeland security requirements.

(d) A Critical Infrastructure Protection Policy Coordinating Committee will advise the Homeland Security Council on interagency policy related to physical and cyber infrastructure protection. This PCC will be chaired by a Federal officer or employee designated by the Assistant to the President for Homeland Security.

(e) The Office of Science and Technology Policy, in coordination with the Department, will coordinate interagency research and development to enhance the protection of critical infrastructure and key resources.

(f) The Office of Management and Budget (OMB) shall oversee the implementation of government-wide policies, principles, standards, and guidelines for Federal government computer security programs. The Director of OMB will ensure the operation of a central Federal information security incident center consistent with the requirements of the Federal Information Security Management Act of 2002.

(g) Consistent with the E-Government Act of 2002, the Chief Information Officers Council shall be the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of information resources of Federal departments and agencies.

(h) The Department of Transportation and the Department will collaborate on all matters relating to transportation security and transportation infrastructure protection. The Department of Transportation is responsible for operating the national air space system. The Department of Transportation and the Department will collaborate in regulating the transportation of hazardous materials by all modes (including pipelines).

(i) All Federal departments and agencies shall work with the sectors relevant to their responsibilities to reduce the consequences of catastrophic failures not caused by terrorism.

(23) The heads of all Federal departments and agencies will coordinate and cooperate with the Secretary as appropriate and consistent with their own responsibilities for protecting critical infrastructure and key resources.

(24) All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. Consistent with the Federal Information Security Management Act of 2002, agencies will identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Coordination with the Private Sector

(25) In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms:

(a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and

(b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

National Special Security Events

(26) The Secretary, after consultation with the Homeland Security Council, shall be responsible for designating events as "National Special Security Events" (NSSEs). This directive supersedes language in previous presidential directives regarding the designation of NSSEs that is inconsistent herewith.

Implementation

(27) Consistent with the Homeland Security Act of 2002, the Secretary shall produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives within 1 year from the issuance of this directive. The Plan shall include, in addition to other Homeland Security-related elements as the Secretary deems appropriate, the following elements:

(a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department intends to work with Federal departments and agencies, State and local governments, the private sector, and foreign countries and international organizations;
(b) a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources;
(c) a summary of initiatives for sharing critical infrastructure and key resources information and for providing critical infrastructure and key resources threat warning data to State and local governments and the private sector; and
(d) coordination and integration, as appropriate, with other Federal emergency management and preparedness activities including the National Response Plan and applicable national preparedness goals.

(28) The Secretary, consistent with the Homeland Security Act of 2002 and other applicable legal authorities and presidential guidance, shall establish appropriate systems, mechanisms, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources with other Federal departments and agencies, State and local governments, and the private sector in a timely manner.

(29) The Secretary will continue to work with the Nuclear Regulatory Commission and, as appropriate, the Department of Energy in order to ensure the necessary protection of:
(a) commercial nuclear reactors for generating electric power and nonpower nuclear reactors used for research, testing, and training;
(b) nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and
(c) the transportation, storage, and disposal of nuclear materials and waste.

(30) In coordination with the Director of the Office of Science and Technology Policy, the Secretary shall prepare on an annual basis a Federal Research and Development Plan in support of this directive.

(31) The Secretary will collaborate with other appropriate Federal departments and agencies to develop a program, consistent with applicable law, to geospatially map, image, analyze, and sort critical infrastructure and key resources by utilizing commercial satellite and airborne systems, and existing capabilities within other agencies. National technical means should be considered as an option of last resort. The Secretary, with advice from the Director of Central Intelligence, the Secretaries of Defense and the Interior, and the heads of other appropriate Federal departments and agencies, shall develop mechanisms

for accomplishing this initiative. The Attorney General shall provide legal advice as necessary.

(32) The Secretary will utilize existing, and develop new, capabilities as needed to model comprehensively the potential implications of terrorist exploitation of vulnerabilities in critical infrastructure and key resources, placing specific focus on densely populated areas. Agencies with relevant modeling capabilities shall cooperate with the Secretary to develop appropriate mechanisms for accomplishing this initiative.

(33) The Secretary will develop a national indications and warnings architecture for infrastructure protection and capabilities that will facilitate:
   (a) an understanding of baseline infrastructure operations;
   (b) the identification of indicators and precursors to an attack; and
   (c) a surge capacity for detecting and analyzing patterns of potential attacks.

In developing a national indications and warnings architecture, the Department will work with Federal, State, local, and non-governmental entities to develop an integrated view of physical and cyber infrastructure and key resources.

(34) By July 2004, the heads of all Federal departments and agencies shall develop and submit to the Director of the OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

(35) On an annual basis, the Sector-Specific Agencies shall report to the Secretary on their efforts to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in their respective sectors. The report shall be submitted within 1 year from the issuance of this directive and on an annual basis thereafter.

(36) The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs will lead a national security and emergency preparedness communications policy review, with the heads of the appropriate Federal departments and agencies, related to convergence and next generation architecture. Within 6 months after the issuance of this directive, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall submit for my consideration any recommended changes to such policy.

(37) This directive supersedes Presidential Decision Directive/NSC-63 of May 22, 1998 ("Critical Infrastructure Protection"), and any Presidential directives issued prior to this directive to the extent of

any inconsistency. Moreover, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall jointly submit for my consideration a Presidential directive to make changes in Presidential directives issued prior to this date that conform such directives to this directive.

(38) This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

George W. Bush

Homeland Security Presidential Directive/HSPD-8

DECEMBER 17, 2003

Subject: National Preparedness

Purpose

(1) This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.

Definitions

(2) For the purposes of this directive:

(a) The term "all-hazards preparedness" refers to preparedness for domestic terrorist attacks, major disasters, and other emergencies.

(b) The term "Federal departments and agencies" means those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.

(c) The term "Federal preparedness assistance" means Federal department and agency grants, cooperative agreements, loans, loan guarantees, training, and/or technical assistance provided to State and local governments and the private sector to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Unless noted otherwise, the term "assistance" will refer to Federal assistance programs.

(d) The term "first responder" refers to those individuals who in the early stages of an incident are responsible for the protection and

preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations.

(e) The terms "major disaster" and "emergency" have the meanings given in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(f) The term "major events" refers to domestic terrorist attacks, major disasters, and other emergencies.

(g) The term "national homeland security preparedness-related exercises" refers to homeland security-related exercises that train and test national decision makers and utilize resources of multiple Federal departments and agencies. Such exercises may involve State and local first responders when appropriate. Such exercises do not include those exercises conducted solely within a single Federal department or agency.

(h) The term "preparedness" refers to the existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from major events. The term "readiness" is used interchangeably with preparedness.

(i) The term "prevention" refers to activities undertaken by the first responder community during the early stages of an incident to reduce the likelihood or consequences of threatened or actual terrorist attacks. More general and broader efforts to deter, disrupt, or thwart terrorism are not addressed in this directive.

(j) The term "Secretary" means the Secretary of Homeland Security.

(k) The terms "State," and "local government," when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

Relationship to HSPD-5

(3) This directive is a companion to HSPD-5, which identifies steps for improved coordination in response to incidents. This directive describes the way Federal departments and agencies will prepare for such a response, including prevention activities during the early stages of a terrorism incident.

Development of a National Preparedness Goal

(4) The Secretary is the principal Federal official for coordinating the implementation of all-hazards preparedness in the United States. In cooperation with other Federal departments and agencies, the Secretary coordinates the preparedness of Federal response assets, and the support for, and assessment of, the preparedness of State and local first responders.

(5) To help ensure the preparedness of the Nation to prevent, respond to, and recover from threatened and actual domestic terrorist attacks, major disasters, and other emergencies, the Secretary, in coordination with the heads of other appropriate Federal departments and agencies and in consultation with State and local governments, shall develop a national domestic all-hazards preparedness goal. Federal departments and agencies will work to achieve this goal by:
   (a) providing for effective, efficient, and timely delivery of Federal preparedness assistance to State and local governments; and
   (b) supporting efforts to ensure first responders are prepared to respond to major events, especially prevention of and response to threatened terrorist attacks.

(6) The national preparedness goal will establish measurable readiness priorities and targets that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them. It will also include readiness metrics and elements that support the national preparedness goal including standards for preparedness assessments and strategies, and a system for assessing the Nation's overall preparedness to respond to major events, especially those involving acts of terrorism.

(7) The Secretary will submit the national preparedness goal to me through the Homeland Security Council (HSC) for review and approval prior to, or concurrently with, the Department of Homeland Security's Fiscal Year 2006 budget submission to the Office of Management and Budget.

