MAKING THE NATION SAFER

THE ROLE OF SCIENCE AND TECHNOLOGY IN COUNTERING TERRORISM

Committee on Science and Technology for Countering Terrorism

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Support for this project was provided with institutional funds.

Library of Congress Cataloging-in-Publication Data

Making the nation safer : the role of science and technology in countering terrorism / Committee on Science and Technology for Countering Terrorism, National Research Council.
p. cm.
ISBN 0-309-08481-4 (perfect)
1. Terrorism—Prevention—Technological innovations. 2. Terrorism—United States—Prevention. I. National Research Council (U.S.). Committee on Science and Technology for Countering Terrorism.

HV6431 .M354 2002
363.3′2′0973—dc21

2002011495

Copies available from:

Naval Studies Board
National Research Council
2101 Constitution Avenue, N.W.
Washington, DC 20418

The National Academies Press
2101 Constitution Ave., N.W.
Box 285
Washington, DC 20055
800-624-6242
202-334-3313 (in the Washington metropolitan area)

Copyright 2002 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. Wm. A. Wulf are chairman and vice chairman, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON SCIENCE AND TECHNOLOGY FOR COUNTERING TERRORISM

LEWIS M. BRANSCOMB, Harvard University, *Co-chair*
RICHARD D. KLAUSNER, Bill and Melinda Gates Foundation, *Co-chair*
JOHN D. BALDESCHWIELER, California Institute of Technology
BARRY R. BLOOM, Harvard School of Public Health
L. PAUL BREMER III, Marsh Crisis Consulting
WILLIAM F. BRINKMAN, Lucent Technologies (retired)
ASHTON B. CARTER, Harvard University
CHARLES B. CURTIS, Nuclear Threat Initiative
MORTIMER L. DOWNEY III, PB-Consult
RICHARD L. GARWIN, Council on Foreign Relations
PAUL H. GILBERT, Parsons Brinckerhoff Quade & Douglas, Inc.
M.R.C. GREENWOOD, University of California, Santa Cruz
MARGARET A. HAMBURG, Nuclear Threat Initiative
WILLIAM HAPPER, Princeton University
JOHN L. HENNESSY, Stanford University
JOSHUA LEDERBERG, Sackler Foundation at the Rockefeller University
THOMAS C. SCHELLING, University of Maryland
MAXINE F. SINGER, Carnegie Institution of Washington
NEIL J. SMELSER, University of California, Berkeley (retired)
PHILIP M. SMITH, McGeary & Smith
P. ROY VAGELOS, Merck & Co., Inc. (retired)
VINCENT VITTO, Charles S. Draper Laboratory, Inc.
GEORGE M. WHITESIDES, Harvard University
R. JAMES WOOLSEY, Shea & Gardner

Staff

RONALD D. TAYLOR, Study Director
ELIZABETH L. GROSSMAN, Program Officer
MARY G. GORDON, Information Officer
SUSAN G. CAMPBELL, Administrative Assistant
IAN M. CAMERON, Project Assistant

Foreword

This report reflects the commitment of the U.S. scientific, engineering, and health communities to help our country respond to the challenges made evident by September 11. It is a contribution from the National Academies—the National Academy of Sciences, National Academy of Engineering, Institute of Medicine, and National Research Council—which initiated this critical effort and paid for it. But this report is also a contribution to the nation from many distinguished individuals, each of whom dedicated a great deal of time to the production of the report. In all, there were 24 members of the main committee, 94 additional individuals who served on its eight subpanels, and 46 expert reviewers who provided critical feedback on the committee's draft report. These 164 individuals were motivated solely by a commitment to public service, and all of them made personal sacrifices to do their part on a very tight schedule.

The great enthusiasm and dedication with which the above groups approached their tasks are but one indication of the strong interest that Americans have shown in contributing to counterterrorism efforts. The vigorous science and technology community in our nation is ready, willing, and able to be called into service, and this report focuses on strategies for harnessing the vast talent and energy available.

This report is about the contributions of science and technology to countering terrorism, but we recognize that they are only one element of a broad array of important responses. These must include, for example, diplomacy, military actions, intelligence, and an understanding of how terrorism originates and is sustained.

Because of the fast-track nature of this effort, it has necessarily focused on the homeland security of the United States. But we must not forget that, with

respect to terrorism, the nations of the world share a common set of enemies. Many of the technical solutions that we develop in the United States to make our nation safer will also be useful for protecting the citizens and facilities of other nations. And the efforts of the scientists, engineers, and health professionals in many nations will be important for bringing the best of science and technology to bear on the world's counterterrorism efforts.

The National Academies have built strong relationships of trust over the years with colleagues around the world. Whether these colleagues are in the United Kingdom, Brazil, Russia, China, India, or elsewhere, we all share the same perspectives and hopes for a better world. This report therefore represents only the first step in what must become a long and continuing global effort to spread peace and prosperity to every nation.

Bruce Alberts President National Academy of Sciences	Wm. A. Wulf President National Academy of Engineering	Kenneth I. Shine President[1] Institute of Medicine

[1]Through June 30, 2002.

Preface

INTRODUCTION AND BACKGROUND

The September 11, 2001, terrorist attacks on the United States galvanized the nation to strengthen its homeland defenses and to pursue those responsible for the terrorist acts. The United States now leads a global effort against terrorism. The aim is to eliminate worldwide terrorist networks and reduce the effectiveness of terrorist threats. Success will depend not only on the leadership, initiative, and capabilities of the United States, but also on the cooperation and capabilities of its international partners and allies.

Immediately following the events of September 11, the presidents of the National Academy of Sciences (Bruce Alberts), the National Academy of Engineering (Wm. A. Wulf), and the Institute of Medicine (Kenneth I. Shine) collectively wrote to President George W. Bush. Stating that the new war against terrorism would "demand a focus on the complex interplay between technological, sociological, and political issues," they offered to provide the nation with the advice and counsel of the National Academies (which includes the National Academy of Sciences, the National Academy of Engineering, the Institute of Medicine, and the National Research Council).

Historically, the National Academies have long recognized the important role of science and technology in helping the nation meet its security needs. The ability to create, maintain, and draw from a reservoir of science, engineering, and medical knowledge has underpinned many of the nation's efforts to combat adversaries. Such a reservoir was the basis for the great science, engineering, and medical contributions made during World War II. It must be recognized, however, that successful application then required dedicated financial resources, sci-

entists, engineers, and physicians who directed themselves to the tasks at hand, and organization and leadership to effectively deploy both knowledge and people in the wartime science effort. The science and engineering community responded in a similar way to the shock of Sputnik and the growing technical capability of the USSR, then our adversary, and the Cold War required a sustained effort by this community over four decades. More recently, the national and international response to AIDS by scientists and physicians has demonstrated once again that science can mobilize to respond to a threat. The response has benefited from a reservoir of knowledge accumulated through two decades of sustained biomedical science that has been well supported financially in the United States and other industrialized nations. A successful response to the threat of catastrophic terrorism will require the same type of long-term dedication and focus.

The security threat the nation now faces affects every phase of domestic life and demands that technical solutions that might be deployed relatively quickly be readily accessible to local and state entities, as well as to the federal government. The challenge is to identify the threats (and the nation's vulnerabilities), to identify responses to those threats, and to organize properly the nation's immense science and engineering capabilities to meet both short- and long-term needs.

The scientific enterprise is enormously complex—consisting of universities, industry, government, professional societies, and such. Although capable of meeting the research and development challenges posed by the threat of terrorism, it is highly fragmented. The institutional, managerial, and public policy problems that must be solved are daunting. They include (1) defining criteria for setting the nation's research priorities, (2) identifying those research priorities, and (3) proposing new institutional arrangements and entities that will enable a stronger interaction between the nation's science and technical enterprise and its security apparatus.

From its vantage point as an adviser to the nation on science, engineering, and medicine, the National Academies have been working diligently since September 11 to marshal a substantial number of the most knowledgeable experts to address how the scientific and technological capabilities of the United States can best be harnessed for the many challenges ahead.

TERMS OF REFERENCE

In December 2001, the National Academies, using institutional funds, initiated this project. The aim was to help the federal government—and, more specifically, the Executive Office of the President—to enlist the nation's and the world's scientific and technical community in a timely response to the threat of catastrophic terrorism. A committee of distinguished scientists and engineers was established to help the government develop an integrated science and technology program plan and a research strategy for combating terrorism.

The terms of reference called for the following three tasks to be completed within 6 months: (1) prepare a carefully delineated framework for the application of science and technology for countering terrorism, (2) prepare research agendas in nine key areas, and (3) examine a series of crosscutting issues. More specifically,

- The framework should characterize the range of threats to the nation's security (in terms of targets, weapons, and delivery systems, and the possible points of intervention).
- Research agendas should be developed in areas of vulnerability related to biological sciences; chemical sciences; nuclear and radiological sciences; information technology and telecommunications; transportation; energy facilities; cities and fixed infrastructure; behavioral, social, and institutional issues; and systems analysis and systems engineering. For each area, the research agenda should identify highly leveraged opportunities for using science and technology in countering terrorism.
- Multidisciplinary research topics that cut across the above domains and the threats that arise from the interdependence of these areas should be considered in developing the final program plan and research strategy.

The objective of this study has been to strengthen the government's ability to use science and technology for combating terrorism. Critical questions also exist about how a comprehensive national counterterrorism effort involving research, development, and deployment can be planned and executed. Many of these questions remain to be addressed, but this study did define a number of the important issues in this area.

THE COMMITTEE'S APPROACH

A committee of 24 of the nation's leading scientific, engineering, medical, and policy experts conducted the study described in this report. The range of expertise on the committee reflected the broad array of scientific and technical topics to be covered under its charge. The committee also included members with the expertise necessary to address issues related to the context in which the research priorities would be set and implemented (e.g., experts in science and technology policy, national security, and public health). Finally, many of the committee's experts were or are active advisers to federal agencies, and they brought to this project an awareness of ongoing governmental counterterrorism efforts. Biographies of the committee are provided in Appendix A.

To supplement the committee's own expertise, eight panels were separately appointed and asked to provide input on the specific topical areas identified in the committee's charge. The panels were (1) Biological Sciences, (2) Chemical Issues, (3) Nuclear and Radiological Issues, (4) Information Technology, (5)

Transportation, (6) Energy Facilities, Cities, and Fixed Infrastructure, (7) Behavioral, Social, and Institutional Issues, and (8) Systems Analysis and Systems Engineering. Each panel was chaired by a member of the committee. The panels brought the expertise and experience of approximately 90 additional scientists, engineers, and medical professionals (supported by approximately 15 NRC senior staff) to the study. These study participants are listed in Appendix B.