Federal Preparedness Assistance

(8) The Secretary, in coordination with the Attorney General, the Secretary of Health and Human Services (HHS), and the heads of other Federal departments and agencies that provide assistance for first responder preparedness, will establish a single point of access to Federal preparedness assistance program information within 60 days of the issuance of this directive. The Secretary will submit to me through the HSC recommendations of specific Federal department and agency programs to be part of the coordinated approach. All Federal departments and agencies will cooperate with this effort. Agencies will

continue to issue financial assistance awards consistent with applicable laws and regulations and will ensure that program announcements, solicitations, application instructions, and other guidance documents are consistent with other Federal preparedness programs to the extent possible. Full implementation of a closely coordinated interagency grant process will be completed by September 30, 2005.

(9) To the extent permitted by law, the primary mechanism for delivery of Federal preparedness assistance will be awards to the States. Awards will be delivered in a form that allows the recipients to apply the assistance to the highest priority preparedness requirements at the appropriate level of government. To the extent permitted by law, Federal preparedness assistance will be predicated on adoption of Statewide comprehensive all-hazards preparedness strategies. The strategies should be consistent with the national preparedness goal, should assess the most effective ways to enhance preparedness, should address areas facing higher risk, especially to terrorism, and should also address local government concerns and Citizen Corps efforts. The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, will review and approve strategies submitted by the States. To the extent permitted by law, adoption of approved Statewide strategies will be a requirement for receiving Federal preparedness assistance at all levels of government by September 30, 2005.

(10) In making allocations of Federal preparedness assistance to the States, the Secretary, the Attorney General, the Secretary of HHS, the Secretary of Transportation, the Secretary of Energy, the Secretary of Veterans Affairs, the Administrator of the Environmental Protection Agency, and the heads of other Federal departments and agencies that provide assistance for first responder preparedness will base those allocations on assessments of population concentrations, critical infrastructures, and other significant risk factors, particularly terrorism threats, to the extent permitted by law.

(11) Federal preparedness assistance will support State and local entities' efforts including planning, training, exercises, interoperability, and equipment acquisition for major events as well as capacity building for prevention activities such as information gathering, detection, deterrence, and collaboration related to terrorist attacks. Such assistance is not primarily intended to support existing capacity to address normal local first responder operations, but to build capacity to address major events, especially terrorism.

(12) The Attorney General, the Secretary of HHS, the Secretary of Transportation, the Secretary of Energy, the Secretary of Veterans Affairs, the Administrator of the Environmental Protection Agency, and the

heads of other Federal departments and agencies that provide assistance for first responder preparedness shall coordinate with the Secretary to ensure that such assistance supports and is consistent with the national preparedness goal.

(13) Federal departments and agencies will develop appropriate mechanisms to ensure rapid obligation and disbursement of funds from their programs to the States, from States to the local community level, and from local entities to the end users to derive maximum benefit from the assistance provided. Federal departments and agencies will report annually to the Secretary on the obligation, expenditure status, and the use of funds associated with Federal preparedness assistance programs.

Equipment

(14) The Secretary, in coordination with State and local officials, first responder organizations, the private sector and other Federal civilian departments and agencies, shall establish and implement streamlined procedures for the ongoing development and adoption of appropriate first responder equipment standards that support nationwide interoperability and other capabilities consistent with the national preparedness goal, including the safety and health of first responders.

(15) To the extent permitted by law, equipment purchased through Federal preparedness assistance for first responders shall conform to equipment standards in place at time of purchase. Other Federal departments and agencies that support the purchase of first responder equipment will coordinate their programs with the Department of Homeland Security and conform to the same standards.

(16) The Secretary, in coordination with other appropriate Federal departments and agencies and in consultation with State and local governments, will develop plans to identify and address national first responder equipment research and development needs based upon assessments of current and future threats. Other Federal departments and agencies that support preparedness research and development activities shall coordinate their efforts with the Department of Homeland Security and ensure they support the national preparedness goal.

Training and Exercises

(17) The Secretary, in coordination with the Secretary of HHS, the Attorney General, and other appropriate Federal departments and agencies and in consultation with State and local governments, shall establish and maintain a comprehensive training program to meet the national preparedness goal. The program will identify standards and maximize

the effectiveness of existing Federal programs and financial assistance and include training for the Nation's first responders, officials, and others with major event preparedness, prevention, response, and recovery roles. Federal departments and agencies shall include private organizations in the accreditation and delivery of preparedness training as appropriate and to the extent permitted by law.

(18) The Secretary, in coordination with other appropriate Federal departments and agencies, shall establish a national program and a multi-year planning system to conduct homeland security preparedness-related exercises that reinforces identified training standards, provides for evaluation of readiness, and supports the national preparedness goal. The establishment and maintenance of the program will be conducted in maximum collaboration with State and local governments and appropriate private sector entities. All Federal departments and agencies that conduct national homeland security preparedness-related exercises shall participate in a collaborative, interagency process to designate such exercises on a consensus basis and create a master exercise calendar. The Secretary will ensure that exercises included in the calendar support the national preparedness goal. At the time of designation, Federal departments and agencies will identify their level of participation in national homeland security preparedness-related exercises. The Secretary will develop a multi-year national homeland security preparedness-related exercise plan and submit the plan to me through the HSC for review and approval.

(19) The Secretary shall develop and maintain a system to collect, analyze, and disseminate lessons learned, best practices, and information from exercises, training events, research, and other sources, including actual incidents, and establish procedures to improve national preparedness to prevent, respond to, and recover from major events. The Secretary, in coordination with other Federal departments and agencies and State and local governments, will identify relevant classes of homeland-security related information and appropriate means of transmission for the information to be included in the system. Federal departments and agencies are directed, and State and local governments are requested, to provide this information to the Secretary to the extent permitted by law.

Federal Department and Agency Preparedness

(20) The head of each Federal department or agency shall undertake actions to support the national preparedness goal, including adoption of quantifiable performance measurements in the areas of training, planning, equipment, and exercises for Federal incident management

and asset preparedness, to the extent permitted by law. Specialized Federal assets such as teams, stockpiles, and caches shall be maintained at levels consistent with the national preparedness goal and be available for response activities as set forth in the National Response Plan, other appropriate operational documents, and applicable authorities or guidance. Relevant Federal regulatory requirements should be consistent with the national preparedness goal. Nothing in this directive shall limit the authority of the Secretary of Defense with regard to the command and control, training, planning, equipment, exercises, or employment of Department of Defense forces, or the allocation of Department of Defense resources.

(21) The Secretary, in coordination with other appropriate Federal civilian departments and agencies, shall develop and maintain a Federal response capability inventory that includes the performance parameters of the capability, the timeframe within which the capability can be brought to bear on an incident, and the readiness of such capability to respond to domestic incidents. The Department of Defense will provide to the Secretary information describing the organizations and functions within the Department of Defense that may be utilized to provide support to civil authorities during a domestic crisis.

Citizen Participation

(22) The Secretary shall work with other appropriate Federal departments and agencies as well as State and local governments and the private sector to encourage active citizen participation and involvement in preparedness efforts. The Secretary shall periodically review and identify the best community practices for integrating private citizen capabilities into local preparedness efforts.

Public Communication

(23) The Secretary, in consultation with other Federal departments and agencies, State and local governments, and non-governmental organizations, shall develop a comprehensive plan to provide accurate and timely preparedness information to public citizens, first responders, units of government, the private sector, and other interested parties and mechanisms for coordination at all levels of government.

Assessment and Evaluation

(24) The Secretary shall provide to me through the Assistant to the President for Homeland Security an annual status report of the Nation's level of preparedness, including State capabilities, the readiness of

Federal civil response assets, the utilization of mutual aid, and an assessment of how the Federal first responder preparedness assistance programs support the national preparedness goal. The first report will be provided within 1 year of establishment of the national preparedness goal.

(25) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance.

(26) Actions pertaining to the funding and administration of financial assistance and all other activities, efforts, and policies in this directive shall be executed in accordance with law. To the extent permitted by law, these policies will be established and carried out in consultation with State and local governments.

(27) This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

George W. Bush

Homeland Security Presidential Directive/HSPD-9

JANUARY 30, 2004

Subject: Defense of United States Agriculture and Food

Purpose

(1) This directive establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

Background

(2) The United States agriculture and food systems are vulnerable to disease, pest, or poisonous agents that occur naturally, are unintentionally introduced, or are intentionally delivered by acts of terrorism. America's agriculture and food system is an extensive, open, interconnected, diverse, and complex structure providing potential targets for terrorist attacks. We should provide the best protection possible against a successful attack on the United States agriculture and food system, which could have catastrophic health and economic effects.

Definitions

(3) In this directive:

(a) The term critical infrastructure has the meaning given to that term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

(b) The term key resources has the meaning given that term in section 2(9) of the Homeland Security Act of 2002 (6 U.S.C. 101(9)).

(c) The term Federal departments and agencies means those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.

(d) The terms State, and local government, when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).
(e) The term Sector-Specific Agency means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category.