The focus of the committee's work was on *making the nation safer* from emerging terrorist threats that would seek to inflict catastrophic damage on the nation's people, its infrastructure, or its economy. The committee's approach was to identify current threats to the nation, understand the most likely vulnerabilities in the face of these threats, and identify highly leveraged opportunities for science and technology contributions to counterterrorism in both the near term and the long term. Such contributions—including intelligence and surveillance, prevention, protection, interdiction, response and recovery, attribution, and analysis—can be made at any point along a time line that extends from before a terrorist act to its aftermath. The committee organized its approach by considering the issues in nine areas: nuclear and radiological threats; human and agricultural health systems; toxic chemicals and explosive materials; information technology; energy systems; transportation systems; cities and fixed infrastructure; the response of people to terrorism; and complex and interdependent systems. Within each of these areas, the relevant panel was tasked with the following:

- Outline current capabilities for countering terrorist threats and describe priorities and time frames for developing additional capabilities. Develop, for each domain, a research strategy that identifies highly leveraged opportunities for science and technology to contribute to counterterrorism. Identify the areas within the framework of terrorist acts and responses to which the panel's technical domain is relevant, evaluate the current state of knowledge and capacity for dealing with the most significant threats, and identify significant barriers to the use of technology, as well as areas in which knowledge may be available but underutilized.
- Consider policies or activities that might be required to reduce any new technologies to practice and facilitate their deployment. Where possible, simultaneously address domain-specific issues and identify needs that either cut across domain lines or are not readily described within the traditional domains.
- Focus on science and technology applications that are relevant to the most pressing issues and/or that would yield the most generic solutions. Identify short-term opportunities and pay special attention to ideas, admittedly some with uncertain outcomes, that might arise from new scientific discoveries and new inventions, even if they might not emerge for 5 years or more. Take note of any opportunities that were identified in earlier studies or that are currently planned or under way at federal agencies.
- Consider how the proposed research agendas could be implemented.

Accordingly, each panel developed a set of recommendations that ranged from long-term research and development to immediate- or near-term deployment of existing technologies or application of available knowledge. The motivation for these recommendations was to illustrate how knowledge gained, capabilities developed, and actions taken could mitigate specific problems. These recommendations do not answer many critical questions for the federal government, to which the majority are addressed. Nor do they provide a single prioritized list of threats, vulnerabilities, or solutions. Neither the panels nor the committee knew of a clear methodology to create such lists, especially since the committee did not access classified intelligence information about the capabilities and intentions of terrorists.

During the course of this fast-track project the committee met four times:

- December 19-20, 2001, Washington, D.C. At this organizational meeting the committee received its charge from the presidents of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. It then developed a preliminary outline of the report, devised a plan for completing its work, and reviewed the membership rosters of the panels and the committee's charge.
- January 31-February 1, 2002, Washington, D.C. The committee reviewed the initial work of the panels on threats, vulnerabilities, and responses and provided feedback to the panel chairs.
- April 8-9, 2002, Washington, D.C. The committee reviewed the work of the panels and discussed issues in the specific areas covered by the panels, as well as the overarching themes for the report.
- May 13-14, 2002, Washington, D.C. At its final meeting the committee reviewed the draft report and finalized its agreement on the findings, conclusions, and recommendations.

The committee also held a number of teleconferences over the course of the study period to review the work status and findings of the panels. Most of the panels met three times between January and March 2002, and they received scores of briefings from federal officials and other experts in the field to inform their judgment and contribute to the base of information (see Appendix C). Written panel inputs were submitted to the committee on March 31, 2002.

The work of the panels informed the committee and provided the basis for Chapters 2 through 11 of the report. The committee also used the work of the panels to motivate the discussions and recommendations on general issues related to the implementation of science and technology for countering terrorism (see Chapters 12 and 13).

Overall, the committee believes that it has identified scientific and technological means by which the nation may reduce—but not eliminate—the vulnerabilities of its society to catastrophic terrorist acts and mitigate the consequences of such acts when they occur. It outlines some research and development priori-

ties that will be needed to make the nation safer and improve its ability to succeed in the war on terrorism. But most importantly, the committee outlines a national strategy by which the strengths of U.S. science and engineering can most effectively be brought to bear on the defense of our nation on a continuing basis.

FINAL NOTES

Although this study is based on the extensive work of the panels and the input that they provided in their domains of expertise, the authorship responsibility for this report rests solely with the committee.

While traditional procedures for an independent NRC study, including review of the report by independent experts, were followed, it is important to note that trade-offs were made in order to accommodate the rapid schedule. For example, the report does not provide extensive references to the scientific literature nor does it marshal detailed evidence to support its findings. Rather, it largely presents the consensus scientific views and judgments of the committee members, based on the knowledge that these individuals have accumulated through their own scholarly efforts and professional experience, through formal and informal interactions with the nation's science, engineering, and medical communities, and through the efforts of the supporting panels.

The committee was deeply aware of the difficulty of writing a report that was sufficiently specific about terrorist threats to explain how science and engineering might be helpful, without providing information that might aid terrorists in determining new means of attack. In many cases, quite specific information that was available to the committee is presented in the report in a more generic form. In the area of nuclear and radiological threats, the relevant panel accessed classified information in the course of this study and has produced a classified annex to this report. An unclassified discussion of the issues related to nuclear and radiological threats is provided in Chapter 2 of this report.

Acknowledgments

The Committee on Science and Technology for Countering Terrorism witnessed firsthand the scientific, engineering, and medical community's unstinting commitment to join with the rest of the civilized international community in the global effort against terrorism. Without hesitation the members of the eight panels supporting this study, the individuals asked to brief the panels, those who spoke informally with committee and panel members, and the National Research Council staff supporting the study shared their expertise and insights and offered their best ideas on short notice to inform the committee, the technical community, and the federal government. The committee extends its sincerest gratitude to the many individuals who provided valuable information and support during the course of this study.

The panel members are listed in Appendix B. Their work provided much of the intellectual base for the study. The panels in turn received inputs from many briefers on a wide array of topics related to counterterrorism activities across a number of disciplines and infrastructures; these inputs to the panels are acknowledged in Appendix C, "Panel Activities."

Ronald D. Taylor, study director, and Elizabeth L. Grossman, program officer, both of the National Research Council, managed this study and contributed significantly to the ideas and their expression in this report. Without their leadership and dedication, it would not have been possible for this project to achieve its objectives on an exceptionally tight schedule with an unusually broad scope of technical and policy content. The committee is immensely grateful to both of them. The committee also appreciates the support it received from the project staff, Susan G. Campbell, Mary G. Gordon, and Ian M. Cameron, over the course of this fast-track study.

The committee is also grateful to have been able to draw on resources from across the National Academies. Individual program staff members from five divisions[1] played a vital role in supporting the work of the panels, as listed with the panels in Appendix B. Thanks are also due to Douglas C. Bauer for undertaking research and gathering background information on some of the issues related to the structure of the federal government as well as the government's interaction with industry. His tireless work in support of the committee is greatly appreciated.

The committee was fortunate to engage the services of a highly professional and experienced editorial staff, including Steven J. Marcus (a nationally known technical editor) and Elizabeth Fikre and Susan Maurizi, both of the National Research Council staff.

The National Academies gratefully acknowledge David and Katherine Bradley for their financial support of the dissemination of this publication.

[1]Program staff from the Division on Engineering and Physical Sciences, Division on Earth and Life Studies, Division of Behavioral and Social Sciences and Education, Institute of Medicine, and Transportation Research Board participated in this study.

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making the published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

John F. Ahearne, Sigma Xi, The Scientific Research Society,
Alfred V. Aho, Lucent Technologies,
Norman R. Augustine, Lockheed Martin Corporation (retired),
Mark Y. Berman, BP America,
Steven M. Block, Stanford University,
Floyd E. Bloom, The Scripps Research Institute,
Lillian C. Borrone, Port Authority of New York and New Jersey (retired),
Norman M. Bradburn, National Science Foundation,
John I. Brauman, Stanford University,
Donald E. Brown, University of Virginia,
George Bugliarello, Polytechnic University,
Richard F. Celeste, Cleveland Heights, Ohio,
Robert R. Everett, MITRE Corporation (retired),
Stanley Falkow, Stanford University,
Robert A. Frosch, Harvard University,

Richard A. Gaggioli, Marquette University,
Bobby R. Gillham, Conoco, Inc.
Ralph E. Gomory, Alfred P. Sloan Foundation,
Andrew J. Goodpastor, Atlantic Council of the United States,
Robert J. Hermann, Global Technology Partners, LLC (retired),
Robert L. Hirsch, RAND Corporation,
Lester A. Hoel, University of Virginia,
John P. Holdren, Harvard University,
Anita K. Jones, University of Virginia,
Thomas J. Kelly, Sloan-Kettering Institute,
William Klemperer, Harvard University,
Steven E. Koonin, California Institute of Technology,
Leslie B. Lamport, Microsoft Research,
James S. Langer, University of California, Santa Barbara,
Nathan S. Lewis, California Institute of Technology,
Barbara H. Liskov, Massachusetts Institute of Technology,
Richard G. Luthy, Stanford University,
Harley W. Moon, Iowa State University,
Joseph S. Nye, Harvard University,
Thomas D. O'Rourke, Cornell University,
George W. Parshall, E.I. du Pont de Nemours & Company (retired),
William H. Press, Los Alamos National Laboratory,
Henry W. Riecken, University of Pennsylvania (emeritus),
James R. Schlesinger, Center for Strategic and International Studies,
Lucy Shapiro, Stanford University,
Harrison Shull, U.S. Naval Postgraduate School (retired),
Jeffrey J. Siirola, Eastman Chemical Company,
William Y. Smith, Institute for Defense Analyses (emeritus),
Joseph M. Sussman, Massachusetts Institute of Technology,
Alvin W. Trivelpiece, Oak Ridge National Laboratory (retired), and
Harold E. Varmus, Memorial Sloan-Kettering Cancer Center.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions and recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by R. Stephen Berry, University of Chicago (emeritus), and Gerald P. Dinneen, Honeywell, Inc. (retired). Appointed by the National Research Council, they were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests solely with the authoring committee and the institution.