Policy

(4) It is the policy of the United States to protect the agriculture and food system from terrorist attacks, major disasters, and other emergencies by:
(a) identifying and prioritizing sector-critical infrastructure and key resources for establishing protection requirements;
(b) developing awareness and early warning capabilities to recognize threats;
(c) mitigating vulnerabilities at critical production and processing nodes;
(d) enhancing screening procedures for domestic and imported products; and
(e) enhancing response and recovery procedures.
(5) In implementing this directive, Federal departments and agencies will ensure that homeland security programs do not diminish the overall economic security of the United States.

Roles and Responsibilities

(6) As established in Homeland Security Presidential Directive-7 (HSPD-7), the Secretary of Homeland Security is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary of Homeland Security shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources. This directive shall be implemented in a manner consistent with HSPD-7.
(7) The Secretaries of Agriculture, Health and Human Services, and the Administrator of the Environmental Protection Agency will perform their responsibilities as Sector-Specific Agencies as delineated in HSPD-7.

Awareness and Warning

(8) The Secretaries of the Interior, Agriculture, Health and Human Services, the Administrator of the Environmental Protection Agency, and the heads of other appropriate Federal departments and agencies shall build upon and expand current monitoring and surveillance programs to:

(a) develop robust, comprehensive, and fully coordinated surveillance and monitoring systems, including international information, for animal disease, plant disease, wildlife disease, food, public health, and water quality that provides early detection and awareness of disease, pest, or poisonous agents;
(b) develop systems that, as appropriate, track specific animals and plants, as well as specific commodities and food; and
(c) develop nationwide laboratory networks for food, veterinary, plant health, and water quality that integrate existing Federal and State laboratory resources, are interconnected, and utilize standardized diagnostic protocols and procedures.

(9) The Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence, in coordination with the Secretaries of Agriculture, Health and Human Services, and the Administrator of the Environmental Protection Agency, shall develop and enhance intelligence operations and analysis capabilities focusing on the agriculture, food, and water sectors. These intelligence capabilities will include collection and analysis of information concerning threats, delivery systems, and methods that could be directed against these sectors.

(10) The Secretary of Homeland Security shall coordinate with the Secretaries of Agriculture, Health and Human Services, and the Administrator of the Environmental Protection Agency, and the heads of other appropriate Federal departments and agencies to create a new biological threat awareness capacity that will enhance detection and characterization of an attack. This new capacity will build upon the improved and upgraded surveillance systems described in paragraph 8 and integrate and analyze domestic and international surveillance and monitoring data collected from human health, animal health, plant health, food, and water quality systems. The Secretary of Homeland Security will submit a report to me through the Homeland Security Council within 90 days of the date of this directive on specific options for establishing this capability, including recommendations for its organizational location and structure.

Vulnerability Assessments

(11) The Secretaries of Agriculture, Health and Human Services, and Homeland Security shall expand and continue vulnerability assessments of the agriculture and food sectors. These vulnerability assessments should identify requirements of the National Infrastructure Protection Plan developed by the Secretary of Homeland Security, as appropriate, and shall be updated every 2 years.

Mitigation Strategies

(12) The Secretary of Homeland Security and the Attorney General, working with the Secretaries of Agriculture, Health and Human Services, the Administrator of the Environmental Protection Agency, the Director of Central Intelligence, and the heads of other appropriate Federal departments and agencies shall prioritize, develop, and implement, as appropriate, mitigation strategies to protect vulnerable critical nodes of production or processing from the introduction of diseases, pests, or poisonous agents.

(13) The Secretaries of Agriculture, Health and Human Services, and Homeland Security shall build on existing efforts to expand development of common screening and inspection procedures for agriculture and food items entering the United States and to maximize effective domestic inspection activities for food items within the United States.

Response Planning and Recovery

(14) The Secretary of Homeland Security, in coordination with the Secretaries of Agriculture, Health and Human Services, the Attorney General, and the Administrator of the Environmental Protection Agency, will ensure that the combined Federal, State, and local response capabilities are adequate to respond quickly and effectively to a terrorist attack, major disease outbreak, or other disaster affecting the national agriculture or food infrastructure. These activities will be integrated with other national homeland security preparedness activities developed under HSPD-8 on National Preparedness.

(15) The Secretary of Homeland Security, in coordination with the Secretaries of Agriculture, Health and Human Services, the Attorney General, and the Administrator of the Environmental Protection Agency, shall develop a coordinated agriculture and food-specific standardized response plan that will be integrated into the National Response Plan. This plan will ensure a coordinated response to an agriculture or food incident and will delineate the appropriate roles of Federal, State, local, and private sector partners, and will address risk communication for the general public.

(16) The Secretaries of Agriculture and Health and Human Services, in coordination with the Secretary of Homeland Security and the Administrator of the Environmental Protection Agency, shall enhance recovery systems that are able to stabilize agriculture production, the food supply, and the economy, rapidly remove and effectively dispose of contaminated agriculture and food products or infected plants and animals, and decontaminate premises.

(17) The Secretary of Agriculture shall study and make recommendations to the Homeland Security Council, within 120 days of the date of this directive, for the use of existing, and the creation of new, financial risk management tools encouraging self-protection for agriculture and food enterprises vulnerable to losses due to terrorism.

(18) The Secretary of Agriculture, in coordination with the Secretary of Homeland Security, and in consultation with the Secretary of Health and Human Services and the Administrator of the Environmental Protection Agency, shall work with State and local governments and the private sector to develop:

(a) A National Veterinary Stockpile (NVS) containing sufficient amounts of animal vaccine, antiviral, or therapeutic products to appropriately respond to the most damaging animal diseases affecting human health and the economy and that will be capable of deployment within 24 hours of an outbreak. The NVS shall leverage where appropriate the mechanisms and infrastructure that have been developed for the management, storage, and distribution of the Strategic National Stockpile.

(b) A National Plant Disease Recovery System (NPDRS) capable of responding to a high-consequence plant disease with pest control measures and the use of resistant seed varieties within a single growing season to sustain a reasonable level of production for economically important crops. The NPDRS will utilize the genetic resources contained in the U.S. National Plant Germplasm System, as well as the scientific capabilities of the Federal-State-industry agricultural research and extension system. The NPDRS shall include emergency planning for the use of resistant seed varieties and pesticide control measures to prevent, slow, or stop the spread of a high-consequence plant disease, such as wheat smut or soybean rust.

Outreach and Professional Development

(19) The Secretary of Homeland Security, in coordination with the Secretaries of Agriculture, Health and Human Services, and the heads of other appropriate Federal departments and agencies, shall work with appropriate private sector entities to establish an effective information sharing and analysis mechanism for agriculture and food.

(20) The Secretaries of Agriculture and Health and Human Services, in consultation with the Secretaries of Homeland Security and Education, shall support the development of and promote higher education programs for the protection of animal, plant, and public health. To the extent permitted by law and subject to availability of funds, the program will provide capacity building grants to colleges and schools

of veterinary medicine, public health, and agriculture that design higher education training programs for veterinarians in exotic animal diseases, epidemiology, and public health as well as new programs in plant diagnosis and treatment.

(21) The Secretaries of Agriculture and Health and Human Services, in consultation with the Secretaries of Homeland Security and Education, shall support the development of and promote a higher education program to address protection of the food supply. To the extent permitted by law and subject to the availability of funds, the program will provide capacity-building grants to universities for interdisciplinary degree programs that combine training in food sciences, agriculture sciences, medicine, veterinary medicine, epidemiology, microbiology, chemistry, engineering, and mathematics (statistical modeling) to prepare food defense professionals.

(22) The Secretaries of Agriculture, Health and Human Services, and Homeland Security shall establish opportunities for professional development and specialized training in agriculture and food protection, such as internships, fellowships, and other post-graduate opportunities that provide for homeland security professional workforce needs.

Research and Development

(23) The Secretaries of Homeland Security, Agriculture, and Health and Human Services, the Administrator of the Environmental Protection Agency, and the heads of other appropriate Federal departments and agencies, in consultation with the Director of the Office of Science and Technology Policy, will accelerate and expand development of current and new countermeasures against the intentional introduction or natural occurrence of catastrophic animal, plant, and zoonotic diseases. The Secretary of Homeland Security will coordinate these activities. This effort will include countermeasure research and development of new methods for detection, prevention technologies, agent characterization, and dose response relationships for high-consequence agents in the food and the water supply.

(24) The Secretaries of Agriculture and Homeland Security will develop a plan to provide safe, secure, and state-of-the-art agriculture biocontainment laboratories that research and develop diagnostic capabilities for foreign animal and zoonotic diseases.

(25) The Secretary of Homeland Security, in consultation with the Secretaries of Agriculture and Health and Human Services, shall establish university-based centers of excellence in agriculture and food security.

Budget

(26) For all future budgets, the Secretaries of Agriculture, Health and Human Services, and Homeland Security shall submit to the Director of the Office of Management and Budget, concurrent with their budget submissions, an integrated budget plan for defense of the United States food system.