Contents

EXECUTIVE SUMMARY 1

1 INTRODUCTION 25
Context of the Study, 25
Content and Structure of This Report, 30

2 NUCLEAR AND RADIOLOGICAL THREATS 39
The Nuclear and Radiological Threat Matrix, 39
Homeland Security Challenges, 49
Reducing Vulnerabilities, 51
Concluding Discussion, 63
References, 64

3 HUMAN AND AGRICULTURAL HEALTH SYSTEMS 65
Introduction, 65
Intelligence, Detection, Surveillance, and Diagnosis, 69
Prevention, Response, and Recovery, 79
Policy and Implementation, 96
Concluding Remarks, 102
References, 104

4 TOXIC CHEMICALS AND EXPLOSIVE MATERIALS 107
Inroduction, 107
Background: Chemicals as Weapons, 108
General Capabilities Needed to Help Mitigate Vulnerabilities, 113

Mitigating Vulnerabilities of Specific Systems, 121
Responding to Attacks, 127
A Strategy to Develop Economically Viable Counterterrorism Technologies, 132
References, 132
Recommended Reading on Food Safety, 133

5 INFORMATION TECHNOLOGY 135
Introduction, 135
Threats Associated with IT Infrastructure, 136
Short-Term Recommendations, 144
Long-Term Recommendations: Investing in IT Research, 146
Privacy and Confidentiality, 170
Planning for the Future, 171
Implementation, 172
References, 175

6 ENERGY SYSTEMS 177
Introduction, 177
Electric Power, 180
Oil and Natural Gas, 196
References, 208

7 TRANSPORTATION SYSTEMS 210
Introduction and Overview, 210
Transportation System Characteristics, 212
Implications for Security Strategies, 214
Research and Technology Needs, 223
Advice to the Transportation Security Administration on Strategic Research and Planning, 231
Concluding Observations, 235
Dedication, 236
References, 236

8 CITIES AND FIXED INFRASTRUCTURE 238
Introduction, 238
Emergency Management and Emergency Operations Centers, 239
Water Supply and Wastewater Systems, 245
Electrical Supply Interruption, 252
Information Technology Systems and Communications, 252
Transportation and Distribution Systems, 252
Major and Monumental Buildings, 252
Stadiums and Other Places for Large Public Gatherings, 258

Underground Facilities, Including Tunnels, 262
References, 265

9 THE RESPONSE OF PEOPLE TO TERRORISM 267
Human Populations as Targets of Terrorism, 268
The Universality of Human Responses, 270
Anticipation and Preparedness, 271
Warnings, 273
The Occurrence of Attack, 274
Recovery, 279
References, 286

10 COMPLEX AND INTERDEPENDENT SYSTEMS 287
Introduction, 287
A Framework for a Systems Approach to Counterterrorism, 288
Systems Management Issues, 290
Counterterrorism Threat Modeling, 294
Infrastructure Modeling, 300
Modeling Challenges for Counterterrorism, 305
Implications for Education, 309
References, 310

11 THE SIGNIFICANCE OF CROSSCUTTING CHALLENGES AND TECHNOLOGIES 313
Introduction, 313
Systems Analysis and Modeling, 315
Integrated Data Management, 317
Sensors and Sensor Networks, 320
Autonomous Mobile Robotic Technologies, 325
Supervisory Control and Data Acquisition Systems, 327
Biometrics, 329
Human and Organizational Factors, 330
Coordination of Programs on Crosscutting Technologies, 331
Conclusions, 332

12 EQUIPPING THE FEDERAL GOVERNMENT TO COUNTER TERRORISM 335
Introduction, 335
Managing the Federal Government's Program of Science and Technology for Countering Terrorism, 338
The Role of the Federal Agencies in Developing and Using Science and Technology for Countering Terrorism, 350
References, 355

13 ESSENTIAL PARTNERS IN A NATIONAL STRATEGY: STATES AND CITIES, INDUSTRY, AND UNIVERSITIES 357
States and Cities, 357
Industry, 359
Universities, 364
References, 371

BIBLIOGRAPHY 372

APPENDIXES

A COMMITTEE AND STAFF BIOGRAPHIES 377

B PANEL MEMBERS AND STAFF 389

C PANEL ACTIVITIES 394

D ACRONYMS AND ABBREVIATIONS 399

INDEX 405

MAKING THE NATION SAFER

Executive Summary

In the war against terrorism, America's vast science and technology base provides us with a key advantage.

— *President George W. Bush, June 6, 2002*[1]

CONTEXT AND CONTENTS OF THE REPORT

Terrorism is a serious threat to the security of the United States and indeed the world. The vulnerability of societies to terrorist attacks results in part from the proliferation of chemical, biological, and nuclear weapons of mass destruction, but it also is a consequence of the highly efficient and interconnected systems that we rely on for key services such as transportation, information, energy, and health care. The efficient functioning of these systems reflects great technological achievements of the past century, but interconnectedness within and across systems also means that infrastructures are vulnerable to local disruptions, which could lead to widespread or catastrophic failures. As terrorists seek to exploit these vulnerabilities, it is fitting that we harness the nation's exceptional scientific and technological capabilities to counter terrorist threats.

This report describes many ways in which science and engineering can contribute to making the nation safer against the threat of catastrophic terrorism. The report identifies key actions that can be undertaken now, based on knowledge and technologies in hand, and, equally important, describes key opportunities for reducing current and future risks even further through longer-term research and development activities. However, science and technology are but one element in

[1]From the President's June 6, 2002, address to the nation. The text of this speech is available online at <http://www.whitehouse.gov/news/releases/2002/06/20020606-8.html>.

a broad array of potential approaches to reducing the threat of terrorism. Diplomacy, international relations, military actions, intelligence gathering, and other instruments of national policy well beyond the scope of this study all have critical roles to play.

Our society is too complex and interconnected to defend against all possible threats. As some threats are diminished others may arise; terrorists may change their goals and tactics. While this report describes what in the committee's best judgment are the top-priority actions and research objectives for harnessing science and technology to meet today's threats, its most important conclusion is that the nation needs a well-organized and disciplined ability to respond as circum-

BOX ES.1
Fourteen of the Most Important Technical Initiatives

Immediate Applications of Existing Technologies

1. Develop and utilize robust systems for protection, control, and accounting of nuclear weapons and special nuclear materials at their sources.
2. Ensure production and distribution of known treatments and preventatives for pathogens.
3. Design, test, and install coherent, layered security systems for all transportation modes, particularly shipping containers and vehicles that contain large quantities of toxic or flammable materials.
4. Protect energy distribution services by improving security for supervisory control and data acquisition (SCADA) systems and providing physical protection for key elements of the electric-power grid.
5. Reduce the vulnerability and improve the effectiveness of air filtration in ventilation systems.
6. Deploy known technologies and standards for allowing emergency responders to reliably communicate with each other.
7. Ensure that trusted spokespersons will be able to inform the public promptly and with technical authority whenever the technical aspects of an emergency are dominant in the public's concerns.

Urgent Research Opportunities

1. Develop effective treatments and preventatives for known pathogens for which current responses are unavailable and for potential emerging pathogens.
2. Develop, test, and implement an intelligent, adaptive electric-power grid.
3. Advance the practical utility of data fusion and data mining for intelligence analysis, and enhance information security against cyberattacks.
4. Develop new and better technologies (e.g., protective gear, sensors, communications) for emergency responders.
5. Advance engineering design technologies and fire-rating standards for blast- and fire-resistant buildings.
6. Develop sensor and surveillance systems (for a wide range of targets) that create useful information for emergency officials and decision makers.
7. Develop new methods and standards for filtering air against both chemicals and pathogens as well as better methods and standards for decontamination.

stances change. In that sense this is not an enduring plan for technical work, but rather a starting point from which the nation can create defenses-in-depth against the new threat. For that reason it is especially important that strengthening the national effort in long-term research that can create new solutions should be a cornerstone of the strategy for countering terrorism.

TOP-PRIORITY TECHNICAL RECOMMENDATIONS

Key elements or infrastructures of society can be means of attack, targets, and means of response. While some systems and technologies can be classified roughly in one or another of these categories (i.e., nuclear weapons are primarily means of attack; energy systems are primarily targets), most systems and technologies can fit into multiple categories. For example, air transportation is both a target and a means of attack, and information and telecommunications systems are both targets and means of response. The Committee on Science and Technology for Countering Terrorism considered nine areas, each of which is discussed in a separate chapter. The areas are nuclear and radiological threats, human and agricultural health systems, toxic chemicals and explosive materials, information technology, energy systems, transportation systems, cities and fixed infrastructure, the response of people to terrorism, and complex and interdependent systems.

The chapters on these nine areas each contain a number of recommendations, all describing what the committee believes are critical ways to make the nation safer from terrorism. The actions and research opportunities described in the chapters cover a wide assortment of approaches, fields, and systems; they range from immediate applications of existing technology to development and deployment efforts to long-term basic research programs. Based on an understanding of the difficulty of launching particular kinds of attacks and the feasibility of limiting the damage of such attacks and of recovering from them, the committee was able to prioritize within each area in order to determine the topics covered below in this executive summary, which describes the committee's top-priority concepts and actions in each area.[2] To definitively determine the most important actions within and across all nine areas would require knowledge of the relative likelihood of threats and information about the intent and capability of terrorists. However, based on information in prior major studies and commission reports about the current threat, the committee provides a short list of important technical initiatives that span the areas (see Box ES.1). This list includes seven ways to

[2]The bold-faced sentences in this executive summary are not necessarily reproductions of the recommendations in the succeeding chapters but instead are meant to emphasize important conclusions and high-priority actions. Several recommendations from different parts of a chapter may be combined or paraphrased here to communicate an important overall point clearly and briefly; the expanded discussions in the chapters provide a more comprehensive picture.

immediately apply existing knowledge and technology to make the nation safer and seven areas of research and development in which it is urgent that programs be initiated or strengthened. These initiatives illustrate the types of actions recommended by the committee throughout this report.[3]

General Principles and Strategies for How Science and Technology Can Help Protect the Nation

In this report, the committee provides a broad range of recommendations designed to demonstrate how science and engineering can contribute to counterterrorism efforts. The suggested actions include support for all phases of countering terrorist threats—intelligence and surveillance, prevention, protection, interdiction, response and recovery, and attribution—as well as ways to improve our ability to perform analysis and invent new technologies. Different phases have varying importance in each of the nine areas examined in the report. For example, the nuclear threat must be addressed at the earliest stages, when intelligence and surveillance based on international cooperation are critical for preventing the manufacture and use of nuclear weapons by terrorists. For biological threats, the situation is reversed: An attack is relatively easy to initiate and hard to prevent, but there are many opportunities for technological intervention to mitigate the effects. In other cases, such as an attack on the electrical power system, it is possible both to make the attack more difficult and to ameliorate its effects after it has been initiated.

Despite such fundamental differences in the approaches needed for countering different classes of terrorist threats, some general principles and strategies underlie recommendations presented in all of the areas:

- Identify and repair the weakest links in vulnerable systems and infrastructures.
- Use defenses-in-depth (do not rely only on perimeter defenses or firewalls).
- Use "circuit breakers" to isolate and stabilize failing system elements.
- Build security into basic system designs where possible.
- Build flexibility into systems so that they can be modified to address unforeseen threats.
- Search for technologies that reduce costs or provide ancillary benefits to civil society to ensure a sustainable effort against terrorist threats.

[3]These important technical initiatives do not mirror individual recommendations in the executive summary or the chapters, but instead indicate actions or needs identified in several chapters or provide brief descriptions of key technology applications or research programs.

Following is a synthesis of the key findings and recommendations in each of the nine areas examined by the committee.