Implementation

(27) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and Presidential guidance.

(28) This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

George W. Bush

Biodefense for the 21st Century

(Unclassified Version of HSPD-10)

APRIL 28, 2004

> "Bioterrorism is a real threat to our country. It's a threat to every nation that loves freedom. Terrorist groups seek biological weapons; we know some rogue states already have them. … It's important that we confront these real threats to our country and prepare for future emergencies."
>
> **President George W. Bush, June 12, 2002**

> "Armed with a single vial of a biological agent, small groups of fanatics, or failing states could gain the power to threaten great nations, threaten the world peace. America, and the entire civilized world, will face this threat for decades to come. We must confront the danger with open eyes, and unbending purpose."
>
> **President Bush, February 11, 2004**

Biological weapons in the possession of hostile states or terrorists pose unique and grave threats to the safety and security of the United States and our allies.

Biological weapons attacks could cause catastrophic harm. They could inflict widespread injury and result in massive casualties and economic disruption. Bioterror attacks could mimic naturally occurring disease, potentially delaying recognition of an attack and creating uncertainty about whether one has even occurred. An attacker may thus believe that he could escape identification and capture or retaliation.

Biological weapons attacks could be mounted either inside or outside the United States and, because some biological weapons agents are contagious, the effects of an initial attack could spread widely. Disease outbreaks, whether natural or deliberate, respect no geographic or political borders.

Preventing and controlling future biological weapons threats will be even more challenging. Advances in biotechnology and life sciences — including the spread of expertise to create modified or novel organisms — present the

prospect of new toxins, live agents, and bioregulators that would require new detection methods, preventive measures, and treatments. These trends increase the risk for surprise. Anticipating such threats through intelligence efforts is made more difficult by the dual-use nature of biological technologies and infrastructure, and the likelihood that adversaries will use denial and deception to conceal their illicit activities. The stakes could not be higher for our Nation. Attacks with biological weapons could:

- Cause catastrophic numbers of acute casualties, long-term disease and disability, psychological trauma, and mass panic;
- Disrupt critical sectors of our economy and the day-to-day lives of Americans; and
- Create cascading international effects by disrupting and damaging international trade relationships, potentially globalizing the impacts of an attack on United States soil.

Fortunately, the United States possesses formidable capabilities to mount credible biodefenses. We have mobilized our unrivaled biomedical research infrastructure and expanded our international research relationships. In addition, we have an established medical and public health infrastructure that is being revitalized and expanded. These capabilities provide a critical foundation on which to build improved and comprehensive biodefenses.

The United States has pursued aggressively a broad range of programs and capabilities to confront the biological weapons threat. These actions, taken together, represent an extraordinary level of effort by any measure. Among our significant accomplishments, we have:

- Expanded international efforts to keep dangerous biological materials out of the hands of terrorists;
- Launched the Proliferation Security Initiative to stem the trafficking in weapons of mass destruction (WMD), including biological weapons;
- Established the BioWatch program, a network of environmental sensors to detect biological weapons attacks against major cities in the United States;
- Initiated new programs to secure and defend our agriculture and food systems against biological contamination;
- Increased funding for bioterrorism research within the Department of Health and Human Services by thirty-fold;
- Expanded the Strategic National Stockpile of medicines for treating victims of bioterror attacks, ensuring that the stockpile.s .push packages. can be anywhere in the United States within 12 hours;

- Stockpiled enough smallpox vaccine for every American, and vaccinated over 450,000 members of the armed services;
- Launched and funded Project BioShield to speed the development and acquisition of new medical countermeasures against biological weapons;
- Provided Federal funds to improve the capacities of state and local health systems to detect, diagnose, prevent, and respond to biological weapons attacks; and
- Worked with the international community to strengthen global, regional and national programs to prevent, detect, and respond to biological weapons attacks.

Building on these accomplishments, we conducted a comprehensive evaluation of our biological defense capabilities to identify future priorities and actions to support them. The results of that study provide a blueprint for our future biodefense program, Biodefense for the 21st century, that fully integrates the sustained efforts of the national and homeland security, medical, public health, intelligence, diplomatic, and law enforcement communities.

Specific direction to departments and agencies to carry out this biodefense program is contained in a classified version of this directive.

Biodefense for the 21st Century

The United States will continue to use all means necessary to prevent, protect against, and mitigate biological weapons attacks perpetrated against our homeland and our global interests. Defending against biological weapons attacks requires us to further sharpen our policy, coordination, and planning to integrate the biodefense capabilities that reside at the Federal, state, local, and private sector levels. We must further strengthen the strong international dimension to our efforts, which seeks close international cooperation and coordination with friends and allies to maximize our capabilities for mutual defense against biological weapons threats.

While the public health philosophy of the 20th Century — emphasizing prevention — is ideal for addressing natural disease outbreaks, it is not sufficient to confront 21st century threats where adversaries may use biological weapons agents as part of a long-term campaign of aggression and terror. Health care providers and public health officers are among our first lines of defense. Therefore, we are building on the progress of the past 3 years to further improve the preparedness of our public health and medical systems to address current and future BW threats and to respond with greater speed and flexibility to multiple or repetitive attacks.

Private, local, and state capabilities are being augmented by and coordinated with Federal assets, to provide layered defenses against biological weapons attacks. These improvements will complement and enhance our defense against emerging or reemerging natural infectious diseases.

The traditional approach toward protecting agriculture, food, and water — focusing on the natural or unintentional introduction of a disease — also is being greatly strengthened by focused efforts to address current and anticipated future biological weapons threats that may be deliberate, multiple, and repetitive.

Finally, we are continuing to adapt United States military forces to meet the biological weapons challenge. We have long recognized that adversaries may seek biological weapons to overcome our conventional strength and to deter us from responding to aggression. A demonstrated military capability to defend against biological weapons and other WMD strengthens our forward military presence in regions vital to United States security, promotes deterrence, and provides reassurance to critical friends and allies. The Department of Defense will continue to ensure that United States military forces can operate effectively in the face of biological weapons attacks, and that our troops and our critical domestic and overseas installations are effectively protected against such threats.

Pillars of Our Biodefense Program

The essential pillars of our national biodefense program are: Threat Awareness, Prevention and Protection, Surveillance and Detection, and Response and Recovery.

Successful implementation of our program requires optimizing critical cross-cutting functions such as: information management and communications; research development and acquisition; creation and maintenance of needed biodefense infrastructure, including the human capital to support it; public preparedness; and strengthened bilateral, multilateral, and international cooperation.

National biodefense preparedness and response requires the involvement of a wide range of Federal departments and agencies. The Secretary of Homeland Security is the principal Federal official for domestic incident management and is responsible for coordinating domestic Federal operations to prepare for, respond to, and recover from biological weapons attacks. The Secretary of Homeland Security coordinates, as appropriate, with the heads of other Federal departments and agencies, to effectively accomplish this mission.

The Secretary of State is the principal Federal officer responsible for international terrorist incidents that take place outside the U.S. territory, including United States support for foreign consequence management and coordinates, as appropriate, with heads of other Federal departments and

agencies, to effectively accomplish this mission. When requested by the Secretary of State, and approved by the Secretary of Defense, the Department of Defense will support United States foreign consequence management operations, as appropriate.

The following sections describe our aims and objectives for further progress under each of the pillars of our national biodefense program, as well as highlight key roles played by Federal departments and agencies.

Threat Awareness

Biological Warfare-Related Intelligence

Timely, accurate, and relevant intelligence enables all aspects of our national biodefense program. Despite the inherent challenges of identifying and characterizing biological weapons programs and anticipating biological attacks, we are improving the Intelligence Community's ability to collect, analyze, and disseminate intelligence. We are increasing the resources dedicated to these missions and adopting more aggressive approaches for accomplishing them. Among our many initiatives, we are continuing to develop more forward-looking analyses, to include Red Teaming efforts, to understand new scientific trends that may be exploited by our adversaries to develop biological weapons and to help position intelligence collectors ahead of the problem.

Assessments

Another critical element of our biodefense policy is the development of periodic assessments of the evolving biological weapons threat. First, the United States requires a continuous, formal process for conducting routine capabilities assessments to guide prioritization of our ongoing investments in biodefense-related research, development, planning, and preparedness. These assessments will be tailored to meet the requirements in each of these areas. Second, the United States requires a periodic senior-level policy net assessment that evaluates progress in implementing this policy, identifies continuing gaps or vulnerabilities in our biodefense posture, and makes recommendations for re-balancing and refining investments among the pillars of our overall biodefense policy. The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, will be responsible for conducting these assessments.