Nuclear and Radiological Threats (Chapter 2)

Science and technology are essential ingredients of a *multilayered systems approach* for defending the United States against terrorist attacks involving stolen nuclear weapons, improvised nuclear devices, and radiological dispersion devices. The first line of homeland defense is robust systems for the protection, control, and accounting of nuclear weapons and special nuclear material at their sources. **The United States has made a good start on deploying such systems in Russia, which possesses large stockpiles of weapons and special nuclear material, but cooperative efforts must be pursued with new urgency. The United States should accelerate its bilateral materials protection, control, and accounting program in Russia to safeguard small nuclear warheads and special nuclear materials, particularly highly enriched uranium. The United States also should increase the priority and pace of cooperative efforts with Russia to safeguard its highly enriched uranium by blending down this material to an intermediate enrichment of less than 20 percent U-235 as soon as possible.**

Systems to detect the movement of illicit weapons and materials could be most effectively deployed at a limited number of strategic transportation choke points such as critical border transit points in countries like Russia, major global cargo-container ports, major U.S. airports, and major pinch points in the U.S. interstate highway system. **A focused and coordinated near-term effort should be made to evaluate and improve the efficacy of special nuclear material detection systems that could be deployed at strategic choke points for homeland defense. Research and development (R&D) support also should be provided for improving the technological capabilities of special nuclear material detection systems, especially for detecting highly enriched uranium.**

Responses to nuclear and radiological attacks fall into two distinct categories that could require very different types of governmental actions: attacks involving the detonation of a nuclear weapon or improvised nuclear device, and attacks involving radiological dispersion devices. Planning has been minimal at the federal or local levels for responding to either class of attack. **Immediate steps should be taken to update the Federal Radiological Emergency Response Plan or to develop a separate plan, to respond to nuclear and radiological terrorist attacks, especially an attack with a nuclear weapon on a U.S. city.**

As the history of the Cold War shows, the most effective defense against attacks with nuclear weapons is a policy of nuclear retaliation, but retaliation requires that the perpetrator of an attack be definitively identified. The technology for developing the needed attribution capability exists but has to be assembled, an effort that is now under way by the Defense Threat Reduction Agency

but is expected to take several years to complete. **Given the potential importance of attribution to deterring nuclear attacks, the Defense Threat Reduction Agency's efforts to develop an attribution capability should continue to declared operability as quickly as practicable.**

Physical and operational changes may have to be made to some of the nation's nuclear power plants to mitigate vulnerabilities to attacks from the air with a large commercial airliner or a smaller aircraft loaded with high explosives and possibly to attacks from the ground using high-explosive projectiles. The technical analyses that are now being carried out by the U.S. Nuclear Regulatory Commission and industry to understand the effects of such attacks on reactor containment buildings and essential auxiliary facilities are critical to understanding the full magnitude of this threat. **These analyses should be carried to completion as soon as possible, and follow-on work to identify vulnerabilities on a plant-by-plant basis should be undertaken as soon as these initial studies are completed.**

The likely aim of a terrorist attack with a radiological dispersion device would be to spread fear and panic and cause disruption. Recovery from an attack would therefore depend on how the attack is handled by first responders, political leaders, the media, and general members of the public. **A technically credible spokesperson at the national level who is perceived as being outside the political arena should be prepared to provide accurate and usable information to the media and public concerning public health and safety risks and appropriate response actions in the aftermath of a nuclear or radiological attack.**

Although radiological attacks would be unlikely to cause large numbers of casualties, the potential for inflicting economic loss and causing terror or panic warrants increased attention to the control and use of radiological sources by regulatory agencies and materials licensees. **The U.S. Nuclear Regulatory Commission and states having agreements with this agency should tighten regulations for obtaining and possessing radiological sources that could be used in terrorist attacks, as well as requirements for securing and tracking these sources.**

Important progress is being made by the R&D and policy communities on reducing the nation's vulnerability to nuclear and radiological terrorism. There is not much evidence, however, that the R&D activities are being coordinated, that thought is being given to prioritizing these activities against other national counterterrorism needs, or that effective mechanisms are in place to transfer the results of these activities to applications. **A single federal agency should be designated as the nation's lead research and development agency for nuclear and radiological counterterrorism.** This agency should develop a focused and adequately funded research and development program and should work to ensure that effective mechanisms are in place for the timely transfer of results to the homeland defense effort.

Human and Agricultural Health Systems (Chapter 3)

Just a few individuals with specialized scientific skills and access to a laboratory could inexpensively and easily produce a panoply of lethal biological weapons that might seriously threaten the U.S. population. Moreover, they could manufacture such biological agents with commercially available equipment—that is, equipment that could also be used to make chemicals, pharmaceuticals, foods, or beer—and therefore remain inconspicuous.

The attacks of September 11 and the release of anthrax spores revealed enormous vulnerabilities in the U.S. public-health infrastructure and suggested similar vulnerabilities in the agricultural infrastructure as well. The traditional public health response—surveillance (intelligence), prevention, detection, response, recovery, and attribution—is the paradigm for the national response not only to all forms of terrorism but also to emerging infectious diseases. Thus, investments in research on bioterrorism will have enormous potential for application in the detection, prevention, and treatment of emerging infectious diseases that also are unpredictable and against which we must be prepared.

The deciphering of the human genome sequence and the complete elucidation of numerous pathogen genomes, our rapidly increasing understanding of the molecular mechanisms of pathogenesis and of immune responses, and new strategies for designing drugs and vaccines all offer unprecedented opportunities to use science to counter bioterrorist threats. But these same developments also allow science to be misused to create new agents of mass destruction. Hence the effort to confront bioterrorism must be a global one.

First, new tools for the surveillance, detection, and diagnosis of bioterrorist threat agents should be developed. Knowledge of the genome sequences of major pathogens allows new molecular technologies to be developed for the sensitive detection of pathogens. These technologies offer enormous possibilities for surveillance of infectious agents in our environment, the identification of pathogens, and rapid and accurate diagnoses. For these new technologies to be used effectively to provide early warnings, there is a need to link information from the doctor's office or the hospital's emergency room to city and state departments of health, thereby enabling detection of an outbreak and a rational and effective response. These capabilities will be important both for responding to attacks on agricultural systems (animals and crops) and for protecting humans, and they will require careful evaluation and standards. There is an urgent need for an integrated system to protect our food supply from the farm to the dinner table.

To be able to respond to current and future biological threats, we will need to greatly expand research programs aimed at increasing our knowledge of the pathogenesis of and immune responses to biological infectious agents. The recent anthrax attacks revealed how little is known about many potential biological threats in terms of dose, mechanisms of disease production,

drug targets, and requirements for immunity. It is clear that development of therapeutics and vaccines will require more research on pathogenesis and protective host responses, but financial incentives, indemnification, and regulatory changes may be needed to allow the pharmaceutical industry to pursue such efforts. **Because markets are very limited for vaccines and drugs for countering potential bioterrorist agents, special institutes may have to be established for carrying out research on biohazards and producing drugs and vaccines. The Department of Health and Human Services and the Food and Drug Administration (FDA) should investigate strategies—including the modification of regulatory procedures—to encourage the development of new drugs, vaccines, and devices to address bioterrorist threats.**

Research efforts critical to deterrence, response, and recovery—particularly decontamination and bioterrorism forensics—should be strengthened. Appropriate scientific expertise should be integrated into the government agencies with principal responsibilities for emergency response and postevent investigations. Modeling tools for analyzing the health and economic impacts of bioterrorist attacks are needed in order to anticipate and prepare for these threats. Techniques for protection of individuals and buildings should be developed, together with methods of decontamination in the event that such defenses are breached. In addition, multidisciplinary research in bioterrorism forensics is necessary to enable attribution of a weapon to its source and the identification of persons involved in a bioterrorist act.

Preparedness for bioterrorist attacks should be improved by creating a public-health reserve system and by developing surge capacity to deal effectively with such terrorist attacks as well as with natural catastrophes. Additionally, new strategies must be developed and implemented for assuring the security, usability, and accurate documentation of existing stocks of supplies at research facilities, hospitals, veterinary facilities, and other host sites. The potential for a major infectious threat to kill and disable thousands of citizens requires a level of preparedness that we currently lack—a surge capacity to mobilize the public-health response and provide emergency care in a health system that has been somewhat downsized in an effort to cut costs. There are immediate needs and opportunities for training first responders, medical, nursing, and health professionals, and communities as a whole in how to respond to biological threats. Also needed is a well-trained, professional public-health reserve, including laboratories and health personnel, that can be mobilized. Standardized protocols for such purposes will be critically important.

Toxic Chemicals and Explosive Materials (Chapter 4)

The toxic, explosive, and flammable properties of some chemicals make them potential weapons in the hands of terrorists. Many such chemicals (e.g., chlorine, ammonium nitrate, and petroleum products) are produced, transported,

and used in large quantities. Chemical warfare agents (such as nerve and blister agents) developed to have extremely high toxicities have been incorporated into a variety of military weapons. These chemical weapons could become available to terrorists through purchase or theft. Some of the chemical agents themselves are not difficult for individuals or organized groups to make.

In principle a number of technologies can be brought to bear for the rapid detection and characterization of a chemical attack, or for detecting explosives before they are used. Large investments have been made in research on sensor technologies, but to date the number of effective fielded systems developed remains comparatively small. If sensor research is to move forward efficiently, mechanisms to focus and exploit the highly fragmented array of existing research and development programs will be needed. **A new program should be created to focus and coordinate research and development related to sensors and sensor networks, with an emphasis on the development of fielded systems. This program should build on relevant sensor research under way at agencies throughout the federal government.**

Research programs on sensor technologies are needed to continue the search for promising new principles on which better sensors might be based. For example, mass spectroscopy offers the possibility of very rapid and specific identification of volatile agents. Also, basic research on how animals accomplish both detection and identification of trace chemicals could yield new concepts that allow us to manufacture better sensor systems and reduce our dependence on trained dogs, which currently are the best broad-spectrum high-sensitivity sensory systems.

Toxic chemicals (or infectious agents) could be used by terrorists to contaminate food production facilities or water supplies. Although a good deal of attention has been paid to ensuring safety and purity throughout the various stages of food production, processing, and distribution, protecting the food supply from intentional contamination has not been a major focus of the U.S. food industry. **The FDA should develop criteria for quantifying hazards in order to define the level of risk for various kinds of food-processing facilities.** The results could be used to determine the minimal level of protection required for making each type of facility secure. **The FDA should also act promptly to extend the current quality control approach (Hazard Analysis and Critical Control Point methodology) so that it might be used to deal effectively with deliberate contamination of the food supply.**

One of the best ways to secure the safety of the water supply is to ensure an adequate residual concentration of disinfectant (usually chlorine) downstream of water treatment plants, although more information is needed to be able to do this well. **The Environmental Protection Agency should direct additional research on determining the persistence of pathogens, chemical contaminants, and other toxic materials in public water supplies in the presence of residual chlorine.**

Once a release of toxic chemicals occurs, proper protection of people and buildings can do a great deal to reduce injury and facilitate cleanup and recovery. **Universities, companies, and federal agencies need to work together to advance filtering and decontamination techniques by both improving existing technologies and developing new methods for removing chemical contaminants from air and water.** Research is especially needed on filter systems capable of treating large volumes, novel media that can help prevent toxic materials from entering facilities through ventilation equipment and ducts, and methods to contain and neutralize clouds of airborne toxic materials. In addition, exploratory programs should be initiated in new approaches to decontamination, including hardened structures, protective systems for microelectronics and other expensive equipment, and environmentally acceptable ways of disposing of contaminated material that cannot be cleaned.

New technologies that offer significant advances should be constantly evaluated. But the process of evaluating different sensor systems, for example, is difficult because their effectiveness depends on the operational environment and on who will be using them. **Because a bewildering array of counterterrorism technologies (including various kinds of sensor systems, filters, and decontamination methods) are being developed, programs to determine standards and to support technology testing and performance verification are needed. These programs should be designed both to help guide federal research investments and to advise state and local authorities on the evolving state of the art.**

Information Technology (Chapter 5)

The three counterterrorism-related areas of highest priority in information technology (IT) are information and network security, information technologies for emergency response, and information fusion and management. In particular, immediate actions should be taken on the critical need to improve the telecommunications and computing infrastructure of first responders and to promote the use of best practices in information and network security, especially by emergency response agencies and telecommunications providers.

All of the research areas outlined here and in Chapter 5 are critically relevant to the nation's counterterrorism effort, but it should be noted that progress in them could also be applied to a wide range of other important national endeavors, such as responses to natural disasters.

Attacks on information technology can amplify the impact of physical attacks and diminish the effectiveness of emergency responses. Reducing such vulnerabilities will require major advances in computer security, with the objective of consequently improving information and network security. Furthermore, reliance on the Internet as the primary networking entity means that severe damage through cyberattacks is more likely. **The administration and Congress**

should decide which agency is to be responsible for promoting information security in the federal government through the adoption and use of what is currently known about enhancing security practices. To the extent that the federal government is successful in improving its procedures, it should make these best practices available to other elements of government and to the private sector.

Command, control, communications, and information (C3I) systems for emergency responders are critical for coordinating their efforts and increasing the promptness and effectiveness of response. Unfortunately, such systems are extremely vulnerable to attack; currently many of them do not even use state-of-the-art mechanisms for security and reliability. **Since emergency-response organizations often do not have the expertise to review and revamp the telecommunications and computing technologies used for emergency response, it is necessary to provide them with authoritative knowledge and support. In addition, designated emergency-response agencies should use existing technology to achieve short-term improvements in the telecommunications and computing infrastructure for first responders.**

All phases of counterterrorism efforts require that large amounts of information from many sources be acquired, integrated, and interpreted. Given the range of data sources and data types, the volume of information each source provides, and the difficulty of analyzing partial information from single sources, the timely and insightful use of these inputs is very difficult. Thus, information fusion and management techniques promise to play a central role in the future prevention, detection, and remediation of terrorist acts.

Unlike some other sectors of national importance, information technology is a sector in which the federal government has little leverage. Thus, constructively engaging the private sector by emphasizing market solutions seems a desirable and practical way for the government to stimulate advances that can strengthen the nation's information technology infrastructure. The challenge for federal policy makers is to change the market dynamics by encouraging the private sector to pay more attention to security-related issues and by facilitating the adoption of effective security (e.g., through federally supported or incentivized research that makes better technologies available and reduces the costs of implementing security-related functionality).

Within the federal government, numerous federal agencies, including the Department of Defense (and especially the Defense Advanced Research Projects Agency), the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), and the Department of Energy (DOE) national laboratories, all play important roles in funding and performing telecommunications and computing research, and many other agencies are major users of IT. **A strategic long-term research and development agenda should be established to address three primary counterterrorism-related areas in IT: information and network security, the IT needs of emergency responders, and informa-**

tion fusion. The R&D in information and network security would include but not be limited to approaches and architectures for prevention, identification, and containment of cyberintrusions and recovery from them. The R&D to address IT needs of emergency responders would include but not be limited to ensuring interoper-ability, maintaining and expanding communications capacity in the wake of a terrorist incident, communicating with the public during an emergency, and providing support for decision makers. The R&D in information fusion for the intelligence, law enforcement, and emergency response communities should include but not be limited to data mining, data integration, language technologies, and processing of image and audio data.

The federal government's efforts should focus on multidisciplinary problem-oriented research that is applicable to both civilian and military users, yet is driven by a deep understanding and assessment of vulnerabilities to terrorism. To achieve long-term advances, the research must extend beyond improving existing systems and investigate new approaches to secure and reliable operation that do not directly evolve from the information technology of today.

Energy Systems (Chapter 6)

Energy systems include the country's electrical supply system and its oil and gas facilities. The electrical system warrants special attention in that a prolonged loss of service to a region would probably cause extensive hardships, economic loss, and many deaths. Outage of an entire regional transmission grid might occur if the damage or destruction of important components of that grid were followed by a cascading failure of interconnected components. To reduce near-term vulnerability to such a loss, **those parties responsible for critical components of the electric-power grid should be urged to install physical barriers, where they do not already exist, to protect these components. In the longer term, technology should be developed, tested, and implemented to enable an intelligent, adaptive electric-power grid.** Work under way at the Electric Power Research Institute would provide a basis for such an effort, and the Department of Energy national laboratories would also be key participants in the work. Such an intelligent grid would provide the system with the ability to fail gracefully, minimizing damage to components and enabling more rapid recovery of power. A key element would be adaptive islanding, a concept employing fast-acting sensors and controls to isolate parts of the power system. Operations models and intelligence would be needed to differentiate between failure of a single component and the kind of concurrent or closely coupled serial failures, at several key nodes, that could indicate the onset of a concerted attack.

Another vulnerability of the power grid is its extra-high-voltage transformers, for which the country stocks limited numbers of replacements. Replacement of a seriously damaged or destroyed unit could take months or even years. To counter this vulnerability, **research and development should be undertaken by**

DOE and the electric power industry to determine if a modular, universal, extra-high-voltage transformer might be developed to provide temporary replacement when key components are damaged. These replacement transformers would be relatively small, easily transported, and capable of being used individually or in sets to replicate the unit being replaced.

Yet another challenge is the vulnerability of the power grid's control systems to cyberattack. In particular, the supervisory control and data acquisition (SCADA) systems pose a special problem. As a result, **the manner in which data are transmitted between control points or SCADA systems used in the grid should be reviewed. Encryption techniques, improved firewalls, and cyberintrusion-detection technologies should be used to improve security and reduce the potential for hacking and disruption.** Because oil and gas systems (and nonenergy systems) are similarly vulnerable, this recommendation applies to those facilities as well.

The country's electric-power transmission grids and oil and gas pipelines extend over thousands of miles and in many cases are quite remote, thus complicating observation and supervision. Therefore **existing surveillance technologies developed for defense and intelligence applications should be investigated for their usefulness in defending against terrorist attacks, as well as against simple right-of-way encroachments, on widely distributed oil, gas, and electrical transmission assets.**

The dependence of major infrastructural systems on the continued supply of electrical energy, and of oil and gas, is well recognized. Telecommunications, information technology, and the Internet, as well as food and water supplies, homes, and worksites, are dependent on electricity; numerous commercial and transportation facilities are also dependent on natural gas and refined oil products. These and many other interdependencies need to be better understood in order to determine which nodes of the various energy systems should be given the highest priority for increased security against terrorism. Simulation models of interdependent infrastructures may help provide such understanding and also prove vital to postevent recovery. Therefore new and improved simulation-design tools should be developed to model and analyze prevention, response, and recovery for energy systems under a variety of terrorist-threat scenarios. These efforts would include simulations of the interdependencies between the energy sector and key infrastructures such as the communication, transportation, and water-supply systems.

Transportation Systems (Chapter 7)

Transportation security is best achieved through well-conceived security systems that are integrated with transportation operations. A layered security system, in which multiple security features are connected and provide backup for one another, has particular advantages. Defeating a single layer cannot breach

such systems, and the difficulty of calculating the overall odds of success may thus deter as well as impede terrorist attacks. Moreover, layered security features that are well integrated with operations and confer multiple benefits, such as enhanced safety and operating efficiency, are likely to be maintained and improved over time.

Many actions are now being taken by the federal government to strengthen air transportation security—from the deployment of explosives-detection systems for checked baggage to the strengthening of cockpit doors to the use of air marshals. Some of these measures are providing much-needed security layers, although not yet as part of a preconceived system designed to address multiple threats and ensure continued improvement over time. Likewise, new security approaches are being considered for marine shipping containers, particularly the possibility of moving inspections out from the U.S. ports of entry and farther down the logistics chain. For these two critical parts of the transportation sector well-conceived security systems must be put in place soon, and research and development are essential for further improving these systems.

Many of the areas recommended for R&D in this report—such as improved sensors, the ability to mine data more effectively, and especially a capability for unconventional, broad-based thinking on terrorist threats and responses—will also be of great value in boosting security for transportation and distribution. However, **the most critical need in the transportation sector is a systematic approach to security. The new Transportation Security Administration (TSA) is positioned to help meet this need by serving as a focal point of responsibility for devising effective and coherent security systems for each transportation mode and by supporting and marshaling relevant R&D.** TSA presents an unprecedented opportunity to build security into the nation's transportation sector in a more methodical way; indeed, Congress has chartered TSA to take on such a strategic role.

Compelled to act quickly in enhancing civil aviation security, TSA is now beginning to examine the security needs of all transport modes and to define its own role in meeting them. **To help meet its obligation to strengthen security in all transportation modes, TSA should create a multimodal strategic research and planning office.** Further, to increase the utility of sensing, decontamination, screening, and other security-related technologies being developed, TSA must have its own research capacity as well as the ability to work with and draw on expertise from both inside and outside the transportation community. By working constructively with the Department of Transportation's modal agencies (such as the Federal Aviation Administration and the Federal Highway Administration), other federal entities, state and local government, and the private sector, this recommended office can serve as a focal point for research, planning, and collaboration. It will be positioned to identify and evaluate promising security-system concepts as well as to promote the development of knowledge, technologies, and processes for implementing them.

Within the Department of Transportation, the individual modal agencies and the Volpe National Transportation Systems Center offer important resources for systems-level research and for technology development. TSA can help guide their investments to better leverage the transportation sector's own R&D investments and ensure their strong security relevance. By making the needs and parameters of transportation-security systems more widely known, especially to the much larger R&D community and sponsoring agencies in government, TSA can help to identify and shape the efforts that are most promising and relevant.

Because the identification of appropriate security systems is essential to guiding related technology development and deployment, **TSA should take the lead in devising and evaluating a set of promising security system concepts for each transportation mode.** The diverse operators, users, and overseers in the transportation sector—public and private alike—must ultimately deploy and operate the security systems; however, their disparate venues and interests can hinder cooperation in the development of alternative system concepts. TSA, through the recommended strategic research and planning office, is particularly well placed to encourage and orchestrate such cooperation.

By working with transportation system owners, operators, and users in exploring alternative security concepts, TSA will be better able to identify opportunities for conjoining security with other objectives, such as improving shipment and luggage tracking. Such multiuse, multibenefit systems have a greater chance of being adopted, maintained, and improved.

The agency will also become more sensitive to implementation issues—from technological and economic factors to political and societal challenges—as evaluations help gauge the need for changes in laws, regulations, financial incentives, and divisions of responsibility among public and private entities. Some of these indicated changes may be practical to achieve; others may not. The prospects of deploying many new technologies and processes in support of security systems, from biometric identification cards to cargo- and passenger-screening devices, will also raise many difficult social issues—concerns over legality, personal privacy, and civil rights, for example. Concerns that may constrain or even preclude implementation must be appreciated early on, before significant resources are devoted to furthering impractical or undesirable concepts.