Anticipation of Future Threats

The proliferation of biological materials, technologies, and expertise increases the potential for adversaries to design a pathogen to evade our existing medical and non-medical countermeasures. To address this challenge, we are taking advantage of these same technologies to ensure that we can anticipate and prepare for the emergence of this threat. We are building the

flexibility and speed to characterize such agents, assess existing defenses, and rapidly develop safe and effective countermeasures. In addition, we must guard against the spread of potentially infectious agents from beyond our borders. We are strengthening the ability of our medical, public health, agricultural, defense, law enforcement, diplomatic, environmental, and transportation infrastructures to recognize and confront such threats and to contain their impact. The Department of Health and Human Services, in coordination with other appropriate Federal departments and agencies, is working to ensure an integrated and focused national effort to anticipate and respond to emerging biological weapons threats.

Prevention and Protection

Proactive Prevention

Preventing biological weapons attacks is by far the most cost-effective approach to biodefense. Prevention requires the continuation and expansion of current multilateral initiatives to limit the access of agents, technology, and know-how to countries, groups, or individuals seeking to develop, produce, and use these agents.

To address this challenge, we are further enhancing diplomacy, arms control, law enforcement, multilateral export controls, and threat reduction assistance that impede adversaries seeking biological weapons capabilities. Federal departments and agencies with existing authorities will continue to expand threat reduction assistance programs aimed at preventing the proliferation of biological weapons expertise. We will continue to build international coalitions to support these efforts, encouraging increased political and financial support for nonproliferation and threat reduction programs. We will also continue to expand efforts to control access and use of pathogens to strengthen security and prevention.

The National Strategy to Combat Weapons of Mass Destruction, released in December 2002, places special emphasis on the need for proactive steps to confront WMD threats. Consistent with this approach, we have improved and will further improve our ability to detect and destroy an adversary's biological weapons assets before they can be used. We are also further expanding existing capabilities to interdict enabling technologies and materials, including through the Proliferation Security Initiative. Additionally, we are working to improve supporting intelligence capabilities to provide timely and accurate information to support proactive prevention.

Responsibilities for proactive prevention are wide-ranging, with the Department of State, Department of Defense, Department of Justice, and the Intelligence Community playing critical roles in our overall government-wide effort.

Critical Infrastructure Protection

Protecting our critical infrastructure from the effects of biological weapons attacks is a priority. A biological weapons attack might deny us access to essential facilities and response capabilities. Therefore, we are working to improve the survivability and ensure the continuity and restoration of operations of critical infrastructure sectors following biological weapons attacks. Assessing the vulnerability of this infrastructure, particularly the medical, public health, food, water, energy, agricultural, and transportation sectors, is the focus of current efforts. The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, leads these efforts, which include developing and deploying biodetection technologies and decontamination methodologies.

Surveillance and Detection

Attack Warning

Early warning, detection, or recognition of biological weapons attacks to permit a timely response to mitigate their consequences is an essential component of biodefense. Through the President's recently proposed biosurveillance initiative, the United States is working to develop an integrated and comprehensive attack warning system to rapidly recognize and characterize the dispersal of biological agents in human and animal populations, food, water, agriculture, and the environment. Creating a national bioawareness system will permit the recognition of a biological attack at the earliest possible moment and permit initiation of a robust response to prevent unnecessary loss of life, economic losses, and social disruption. Such a system will be built upon and reinforce existing Federal, state, local, and international surveillance systems. The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, integrates these efforts.

Attribution

Deterrence is the historical cornerstone of our defense, and attribution — the identification of the perpetrator as well as method of attack — forms the foundation upon which deterrence rests. Biological weapons, however, lend themselves to covert or clandestine attacks that could permit the perpetrator to remain anonymous. We are enhancing our deterrence posture by improving attribution capabilities. We are improving our capability to perform technical forensic analysis and to assimilate all-source information to enable attribution assessments. We have created and designated the National Bioforensic Analysis Center of the National Biodefense Analysis and Countermeasure Center, under the Department of Homeland Security, as the lead Federal facility to conduct and facilitate the technical forensic analysis and

interpretation of materials recovered following a biological attack in support of the appropriate lead Federal agency.

Response and Recovery

Once a biological weapons attack is detected, the speed and coordination of the Federal, state, local, private sector, and international response will be critical in mitigating the lethal, medical, psychological, and economic consequences of such attacks. Responses to biological weapons attacks depend on pre-attack planning and preparedness, capabilities to treat casualties, risk communications, physical control measures, medical countermeasures, and decontamination capabilities.

Response Planning

A biological response annex is being drafted as part of our National Response Plan (NRP). We are catalyzing the development of state and local plans that are consistent with the NRP and ensure a seamless coordinated effort. Capabilities required for response and mitigation against biological attacks will be based on interagency-agreed scenarios that are derived from plausible threat assessments. These plans will be regularly tested as part of Federal, state, local, and international exercises. The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, is developing comprehensive plans that provide for seamless, coordinated Federal, state, local, and international responses to a biological attack.

Mass Casualty Care

Following a biological weapons attack, all necessary means must be rapidly brought to bear to prevent loss of life, illness, psychological trauma, and to contain the spread of potentially contagious diseases. Provision of timely preventive treatments such as antibiotics or vaccines saves lives, protects scarce medical capabilities, preserves social order, and is cost effective.

The Administration is working closely with state and local public health officials to strengthen plans to swiftly distribute needed medical countermeasures. Moreover, we are working to expand and, where needed, create new Federal, state, and local medical and public health capabilities for all-hazard mass casualty care.

The Department of Health and Human Services, in coordination with other appropriate Federal departments and agencies, is the principal Federal agency responsible for coordinating all Federal-level assets activated to support and augment the state and local medical and public health response to mass casualty events. For those mass casualty incidents that require parallel deployment of Federal assets in other functional areas such as transportation or law enforcement, the Department of Homeland Security will coordinate

the overall Federal response in accordance with its statutory authorities for domestic incident management. Under certain circumstances, the Department of Veterans Affairs and the Department of Defense, given their specialized expertise and experience, may be called upon to play important supporting roles in mass casualty care.

Risk Communication

A critical adjunct capability to mass casualty care is effective risk communication. Timely communications with the general public and the medical and public health communities can significantly influence the success of response efforts, including health- and life-sustaining interventions. Efforts will be made to develop communication strategies, plans, products, and channels to reach all segments of our society, including those with physical or language limitations. These efforts will ensure timely domestic and international dissemination of information that educates and reassures the general public and relevant professional sectors before, during, and after an attack or other public health emergency.

The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, is developing comprehensive coordinated risk communication strategies to facilitate emergency preparedness for biological weapons attacks. This includes travel and citizen advisories, international coordination and communication, and response and recovery communications in the event of a large-scale biological attack.

Medical Countermeasure Development

Development and deployment of safe, effective medical countermeasures against biological weapons agents of concern remains an urgent priority. The National Institutes of Health (NIH), under the direction of the Department of Health and Human Services, is working with the Department of Homeland Security, the Department of Defense, and other agencies to shape and execute an aggressive research program to develop better medical countermeasures. NIH's work increasingly will reflect the potential for novel or genetically engineered biological weapons agents and possible scenarios that require providing broad-spectrum coverage against a range of possible biological threats to prevent illness even after exposure. Additionally, we have begun construction of new labs. We are striving to assure the nation has the infrastructure required to test and evaluate existing, proposed, or promising countermeasures, assess their safety and effectiveness, expedite their development, and ensure rapid licensure.

The Department of Health and Human Services, in coordination with other appropriate Federal departments and agencies, will continue to ensure the development and availability of sufficient quantities of safe and efficacious medical countermeasures to mitigate illness and death in the event of a biological weapons attack.

Decontamination

Recovering from a biological weapons attack may require significant decontamination and remediation activities. We are working to improve Federal capabilities to support states and localities in their efforts to rapidly assess, decontaminate, and return to pre-attack activities, and are developing standards and protocols for the most effective approaches for these activities.

The Administrator of the Environmental Protection Agency, in coordination with the Attorney General and the Secretaries of Defense, Agriculture, Labor, Health and Human Services, and Homeland Security, is developing specific standards, protocols, and capabilities to address the risks of contamination following a biological weapons attack and developing strategies, guidelines, and plans for decontamination of persons, equipment, and facilities.

Homeland Security Presidential Directive/HSPD-11

AUGUST 27, 2004

Subject: Comprehensive Terrorist-Related Screening Procedures

(1) In order to more effectively detect and interdict individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism ("suspected terrorists") and terrorist activities, it is the policy of the United States to:
   (a) enhance terrorist-related screening (as defined below) through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security, and to do so in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law, and builds upon existing risk assessment capabilities while facilitating the efficient movement of people, cargo, conveyances, and other potentially affected activities in commerce; and
   (b) implement a coordinated and comprehensive approach to terrorist-related screening – in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure – that supports homeland security, at home and abroad.

(2) This directive builds upon HSPD-6, "Integration and Use of Screening Information to Protect Against Terrorism." The Terrorist Screening Center (TSC), which was established and is administered by the Attorney General pursuant to HSPD-6, enables Government officials to check individuals against a consolidated Terrorist Screening Center Database. Other screening activities underway within the Terrorist Threat Integration Center (TTIC) and the Department of Homeland Security further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism.