As TSA seeks to develop and deploy security system concepts, consideration of human factors will be critical. Human factors expertise is necessary for crafting layered security systems that, as a whole, increase the perceived risk of getting caught and maximize the ability of security personnel to recognize unusual and suspicious patterns of activity and behavior. **Recognition of human factors is important for ensuring that the role of people in providing security is not determined by default on the basis of what technology promises, but rather as a result of systematic evaluations of human strengths and weaknesses that technology can both complement and supplement. TSA can take the lead in making sure that human factors are fully considered in all security initiatives and at the earliest possible stages.**

Cities and Fixed Infrastructure (Chapter 8)

American cities present a target-rich environment for the terrorist. The urban setting provides access to a set of highly integrated infrastructure systems—such as water, electrical, and gas supplies; communications; and mass transit—as well as to numerous major buildings and places of public assembly.

Major buildings have been recognized as especially attractive targets, and, based on the events of September 11, they have also become the subject of serious structural reexamination—in particular, to determine what weaknesses must be corrected to prevent catastrophic collapse following an attack, as happened with the twin towers of the World Trade Center. Study of the information coming from the failure of those buildings indicates that **research and development leading to improved blast- and fire-resistant designs should be undertaken by NIST, the national laboratories, Underwriters Laboratories, the National Fire Protection Association, and appropriate code-writing organizations. In the near term, while results of this research and development are being realized, provisional guidelines may be issued that are based on the more advanced fire-rating practices now employed in Europe, Australia, and New Zealand.** The results of this work should be disseminated so that new knowledge is incorporated into the codes and standards for the design and construction of new buildings and for remodeling the existing stock as well. Specific testing programs are recommended in Chapter 8, with particular attention given to methods and materials for fire protection and to connections and curtain walls.

Major buildings are also vulnerable to infectious or toxic materials being circulated by heating, ventilation, and air-conditioning (HVAC) systems after their release into the air. To counter this threat, it is necessary that NIST, perhaps together with other agencies and the national laboratories, undertake a research and development program for sensors that can be installed in the air-handling ducts. These sensors could determine whether air is safe or not, and allied controls could adjust the functioning of HVAC systems accordingly.

The heart of a city's response to a terrorist attack is an emergency operations center (EOC) and the first responders—those who are typically dispatched to the scene of a problem before the EOC can determine its nature or cause. **An urgent near-term task is to develop credible terrorist-threat scenarios that EOC teams can prepare to meet. Further, a technical assessment of the adequacy of an EOC's physical facilities to address and survive these threat scenarios should be performed.**

The ability of first responders to quickly determine if the dust and smoke at a site contain toxins will likely mean the difference between life and death. **It is important that research and development be undertaken with the aim of producing new, small, reliable, and quick-reading sensors of toxic materials for use by first responders.** These devices might be based on the same core element as the sensors recommended for HVAC systems.

EOC crisis management teams around the country have had experience in dealing with natural disasters and perhaps some human-made threats (such as riots) to cities, but very few have had any experience in dealing with a terrorist attack. This lack of experience, and the potential problems it implies for attack recognition, response, interagency operations, and public information management and media relations, is a serious vulnerability. **The Office of Homeland Security and the Federal Emergency Management Agency (FEMA), in conjunction with state and local officials, should collaborate to develop and deploy threat-based simulation models and training modules for EOC training, for identification of weaknesses in systems and staff, and for testing and qualifying EOC teams throughout the country.**

The Response of People to Terrorism (Chapter 9)

Most thinking and planning related to preparedness, warning, and response rest on the assumption of an undifferentiated "community" or "public." Research on disasters, however, reveals that individuals and groups differ in both readiness and response according to previous disaster experience, ethnic and minority status, knowledge of the language, level of education, level of economic resources, and gender. In addition, individual households vary in their responses to crises, depending on factors such as perceived risk, credibility of warning system, and concerns about family and property. The behavioral and social sciences can thus make important contributions to understanding group responses to crises. **A program of research should be established to understand how differences based on cultural background, experience with previous disasters, and other factors should be taken into account when systems are designed for preparedness, warning, and response to terrorist attacks and other disaster situations.** A basic research program in the National Science Foundation could build the groundwork for this counterterrorism research.

While research will lay the groundwork for long-term improvements in the quality of preparedness, warning, and response communications, in the near term the government must be preparing now to communicate as best it can in the aftermath of a crisis. **Appropriate and trusted spokespeople should be identified and trained now so that, if a terrorist attack occurs, the government will be prepared to respond not only by supplying emergency services but also by providing important, accurate, and trustworthy information clearly, quickly, and authoritatively.**

To strengthen the government's ability to provide emergency services, in-depth research should be conducted to characterize the structure of agencies responsible for dealing with attacks and other disasters. These studies would focus on discovering optimal patterns of information dissemination and communication among the agencies, the most effective strategies for coordination under

extreme conditions, ways of responding to the need for spontaneous and informal rescues, and approaches to dealing with citizen noncooperation. Research should also focus on the origins and consequences of organizational failure, miscommunication, lack of coordination, and jurisdictional conflict. Comparative work on cases of successful coordination should also be prominent on the research agenda. **The NSF, FEMA, and other agencies should support research—basic, comparative, and applied—on the structure and functioning of agencies responsible for dealing with attacks and other disasters.**

The interface between technology and human behavior is an important subject for investigation. The research agenda should be broad-based, including topics such as decision making that affect the use of detection and prevention technologies; the ways in which deployment of technologies can complement or conflict with the values of privacy and civil liberty; and factors that influence the trustworthiness of individuals in a position to compromise or thwart security. **All the agencies creating technological systems for the support of first responders and other decision makers should base their system designs and user interfaces on the most up-to-date research on human behavior, especially with respect to issues critical to the effectiveness of counterterrorism technologies and systems.**

Complex and Interdependent Systems (Chapter 10)

A major theme of this report is the need for an overall systems approach to counterterrorism. But many of the U.S. government's departments and agencies do not have the capabilities needed to assess terrorist threats, infrastructure vulnerabilities, and mitigation strategies from a systems perspective. For example, **in order to perform the analyses needed to identify vulnerabilities in complex systems and weaknesses due to interconnections between systems, various threat and infrastructure models must be extended or developed and used in combination with intelligence data.** A systems approach is especially necessary for understanding the potential impacts of multiple attacks occurring simultaneously, such as a chemical attack combined with a cyberattack on first responder communications and designed to increase confusion and interfere with the response.

The required range of expertise is very broad. Information about threats must come from communities knowledgeable about chemical, biological, nuclear weapons, and information warfare, while vulnerability analysis will depend on information about critical infrastructures such as the electric-power grid, telecommunications, gas and oil, banking and finance, transportation, water supply, public health services, emergency services, and other major systems. In all these areas **threat assessments and red-team activities will be essential.**

Currently, there is a large volume of information collected and analyzed by the U.S. intelligence community and in industry that is relevant to assessing

terrorist threats and system vulnerabilities. However, to maximize the usefulness of these data and increase the ability to cross-reference and analyze them efficiently, **counterterrorism-related databases will have to be identified and metadata standards for integrating diverse sets of data established.**

Important information about vulnerabilities can also be gained by modeling of critical infrastructures. Computational or physical-analogue models of infrastructure for use in simulating various counterterrorism activities can help with identifying patterns of anomalous behavior, finding weak points in the infrastructure, training personnel, and learning how to maintain continuity of operations following terrorist attacks. **Existing modeling and analysis capabilities, as well as new methods, could allow the use of integrated models to determine linkages and interdependencies between major infrastructure systems.** These results, in turn, could be used to develop sensor-deployment strategies and infrastructure-defense approaches in areas of major vulnerability.

The basic tools of systems analysis and modeling are available today and are widely used in military and industrial applications. But these tools have severe limitations when applied to interdependent complex systems, and research is required to extend them. Thus a long-term research agenda in systems engineering should be established by the federal government. Relevant research projects will involve many domains of expertise; a single disciplinary perspective should not dominate the agenda. Relevant initiatives would focus on the following:

- System-of-systems perspectives for homeland security;
- Agent-based and system-dynamics modeling;
- Analysis of risk assessment and management from multiple perspectives, including the risk of potentially extreme and catastrophic events;
- Modeling of interdependencies among critical infrastructures; and
- Development of simulators and learning environments.

The Significance of Crosscutting Challenges and Technologies (Chapter 11)

The survey of key vulnerabilities and potential solutions outlined above and discussed in greater detail in Chapters 2 to 10 reveals a striking set of crosscutting issues. Apparent in more than one of the areas examined, these issues make it clear that countering terrorism will require insights and approaches that cut across traditional boundaries of scientific and engineering disciplines. Seven crosscutting challenges were identified by the committee: systems analysis, modeling, and simulation; integrated data management; sensors and sensor networks; autonomous mobile robotic technologies; SCADA systems; control of access to physical and information systems using technologies such as biometrics; and human and organizational factors.

Systems analysis and modeling tools are required for threat assessment;

identification of infrastructure vulnerabilities and interdependencies; and planning and decision making (particularly for threat detection, identification, and response coordination). Modeling and simulation also have great value for training first responders and supporting research on preparing for, and responding to, biological, chemical, and other terrorist attacks.

As the intelligence problems prior to September 11 demonstrate, ways to integrate and analyze data are required to support intelligence activities as well as development and use of comprehensive, systems-based defenses for the nation's cities and infrastructures. New data management standards and techniques will also be required.

The development and use of sensors and sensor networks will be critical for the detection of conventional, biological, chemical, nuclear, and information-warfare weapons and means for their delivery. To be effective and acceptable for operational use, these systems must operate at appropriate levels of sensitivity and specificity to balance the danger of false negatives and the disruption caused by false positives.

Continued development and use of robotic platforms will enable the deployment of mobile sensor networks for threat detection and intelligence collection. Robotic technologies can also assist humans in such activities as ordnance disposal, decontamination, debris removal, and firefighting.

SCADA systems are widely used for managing and monitoring most components of the nation's basic infrastructures. Effective security for these systems is not currently well defined, much less implemented.

In many areas, effective security will depend on controlling people's access to physical and information systems while not adversely affecting the performance of these systems. Biometrics is one example of how technology might be used to achieve more effective and less disruptive security systems.

All of the technologies discussed in this report are critically important, but none of them is the sole solution to any problem. Because technologies are implemented and operated by human agents and social organizations, their design and deployment must take human, social, and organizational factors into account.

REALIZING THE POTENTIAL OF SCIENCE AND TECHNOLOGY TO COUNTER CATASTROPHIC TERRORISM

The recommendations offered in this report should not be judged or acted upon individually. It is important instead that the federal government define a coherent overall strategy for protecting the nation, harness the strengths of the U.S. science and engineering communities, and direct them most appropriately toward critical goals, both short term and long. Chapter 12 identifies the steps needed in the federal government (both in the White House and in the agencies that contribute to homeland security) to ensure that today's technological counters

to terrorism are fielded and tomorrow's solutions are found. Chapter 13 describes the important roles of the federal government's partners in homeland security efforts: state and local governments, industry, universities, not-for-profit laboratories and organizations, and other institutions.

Capabilities Needed to Develop a Counterterrorism Strategy and Effectively Deploy Technologies (Chapter 12)

Research performed but not exploited, and technologies invented but not manufactured and deployed, do not help the nation protect itself from the threat of catastrophic terrorism. In this report, the committee urgently recommends a number of steps to ensure that technical opportunities are properly realized. In particular, in recognition of the importance and difficulty of determining goals and priorities, the committee discusses how the federal government might gain access to crucial analytic capabilities to inform decision making—allowing improved assessment of risk and of the effectiveness of measures to counter risk.

Most important is that there be a federal office or agency with central responsibility for homeland security strategy and coordination and that this organization have the structure and framework necessary to bring responsibility, accountability, and resources together to effectively utilize the nation's science and engineering capabilities. The committee believes that the technical capabilities to provide the analysis necessary to support this organization do not currently exist in the government in a unified and comprehensive form. Thus **the committee recommends the creation of a Homeland Security Institute to serve the organization setting priorities for homeland security.**

This institute would provide systems analysis, risk analysis, and simulation and modeling to determine vulnerabilities and the effectiveness of the systems deployed to reduce them; perform sophisticated economic and policy analysis; manage red-teaming activities; facilitate the development of common standards and protocols; provide assistance to agencies in establishing testbeds; design and use metrics to evaluate the effectiveness of homeland security programs; and design and support the conduct of exercises and simulations. The committee believes that to function most efficiently, this institute should be located in a dedicated, not-for-profit, contractor-operated organization.

In the current structure, the primary customer for this Homeland Security Institute would be the Office of Homeland Security, which is currently responsible for producing a national homeland security strategy. Whether this office will also be responsible for monitoring progress on this strategy and revising it in the future is not clear. On June 6, 2002, the President proposed a reorganization in which many of the agencies and programs operating on the front line of counterterrorism would be brought together to form a new Department of Homeland Security. However, even within this department, the programs with the expertise and experience in science and engineering research would not necessar-

ily be closely connected to the units with the responsibility for technology deployment. Perhaps more important, the federal agencies with the best access to the nation's sources of scientific, engineering, and medical research capability lie outside the proposed department, and close connections with these groups will be needed to allow the department to produce the best-quality effort on counterterrorism.

Thus, however the leadership of the federal effort in homeland security is organized, the government will need mechanisms to engage the technical capabilities of the government and the nation's scientific, engineering, and medical communities in pursuit of homeland security goals. Today the focus is on determining these goals, and the link between the Office of Homeland Security and the Office of Science and Technology Policy is a key element in setting the science and technology component of the national counterterrorism strategy. This link will continue to be essential, but if a new department is formed it will not be enough. A new department will need an Undersecretary for Technology to provide a focal point for guiding key research and technology development programs within the department and connecting with relevant technology agencies outside it. In addition, the Office of Homeland Security will need to work closely with the Office of Science and Technology Policy, perhaps through the National Science and Technology Council, on coordinating multiagency projects and their linkages to related programs devoted primarily to other high-priority national objectives.

Essential Partners in a National Strategy: States and Cities, Industry, and Universities (Chapter 14)

The federal government must take the lead in the national counterterrorism effort, but effective use of existing technologies, research and development activities, and deployment of new approaches to mitigating the nation's vulnerabilities will depend critically on close cooperation with other entities: nonfederal governments, industry, universities, not-for-profit laboratories and organizations, and other institutions.

Primary responsibility for response to and recovery from terrorist attacks will fall to cities, counties, and states. The first responders (police, firefighters, and others) and local governments possess practical knowledge about their technological needs and relevant design limitations that should be taken into account in federal efforts to provide new equipment (such as protective gear and sensor systems) and help set standards for performance and interoperability. Federal agencies will have to develop collaborative relationships with local government and national organizations of emergency services providers to facilitate technological improvements and encourage cooperative behavior.

Private companies own many of the critical infrastructures that are targets for

terrorism. Inducing industry to play its critical role in homeland security activities—to invest in systems for reducing their vulnerabilities and to develop and manufacture counterterrorism technologies that may not have robust commercial markets—may require new regulatory requirements, financial incentives, and/or voluntary consensus agreements. A public-private dialogue is required to define the best approach for particular industrial sectors and types of vulnerabilities.

Sustaining a long-term national effort against terrorism will require minimizing the costs of security efforts and avoiding as much as possible placing extra burdens on accustomed conveniences or constraints on civil liberties. Most of the recommendations in this report, if acted on, will not only make the nation safer from terrorist attacks but can also make it safer from natural disasters, infectious diseases, hackers disrupting the Internet, failures in electric power distribution and other complex public services, and human error causing failures in such systems. This promise will help sustain the public's commitment to addressing the terrorism threat, and suggests that it is not inappropriate that many of the research and development programs to counter terrorism should be pursued in close coordination with similar efforts to improve the quality of life in civil society.

Indeed, America's historical strength in science and engineering is perhaps its most critical asset in countering terrorism without degrading our quality of life. It is essential that we balance the short-term investments in technology intended to solve the problems that are defined today with a longer-term program in fundamental science designed to lay foundations for countering future threats that we cannot currently define. These long-term programs must take full advantage of the nation's immense capacity for performing creative basic research, at universities, government laboratories, industrial research facilities, and nongovernmental organizations. A dialogue should take place between the federal government and the research universities on how to balance the protection of information vital to national security with the requirement for the free and open environment in which research is most efficiently and creatively accomplished. This dialogue should take place *before* major policy changes affecting universities are enacted.

The nation's ability to perform the needed short- and long-term research and development rests fundamentally on a strong scientific and engineering workforce. Here there is cause for concern, as the number of American students interested in science and engineering careers is declining, as is support for physical science and engineering research. A dialogue should take place between the federal government and the research universities on how best to reverse this trend in human resources. If the number of qualified foreign students declines, the need to reverse this trend will become even more urgent. The report summarized here focuses almost exclusively on U.S. actions. However, the committee is not suggesting that the United States alone should provide all of the needed counter-

terrorism science and technology. Many other nations are vulnerable to the same terrorist threats, and they have valuable scientific and technical skills to contribute to the mitigation of vulnerabilities. The world will become safer, faster, if the scientific and engineering contributions to counterterrorism are based on cooperative international efforts.

1

Introduction

CONTEXT OF THE STUDY

On September 11, 2001, a complex but ubiquitous technological system—air transport—was transformed into a guided weapon. The targets were elements of the nation's physical infrastructure and icons of the United States: the World Trade Center in New York City and the Pentagon, ordinarily an institution of security and public order. In the anthrax attacks later that month, it was the mail-transport system rather than the air-transport system that provided the means of destruction. In this case, the weapon was a biological agent and the target was the health of various individuals and the well-being and sense of security of the U.S. population as a whole. The perpetrator of the September 11 attacks was not a nation-state but an organization not formally affiliated with any particular country and whose members were mostly non-Americans. The perpetrators of the anthrax attack are unknown at this time, but it is entirely conceivable that a single individual, perhaps an American, was behind it.

One can see in these events two trends, both of them made possible in part by science and technology, that will make terrorism a major threat to 21st-century civilization and an enduring challenge to human ingenuity.

First there is the interconnected, highly technological nature of modern civilization's basic systems. Market forces and a tradition of openness have combined to maximize the efficiency of many of our vital systems—such as those that provide transportation, information technology, energy, and health care. However, economic systems, like ecological systems, tend to become less resilient (more prone to failure when strongly perturbed) as they become more efficient, so our infrastructures are vulnerable to local disruptions, which could

lead to widespread or catastrophic failures. In addition the high level of interconnectedness of these systems means that the abuse, destruction, or interruption of any one of them quickly affects the others. As a result the whole society is vulnerable, with the welfare and even lives of significant portions of the population placed at risk.

Second, as technology advances, the means of mass destruction are falling into the hands of smaller and smaller entities. In the war against terrorism, the enemy may be living among us and is largely unknown, or at least unidentifiable. Today that enemy includes international terrorist organizations such as al Qaeda, operating from overseas bases and supported or protected—and possibly assisted—by a variety of states and independent sources.[1] It also includes homegrown fanatics.

These two trends affect all societies and their increasing vulnerability to terrorism, but the United States has a particular need for protection because its military preeminence makes terrorism virtually the only method by which those who wish to take violent action against it can do so. Moreover, U.S. vulnerability is exacerbated by some of the features that its people most treasure—freedom, personal initiative, openness, mobility—and that technology has helped make possible.

Catastrophic Terrorism

Terrorism—commonly defined as attack on the innocent, outside the context of organized armed conflict, with the objective of spreading fear and intimidation—has always been a danger to society. But what is new and especially troubling about the above two trends is their potential to combine, giving rise to the fearsome risk that the welfare of the many may be held hostage by the few—what this report calls "catastrophic terrorism."

While science and technology can be used to combat all forms of terrorism, this report focuses on catastrophic terrorism. It is not possible to quantify catastrophic terrorism or to precisely distinguish it from "ordinary" terrorism;[2] this

---

[1]Gerald Holton, in a presentation in 1976, identified an emerging combination threat from what he called type III terrorism: nonstate groups of terrorists operating transnationally (type I terrorists) with the financial, logistic, and technical help of failed states (type II terrorists). For this reason it must not be assumed that terrorists will be unable to avail themselves of technologies that require a government level of investment for their development and acquisition ("Reflections on Modern Terrorism," in *Edge*, available online at <http://www.edge.org/3rd_culture/holton/holton_print.html>, and based on a presentation at the Conference on Terrorism (1976) and a publication in *Terrorism: An International Journal* in 1978.)

[2]Terrorism in general is difficult to define. According to the State Department's annual publication *Patterns of Global Terrorism*, "No one definition of terrorism has gained universal acceptance." The State Department uses the definition contained in Title 22 of the United States Code, Section 2656f(d): "The term terrorism means premeditated, politically motivated violence perpetrated against

study generally focuses on terrorist incidents that involve serious consequences measured by both "hard" and "soft" variables. Hard variables quantify large numbers of injuries and deaths and extensive and costly damage to property; soft variables may include widespread disruption of society's key functions, loss of public confidence in government's ability to provide protection against assault, pervasive injury to the population's way of life and overall peace of mind, and erosion of the economic health of the nation.

The anthrax attacks present a vivid illustration of soft variables. While the number of casualties was modest, the emotional, psychological, and economic impacts were enormous. Hard variables, of course, would have made the situation far worse (imagine if the killers had instead chosen to attack with an agent that causes a deadly contagious disease like smallpox). Nonetheless, the cumulative effect on the nation of a systematic series of small but repeated attacks can be significant.