(3) In this directive, the term "terrorist-related screening" means the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. Terrorist-related screening also includes risk assessment, inspection, and credentialing.

(4) Not later than 75 days after the date of this directive, the Secretary of Homeland Security, in coordination with the Attorney General, the Secretaries of State, Defense, Transportation, Energy, Health and Human Services, Commerce, and Agriculture, the Directors of Central Intelligence and the Office of Management and Budget, and the heads of other appropriate Federal departments and agencies, shall submit to me, through the Assistant to the President for Homeland Security, a report setting forth plans and progress in the implementation of this directive, including as further described in sections 5 and 6 of this directive.

(5) The report shall outline a strategy to enhance the effectiveness of terrorist-related screening activities, in accordance with the policy set forth in section 1 of this directive, by developing comprehensive, coordinated, systematic terrorist-related screening procedures and capabilities that also take into account the need to:
   (a) maintain no less than current levels of security created by existing screening and protective measures;
   (b) encourage innovations that exceed established standards;
   (c) ensure sufficient flexibility to respond rapidly to changing threats and priorities;
   (d) permit flexibility to incorporate advancements into screening applications and technology rapidly;
   (e) incorporate security features, including unpredictability, that resist circumvention to the greatest extent possible;
   (f) build upon existing systems and best practices and, where appropriate, integrate, consolidate, or eliminate duplicative systems used for terrorist-related screening;
   (g) facilitate legitimate trade and travel, both domestically and internationally;
   (h) limit delays caused by screening procedures that adversely impact foreign relations, or economic, commercial, or scientific interests of the United States; and
   (i) enhance information flow between various screening programs.

(6) The report shall also include the following:
   (a) the purposes for which individuals will undergo terrorist-related screening;
   (b) a description of the screening opportunities to which terrorist-related screening will be applied;

(c) the information individuals must present, including, as appropriate, the type of biometric identifier or other form of identification or identifying information to be presented, at particular screening opportunities;
(d) mechanisms to protect data, including during transfer of information;
(e) mechanisms to address data inaccuracies, including names inaccurately contained in the terrorist screening data consolidated pursuant to HSPD-6;
(f) the procedures and frequency for screening people, cargo, and conveyances;
(g) protocols to support consistent risk assessment and inspection procedures;
(h) the skills and training required for the screeners at screening opportunities;
(i) the hierarchy of consequences that should occur if a risk indicator is generated as a result of a screening opportunity;
(j) mechanisms for sharing information among screeners and all relevant Government agencies, including results of screening and new information acquired regarding suspected terrorists between screening opportunities;
(k) recommended research and development on technologies designed to enhance screening effectiveness and further protect privacy interests; and
(l) a plan for incorporating known traveler programs into the screening procedures, where appropriate.

(7) Not later than 90 days after the date of this directive, the Secretary of Homeland Security, in coordination with the heads of the Federal departments and agencies listed in section 4 of this directive, shall also provide to me, through the Assistant to the President for Homeland Security and the Director of the Office of Management and Budget, a prioritized investment and implementation plan for a systematic approach to terrorist-related screening that optimizes detection and interdiction of suspected terrorists and terrorist activities. The plan shall describe the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities to implement the policy set forth in section 1 of this directive. The Secretary of Homeland Security shall further provide a report on the status of the implementation of the plan to me through the Assistant to the President for Homeland Security 6 months after the date of this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

(8) In order to ensure comprehensive and coordinated terrorist-related screening procedures, the implementation of this directive shall be consistent with Government-wide efforts to improve information sharing. Additionally, the reports and plan required under sections 4 and 7 of this directive shall inform development of Government-wide information sharing improvements.

(9) This directive does not alter existing authorities or responsibilities of department and agency heads including to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees, or agents, or any other person.

George W. Bush

Homeland Security Presidential Directive/HSPD-12

AUGUST 27, 2004

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

George W. Bush

National Security Presidential Directive/NSPD-41 Homeland Security Presidential Directive/HSPD-13

DECEMBER 21, 2004

MEMORANDUM FOR

THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF THE INTERIOR
THE SECRETARY OF COMMERCE
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE SECRETARY OF HOMELAND SECURITY
CHIEF OF STAFF TO THE PRESIDENT
DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
THE UNITED STATES TRADE REPRESENTATIVE
ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
COUNSEL TO THE PRESIDENT
ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY
CHAIRMAN, COUNCIL ON ENVIRONMENTAL QUALITY
DIRECTOR OF CENTRAL INTELLIGENCE
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
COMMANDANT OF THE COAST GUARD
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
DIRECTOR, NATIONAL COUNTERTERRORISM CENTER

Subject: Maritime Security Policy

This directive establishes U.S. policy, guidelines, and implementation actions to enhance U.S. national security and homeland security by protecting U.S. maritime interests. It directs the coordination of United States Government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities. This directive also establishes a Maritime Security Policy Coordinating Committee to coordinate interagency maritime security policy efforts.

As specified herein, the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security, in cooperation with appropriate Federal departments and agencies, will jointly coordinate the implementation of the policy set forth in Section II of this directive.

I. Background

For the purposes of this directive, "Maritime Domain" means all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances. Due to its complex nature and immense size, the Maritime Domain is particularly susceptible to exploitation and disruption by individuals, organizations, and States. The Maritime Domain facilitates a unique freedom of movement and flow of goods while allowing people, cargo, and conveyances to transit with anonymity not generally available by movement over land or by air. Individuals and organizations hostile to the United States have demonstrated a continuing desire to exploit such vulnerabilities.

The United States must deploy the full range of its operational assets and capabilities to prevent the Maritime Domain from being used by terrorists, criminals, and hostile States to commit acts of terrorism and criminal or other unlawful or hostile acts against the United States, its people, economy, property, territory, allies, and friends, while recognizing that maritime security policies are most effective when the strategic importance of international trade, economic cooperation, and the free flow of commerce are considered appropriately.

II. Policy

The security of the Maritime Domain is a global issue. The United States, in cooperation with our allies and friends around the world and our State, local, and private sector partners, will work to ensure that lawful private and public activities in the Maritime Domain are protected against attack and criminal and

otherwise unlawful or hostile exploitation. These efforts are critical to global economic stability and growth and are vital to the interests of the United States.

It is the policy of the United States to take all necessary and appropriate actions, consistent with U.S. law, treaties and other international agreements to which the United States is a party, and customary international law as determined for the United States by the President, to enhance the security of and protect U.S. interests in the Maritime Domain, including the following:

- Preventing terrorist attacks or criminal acts or hostile acts in, or the unlawful exploitation of, the Maritime Domain, and reducing the vulnerability of the Maritime Domain to such acts and exploitation;
- Enhancing U.S. national security and homeland security by protecting U.S. population centers, critical infrastructure, borders, harbors, ports, and coastal approaches in the Maritime Domain;
- Expediting recovery and response from attacks within the Maritime Domain;
- Maximizing awareness of security issues in the Maritime Domain in order to support U.S. forces and improve United States Government actions in response to identified threats;
- Enhancing international relationships and promoting the integration of U.S. allies and international and private sector partners into an improved global maritime security framework to advance common security interests in the Maritime Domain; and
- Ensuring seamless, coordinated implementation of authorities and responsibilities relating to the security of the Maritime Domain by and among Federal departments and agencies.

These actions must be undertaken in a manner that facilitates global commerce and preserves the freedom of the seas for legitimate military and commercial navigation and other legitimate activities as well as civil liberties and the rights guaranteed under the Constitution.

III. Policy Coordination

The Maritime Security Policy Coordinating Committee (MSPCC) is hereby established, consistent with NSPD-1 and HSPD-1. The MSPCC, in consultation with the relevant regional and functional policy coordinating committees of the Federal Government, and without exercising operational oversight, shall act as the primary forum for interagency coordination of the implementation of this directive. As part of that effort, the MSPCC shall review existing interagency practices, coordination, and execution of U.S. policies and strategies

relating to maritime security, and shall recommend specific improvements to all of them as warranted. The MSPCC shall provide analysis of new U.S. policies, strategies, and initiatives relating to maritime security for consideration by the Deputies and Principals Committees of the NSC and the HSC, and subsequently by the NSC and the HSC, and shall ensure ongoing coordination and implementation of such policies, strategies, and initiatives.

The reviews, plans, and recommendations required by this directive (as set forth in Sections IV and V below) shall be completed by the departments and agencies designated herein in coordination with the MSPCC, and shall then be prepared for consideration by and submitted to the Deputies and Principals Committees of the HSC and the HSC, and subsequently to the NSC and the HSC.

The MSPCC shall be co-chaired by an NSC staff representative selected by the Assistant to the President for National Security Affairs and an HSC representative selected by the Assistant to the President for Homeland Security, and shall include the following officers or their designated representatives:

- The Vice President
- The Secretary of State
- The Secretary of the Treasury
- The Secretary of Defense
- The Attorney General
- The Secretary of the Interior
- The Secretary of Commerce
- The Secretary of Transportation
- The Secretary of Energy
- The Secretary of Homeland Security
- Director, Office of Management and Budget
- The United States Trade Representative
- Chairman of the Council on Environmental Quality
- Director of Central Intelligence
- Chairman of the Joint Chiefs of Staff
- Director, Federal Bureau of Investigation
- Director, National Counterterrorism Center

The co-chairs of the MSPCC may invite representatives of other departments and agencies to attend MSPCC meetings as they deem appropriate.

IV. Policy Implementation

National Strategy for Maritime Security. A coordinated and integrated government-wide effort to enhance the security of the Maritime Domain requires an over-arching strategy. The Secretaries of Defense and Homeland Security shall jointly lead a collaborative interagency effort to draft a recommended

National Strategy for Maritime Security, which shall be submitted for my consideration within 180 days after the effective date of this directive. Such a strategy must present an over-arching plan to implement this directive and address all of the components of the Maritime Domain, including domestic, international, public, and private components. It shall further incorporate a global, cross-discipline approach to the Maritime Domain centered on a layered, defense-in-depth framework that may be adjusted based on the threat level. The strategy shall build on current efforts and those initiated by this directive, as well as complement existing strategies, tools, and resources. All relevant Federal departments and agencies shall cooperate with the Secretaries of Defense and Homeland Security in this effort and provide all appropriate assistance.

V. Policy Actions

In concert with the development of a National Strategy for Maritime Security, the following actions shall be taken:

Maritime Domain Awareness (MDA). Maritime Domain Awareness is the effective understanding of anything associated with the global Maritime Domain that could impact the security, safety, economy, or environment of the United States. It is critical that the United States develop an enhanced capability to identify threats to the Maritime Domain as early and as distant from our shores as possible by integrating intelligence, surveillance, observation, and navigation systems into a common operating picture accessible throughout the United States Government.

The Secretaries of Defense and Homeland Security have established a Maritime Domain Awareness Senior Steering Group (MDASSG). The MDASSG is co-chaired by representatives of the Secretaries of Defense and Homeland Security and includes representatives from departments and agencies that will participate in the MSPCC.

The MDASSG shall coordinate national efforts to achieve maximum Maritime Domain Awareness. No later than 180 days after the effective date of this directive, the MDASSG will develop and submit to me, through the Secretaries of Defense and Homeland Security, a national plan to improve Maritime Domain Awareness, which shall include near-term and long-term objectives, required program and resource implications, and any recommendations for organizational or policy changes.

Global Maritime Intelligence Integration. A robust and coordinated intelligence effort serves as the foundation for effective security efforts in the Maritime Domain. In support of this effort, I direct the Secretaries of Defense and Homeland Security, with the support of the Director of Central Intelligence, and in coordination with the Director of the National

Counterterrorism Center (NCTC) and the Director of the Federal Bureau of Investigation (FBI), to use existing intelligence capabilities to integrate all available intelligence on a global basis regarding the location, identity, and operational capabilities and intentions of potential threats to U.S. interests in the Maritime Domain. The Secretaries of Defense and Homeland Security, with the support of the Director of Central Intelligence, and in coordination with the Director of the NCTC, the Director of the FBI, and other appropriate departments and agencies, shall submit to me for approval, through the Assistants to the President for National Security Affairs and Homeland Security, a plan for global maritime intelligence integration within 180 days after the effective date of this directive. The plan shall include appropriate interagency participation to ensure effective government-wide sharing of information and data critical to intelligence production.

Domestic Outreach. A successful strategy to implement this directive must include coordination with State and local authorities and consultation with appropriate private sector persons and entities. The Secretary of Homeland Security, in coordination with the Attorney General and the Secretaries of the Treasury, Interior, Commerce, and Transportation, shall lead the development of a comprehensive engagement plan that ensures that the interests of State and local governments and the private sector are considered in the Federal Government's implementation of this directive. The plan shall be completed within 180 days after the effective date of this directive and shall take effect upon approval by the Secretary of Homeland Security.

Coordination of International Efforts and International Outreach. Ensuring the security of the Maritime Domain must be a global effort, in which United States Government efforts are developed and furthered with the support of other governments and international organizations resulting in lasting international cooperation. The Secretary of State shall lead the coordination of United States Government initiatives in the implementation of this directive with regard to activities with foreign governments and international organizations. All Federal departments and agencies shall coordinate with the Department of State on policies, programs, and initiatives relating to the implementation of this directive that could affect the conduct of foreign policy. In addition, the Secretary of State, in coordination with the Secretaries of Defense, Commerce, Transportation, and Homeland Security, and the U.S. Trade Representative, and in consultation with appropriate private sector persons and entities, shall develop, within 180 days after the effective date of this directive, a comprehensive plan to solicit international support for an improved global maritime security framework. Such plan shall take effect upon approval by the Secretary of State.

Maritime Threat Response. The Secretaries of Defense and Homeland Security, in consultation with the Attorney General and the Secretaries of State, the Treasury, Commerce, and Transportation, shall develop a comprehensive National Maritime Security Response Plan to ensure seamless United States Government response to maritime threats against the United States. This plan, when approved by me, shall supplement the National Response Plan required by HSPD-5 and complement the critical infrastructure protection plans required by HSPD-7 and the domestic all-hazards preparedness goals and structures required by HSPD-8. The plan, at a minimum, shall reflect lead agency roles and responsibilities, including recommendations regarding changes to existing policy, including those reflected in PDD-39 and PDD-62, in the following areas: 1) maritime security response and counterterrorism operations; 2) maritime interception operations; 3) prevention and detection of, and response to, the mining of U.S. ports; 4) detection, interdiction and disposition of targeted cargo, people, and vessels; and 5) attacks on vessels with U.S. citizens aboard or that affect U.S. interests anywhere in the world. The plan also shall: 1) include recommended protocols that establish clear coordination relationships governing protection and defense of the United States against threats to its interests in the Maritime Domain; and 2) provide recommendations concerning the designation of an interagency planning and command-and-control entity to ensure unity of command for national execution of maritime security policy. An interim plan shall be submitted no later than 180 days after the effective date of this directive, through the Assistants to the President for National Security Affairs and Homeland Security, and shall be finalized after completion of the National Strategy for Maritime Security.

Maritime Infrastructure Recovery. Rapid recovery from an attack or similar disruption in the Maritime Domain is critical to the economic well-being of our Nation. A credible capability for rapid recovery will not only minimize an incident's economic impact but also serve as a deterrent. The Secretary of Homeland Security, in coordination with other appropriate officials, including the Secretaries of Defense, State, the Treasury, the Interior, Commerce, and Transportation, and in consultation with key industry stakeholders, shall be responsible for the development of recommended minimum Federal standards, where appropriate, for maritime recovery operations, and shall develop comprehensive national maritime infrastructure recovery standards and a plan, complementary to the national preparedness goals and standards required by HSPD-8. Such standards and plan shall be completed no later than 180 days after the effective date of this directive, shall focus on the restoration of physical assets and transportation systems, and shall take effect when approved by the Secretary of Homeland Security. The standards and plan also shall describe a maritime

infrastructure recovery exercise program consistent with the National Exercise Program administered by the Department of Homeland Security. The program shall address coordination with State, local, and private sector partners, and cooperation with foreign governments and international entities as appropriate.

Maritime Transportation System Security. The Secretary of Homeland Security, in coordination with the Secretaries of Defense, State, Commerce, and Transportation, and the U.S. Trade Representative, and in consultation with appropriate industry representatives, shall develop recommendations for improvements to the national and international regulatory framework with respect to licensing, carriage, communications, safety equipment, and other critical systems for all private vessels, including commercial vessels, operating in the Maritime Domain. The recommendations shall be submitted to me, through the Assistants to the President for National Security Affairs and Homeland Security, no later than 180 days after the effective date of this directive.

Maritime Commerce Security. To implement this directive effectively and to enhance economic growth, the United States must promote global supply chain security practices to reduce the risk of terrorists or criminals acting against the United States from within the Maritime Domain. The Secretary of Homeland Security, in coordination with the Secretaries of Defense, State, the Treasury, Commerce, Transportation, and Energy and the U.S. Trade Representative shall lead a collaborative interagency effort, in consultation with appropriate industry representatives, to develop a comprehensive international maritime supply chain security plan no later than 180 days after the effective date of this directive. The plan shall define supply-chain security requirements, include recommendations to further secure commercial operations from point of origin to point of destination, build on available resources, and provide a recommended framework of roles, responsibilities, and implementation actions. The plan shall define measurable national "end state" supply chain security goals and develop contingency plans to continue the flow of commerce in the event of an incident necessitating total or partial closure of U.S. borders to maritime commerce. The plan shall take effect upon approval by the Secretary of Homeland Security.