In addition to assessing the consequences of a particular act of terrorism, we must of course also take into account its likelihood; the product of likelihood times severity of consequence helps us determine how much cost and disruption society should accept in the effort to combat it. One indicator of likelihood is the ease with which the act may be accomplished. Does it require many terrorists working together, or will just one person suffice? Does it involve the complicity of an insider—a nuclear reactor operator, say, or a computer network administrator—who is part of the conspiracy? Does the scale of the effort entail a large expenditure of funds, complex organization, or sophisticated technology that only a nation-state or an established terrorist network could assemble? Or is it simple enough that someone could undertake it in his or her garage?

Phases of Response

In responding to the threat of terrorism, the United States needs a multifaceted approach. This includes the following capabilities, organized according to a time line that extends from before a hypothetical terrorist incident to its aftermath:

- *Intelligence and surveillance* involve the observation of persons, groups, and motives—a delicate matter—as well as of potential means of destruction, such as nuclear materials, toxic chemicals, and biological agents.

---

noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience." From p. xvi of *Patterns of Global Terrorism 2001*, released May 21, 2002, and available online at <http://www.state.gov/documents/organization/10319.pdf>. Meanwhile, the Department of Defense defines terrorism as "the calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."

- *Prevention* involves disrupting the terrorists' networks and keeping the means of mass destruction out of the hands of would-be terrorists, as in safeguarding fissile materials or foiling plans for the hijacking of airliners.
- *Protection* is needed should detection and prevention fail. In military parlance, protection means hardening the target so that destruction or disruption becomes more difficult for the terrorist. Examples include technological design and procedures for making borders, buildings, airplanes, and critical infrastructures more difficult to breach, disrupt, or destroy. Protection might also mean the use of vaccination and other public health measures to make people more resistant to disease.
- *Interdiction*, or crisis management, seeks to detect an imminent attack and prevent its occurrence either by disrupting and destroying potential perpetrators of catastrophic terrorism and their base of support before they can mount an attack, as in the current campaign against al Qaeda in Afghanistan, or, when an attack is imminent, by identifying the attackers, preventing their access to the target, or frustrating the attack itself by technical means.
- *Response and recovery*, also called "consequence management," means containing and limiting the level of damage and the number of casualties by organizing emergency responses and public health measures and restoring critical functions in the aftermath of a terrorist attack.
- *Attribution* refers to the ability to identify the perpetrators of an act (by typing an anthrax culture, for example, or performing radiochemical analysis of nuclear bomb debris) and is key to the choice of responses, such as retaliation or prosecution.

In addition, all of these phases benefit from analysis and invention, which involve systematic learning from incidents that do occur, studying terrorist tactics and devising countermeasures through "red team/blue team" exercises,[3] understanding motivations and factors that influence deterrence, and developing systematic plans for ongoing operations, future investments, and scientific and technological innovations.

---

[3]Red teaming and blue teaming are an approach to defining the weaknesses of a system and devising ways to mitigate the resulting vulnerabilities: "The red team tries to devise attack tactics, and the blue team tries to design countermeasures. When the United States developed the first stealth aircraft, for example, the Air Force created a red team to try to detect and shoot them down. When the red team identified a weakness in the stealth design, the blue team was charged to fix it, systematically balancing risk of detection against the cost and inconvenience of countermeasures" (Ashton B. Carter, "The Architecture of Government in the Face of Terrorism," *International Security*, Vol. 26, No. 2, Winter 2001-2002, p. 17).

Science and Technology for Defending the Nation

While the advance of science and technology is one reason why terrorism has the potential to be catastrophic in the 21st century, science and technology are also critical tools for guarding the United States against that threat. Beyond its inherent strengths of immense size and wealth, high level of education, and political cohesion and values, another great comparative advantage of this nation is its scientific and technological prowess. The highly developed, diverse, and productive U.S. science-and-technology enterprise has proved its ability to serve the needs of the nation in a variety of ways: It supplied key military technology for conventional wars and the long Cold War, produced enormous improvements in the health and prosperity of its people, and addressed pressing societal needs such as protection of the environment. Historically, the science and engineering communities have enthusiastically contributed to these national goals, and the same level of energy and commitment will surely be devoted to meeting the vast array of challenges raised by terrorism. Experts from many fields, including physical, biological, and mathematical sciences, engineering, and the social and behavioral sciences, stand ready to create new knowledge that, in turn, creates new capabilities.

Scientists and engineers can put a powerful set of counterterrorism tools at our disposal. But whether, when, where, and how we use these tools will be far from obvious and will require careful thought and analysis. Technologies that protect us may well impose economic, social, and cultural costs that we might not be willing to bear. Sensors, monitors, and intelligence gathering may be intrusive in ways that clash with our values of individual rights and privacy. Protective technologies may be incompatible with the freedom of movement and open access to information that we cherish. In addition, the protection afforded by technology can be overestimated. For these reasons, a careful and realistic evaluation of the performance characteristics of any technology, coupled with systems and risk analyses to determine our level of need for it, is recommended throughout this report.

Science and technology are but one element in a broad array of potential approaches to reducing the threat of terrorism. Diplomacy, international relations, military actions, intelligence gathering, and other instruments of national policy all have critical roles to play. In fact, advanced technologies have long been key to the preeminence of the United States in military affairs. Today, the United States continues to rely on the products of science and engineering—precision munitions, stealth aircraft, and spy satellites, for example—to compensate for an opponent's superior number of soldiers, favorable geographic access to the battlefield, or greater willingness to accept casualties and impose sacrifices on the citizenry. These military applications of science and technology will play an important role in our nation's counterterrorism effort, as can be seen in the ongoing U.S. actions in Afghanistan. However, these applications are being

treated by many other groups, and this report is focused on threats to homeland security, for which a new suite of tools and capabilities will be needed.

In the effort to counter catastrophic terrorism, as in traditional military affairs, science and technology can provide the United States with a critical edge against enemies willing to resort to tactics that our society condemns. The goal would be to create and deploy technical means to reduce the nation's vulnerability while minimizing the kinds of adverse social, political, or psychological responses that would make it a less desirable place in which to live, thereby handing terrorists the ultimate victory. Neither military actions abroad nor the most rigorous homeland defenses can reduce the threat of catastrophic terrorism to zero. But technologies, both those available and those created through new research, can reduce the likelihood of terrorism and the severity of its consequences. Describing how this might be done is the objective of this report.

CONTENT AND STRUCTURE OF THIS REPORT

The purpose of this report is to outline how a response to the threat of catastrophic terrorism that draws on the nation's scientific and technological resources can make the nation safer.

The committee emphasizes the following points:

- It is inherently impossible to defend our nation against all conceivable terrorist threats. Our society is far too complex, too open, and too dependent on interconnected infrastructure and advanced technologies for such a goal to be feasible. Our best long-term strategies for reducing the threats may be diplomatic, military, and economic, but in the short term we must make every effort to protect ourselves as best we can.
- Some already-available technologies can be deployed now, and they could significantly reduce current vulnerabilities. Science and engineering also hold the potential for future inventions and discoveries that could reduce these vulnerabilities further and for addressing yet-to-be-discovered vulnerabilities. Often, these new solutions will require innovative multidisciplinary research and development programs, and many could come from basic research in areas far removed from the problems themselves. Each element of our science and engineering community—government, universities, industry, not-for-profit laboratories and organizations, and other institutions—has important contributions to make in countering terrorism.

The primary focus of the report is the scientific and technological means by which we can reduce the vulnerabilities of our society to terrorist attacks and mitigate the consequences of those attacks when they occur.

Systems and Technologies as Means of Attack, Targets, and Means of Response

Key elements or infrastructures of our society can serve as means of attack, targets, and means of response.

- *Means of attack* include weapons of mass destruction (nuclear, chemical, and biological weapons).
- *Targets* include key systems such as transportation systems and the electric-power grid.
- *Means of response* include critical technologies for responding to attacks, such as telecommunication systems for coordinating the actions of emergency personnel and the public health system for treatment of victims.

While some systems and technologies can be classified roughly in one or another of these categories (i.e., nuclear weapons are primarily means of attack and energy systems are primarily targets), most systems and technologies fall into multiple categories. For example, air transportation is both a target and a means of attack.

This report looks at a collection of systems and infrastructures and in each area focuses on identifying solutions—specific ways of reducing vulnerabilities to catastrophic terrorism—that are achievable through the application of science and technology. The areas are as follows:

- *Nuclear and radiological threats*;
- *Human and agricultural health systems*, including topics such as bio-terrorism, medicine, and public health;
- *Toxic chemicals and explosive materials*;
- *Information technology,* including communications, data management, and identification and authentication systems;
- *Energy systems*, including electrical power systems and oil and natural gas systems;
- *Transportation systems*;
- *Cities and fixed infrastructure,* including buildings;
- *The response of people to terrorism,* including how quality of life and morale of the population can be a target of terrorists and how people respond to terrorist attacks;
- *Complex and interdependent systems,* including linked vulnerabilities, modeling, and simulation. (This category covers the vital interdependencies of different infrastructures. For example, the energy distribution system depends on an IT system to control its functions. Because modeling and simulation are necessary for predicting the responses of society's complex and interrelated infrastructures to terrorist attack, the most important disciplines in this area are systems analysis and systems engineering.)

These systems and infrastructures contribute to society's key functions. For example, emergency services (police, fire, ambulance services) depend on both physical and IT infrastructures. The economy depends on people, finance (IT), energy, transportation and distribution, and other infrastructures. The military relies on people (so biological and behavioral factors come into play), bases (physical infrastructure), and intelligence and command and control systems (IT). The government as a whole, from the President to the departments to the field-level agencies, embraces almost all of the above systems.

Each of the areas in the above list is treated in a separate chapter, along with analyses of vulnerabilities[4] and responses in specific domains (see Box 1.1 for a reader's guide to the report).

These chapters focus on solutions, on ways to harden society against terrorist attacks, to make critical systems more robust and resilient, and to enhance the ability to recover from such attacks. The report also touches on ways in which technical approaches can assist in other aspects of counterterrorism efforts, from supporting intelligence gathering and analysis and providing warning and detection of intent before an attack to conducting forensic investigations afterward. In some cases, the report identifies areas in which existing technologies could be deployed, perhaps after being adapted or extended. In other cases, the report identifies areas in which research could be undertaken to develop new capabilities that might substantially reduce the difficulty of protecting the homeland *in the future*. In both cases, the goal is to use scientific and engineering research and invention to counter terrorism.

The nation must be prepared for a range of contingencies, and the recommended technological responses described by the committee in each area are often quite different. The nuclear threat must be addressed in its earliest stage, when intelligence and international cooperation are most critical. Once terrorists obtain certain nuclear materials, there are limited opportunities for preventing their use. For biological threats, the situation is the reverse: An attack is relatively easy to initiate, but there are many opportunities for technological intervention to mitigate the effects. In some other cases, such as attacks on the electrical power system, it may be possible both to make the attack more difficult and to ameliorate its effects once initiated.

Despite such fundamental differences in the approaches needed for countering different classes of terrorist threats, some general principles and strategies underlie recommendations presented in all of the areas:

[4]The committee