VI. General

This directive does not alter existing authorities or responsibilities of the department and agency heads, including their authorities, to carry out operational activities or to provide or receive information. This directive is intended only to improve the internal management of the Executive Branch

and is not intended to, and does not; create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees, or agents, or any other person.

Nothing in this directive impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President and Commander-in-Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

The Assistants to the President for National Security Affairs and Homeland Security and the Chairman of the Council on Environmental Quality shall coordinate as appropriate the work of the MSPCC under this directive and the work of the Committee on Ocean Policy under the Executive Order of December 17, 2004.

George W. Bush

National Security Presidential Directive/NSPD-43 Homeland Security Presidential Directive/HSPD-14

APRIL 15, 2005

Subject: Domestic Nuclear Detection

(1) To protect against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material in the United States, and to protect against attack using such devices or materials against the people, territory, or interests of the United States, it is the policy of the United States to:
   (a) Continue to develop, deploy, and enhance national nuclear and radiological detection capabilities in an effort to better detect, report on, disrupt, and prevent attempts to import, possess, store, transport, develop, or use such devices and materials;
   (b) Continue to enhance the effective integration of nuclear and radiological detection capabilities across Federal, State, local, and tribal governments and the private sector for a managed, coordinated response; and
   (c) Continue to advance the science of nuclear and radiological detection through an aggressive, expedited, evolutionary, and transformational program of research and development in such detection technologies.

(2) To implement the policy set forth in paragraph (1), the Secretary of Homeland Security, in coordination with the Secretaries of State, Defense, and Energy, and the Attorney General, shall establish a national level Domestic Nuclear Detection Office (DNDO) within the Department of Homeland Security. The DNDO shall include personnel from the departments of Homeland Security (DHS), Defense (DOD), Energy (DOE), State (DOS), Justice (DOJ), and

other Federal departments and agencies as appropriate. The Secretary of Homeland Security shall have authority, direction, and control over the DNDO as provided in section 102 (a) (2) of the Homeland Security Act of 2002. The DNDO shall:

(a) Serve as the primary entity in the United States Government to further develop, acquire, and support the deployment of an enhanced domestic system to detect and report on attempts to import, possess, store, transport, develop, or use an unauthorized nuclear explosive device, fissile material, or radiological material in the United States, and improve that system over time;

(b) Enhance and coordinate the nuclear detection efforts of Federal, State, local, and tribal governments and the private sector to ensure a managed, coordinated response;

(c) Establish, with the approval of the Secretary of Homeland Security and in coordination with the Attorney General and the Secretaries of Defense and Energy, additional protocols and procedures for use within the United States to ensure that the detection of unauthorized nuclear explosive devices, fissile material, or radiological material is promptly reported to the Attorney General, the Secretaries of Defense, Homeland Security, and Energy, and other appropriate officials or their respective designees for appropriate action by law enforcement, military, emergency response, or other authorities;

(d) Develop, with the approval of the Secretary of Homeland Security and in coordination with the Attorney General and the Secretaries of State, Defense, and Energy, an enhanced global nuclear detection architecture with the following implementation: (i) the DNDO will be responsible for the implementation of the domestic portion of the global architecture; (ii) the Secretary of Defense will retain responsibility for implementation of DOD requirements within and outside the United States; and (iii) the Secretaries of State, Defense, and Energy will maintain their respective responsibilities for policy guidance and implementation of the portion of the global architecture outside the United States, which will be implemented consistent with applicable law and relevant international arrangements;

(e) Conduct, support, coordinate, and encourage an aggressive, expedited, evolutionary, and transformational program of research and development efforts to support the policy set forth in paragraph (1);

(f) Support and enhance the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as provide appropriate information to these entities; and

(g) Further enhance and maintain continuous awareness by analyzing information from all DNDO mission-related detection systems.

(3) To ensure the success of DNDO efforts in support of the policy, the Secretaries of State, Defense, Energy, and Homeland Security, and the Attorney General shall: (i) determine and provide appropriate nuclear, scientific, and other expertise to the DNDO; (ii) participate within the DNDO in jointly developing and coordinating detection and response guidance, protocols, and training for Federal. State, local, and tribal officials; (iii) participate within the DNDO in jointly developing and coordinating the global nuclear detection architecture; and (iv) where appropriate, participate in the conduct of research and development for nuclear detection.

(4) The Secretary of Energy shall lead the development of nonproliferation research and development and, where appropriate, make available dual-use counter-proliferation and counter-terrorism nuclear detection research and development to DNDO and other entities and officials to support the development of the domestic nuclear and radiological detection system. The Secretary of Energy will make maximum appropriate use of DNDO research, development, test and evaluation programs, and procedures for deploying equipment, taking due account of foreign sensitivities. The Secretary of Energy shall also report information related to detection events to the DNDO. Nothing in this Directive shall be construed to limit or otherwise affect any of the authorities or responsibilities of the Secretary of Energy under any statute, regulation, or executive order.

(5) The Secretary of Defense shall consult with the Secretary of Homeland Security on all aspects of the DNDO to ensure efficiencies, interoperability, and sharing of innovative concepts and operational procedures designed to protect the United States. Nothing in this Directive shall be construed to impair or otherwise affect the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commanders of the combatant commands, or military command and control procedures.

(6) The Attorney General shall coordinate with the Secretary of Homeland Security on all aspects of DNDO's global nuclear detection architecture, particularly as they relate to the development of response guidance protocols and training for Federal, State, local, and tribal law enforcement and information sharing activities. Nothing in this Directive shall be construed to impair or otherwise affect the authority of the Attorney General as stated in Homeland Security Presidential Directive/HSPD-5, "Management of Domestic Incidents," of February 28, 2003.

(7) The Secretary of State shall coordinate with the Secretary of Homeland Security on all aspects of DNDO's global nuclear detection architecture, particularly as they relate to overseas detection and reporting activities and to the formulation and implementation of U.S. foreign policy.

(8) The Director of National Intelligence (DNI) shall coordinate with the Secretary of Homeland Security on all aspects of DNDO's global nuclear detection architecture. The DNI also shall ensure the timely dissemination to the DNDO of all radiological, nuclear, and related threats to the United States and other intelligence information relevant to the support, development, and maintenance of the global nuclear detection architecture and related efforts. Functions assigned by this Directive to the DNI shall be performed by the Director of Central Intelligence until the first DNI is appointed by the President.

(9) This Directive shall be implemented in a manner consistent with applicable law, including the Atomic Energy Act of 1954, the Homeland Security Act of 2002, and the National Security Act of 1947 (all as amended), and presidential guidance, and subject to the availability of appropriations. Nothing in this Directive alters, or impedes the ability to carry out, existing authorities or responsibilities of department and agency heads to perfonn their responsibilities under law and consistent with applicable legal authorities and presidential guidance. With regard to nuclear search activities, nothing in this Directive alters in any way existing directives, responsibilities, and roles. This Directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, entities, officers, employees, or any other person.

(10) Within 120 days after the date of this Directive, and thereafter not less than annually, the Secretary of Homeland Security shall report to me through the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs on the implementation of this Directive, including an assessment of the effectiveness of DNDO and any recommendations for additional enhancements or efforts. The initial implementation report shall include (a) the plans for integrated program and budget planning between the appropriate agencies needed to properly execute the DNDO responsibilities and (b) a joint staffing plan for the DNDO.

George W. Bush

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z

FORENSICS AND CRIMINAL JUSTICE

National Security Issues in Science, Law, and Technology

The tragedy of 9/11 placed homeland security and the prevention of further attacks into the central focus of our national consciousness. With so many avenues of terror open to our enemies in terms of mode, medium, and location, effective management and mitigation of threat must be grounded in objective risk assessment. The structure of national security decisions should be premised on decision theory and science with minimal political posturing or emotional reactivisim.

National Security Issues in Science, Law, and Technology demonstrates a mature look at a frightening subject and presents sound, unbiased tools with which to approach any situation that may threaten human lives. By applying the best of scientific decision-making practices this book introduces the concept of risk management and its application in the structure of national security decisions. It examines the acquisition and utilization of all-source intelligence, including the ability to analyze data and forecast patterns, to enable policymakers to make better informed decisions. The text addresses reaction and prevention strategies applicable to chemical, biological, and nuclear weapons; agricultural terrorism; cyberterrorism; and other potential threats to our critical infrastructure. It discusses legal issues that inevitably arise when integrating new legislation with the threads of our Constitution and illustrates the dispassionate analysis of our intelligence, law enforcement, and military operations and actions. Finally, the book considers the redirection of our national research and laboratory system to investigate the very problems terrorists can induce through the use of weapons we have as yet to confront.

DK5817

ISBN 1-57444-908-7

90000

9 781574 449082

www.crcpress.com

CRC Press
Taylor & Francis Group
an informa business
www.taylorandfrancisgroup.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK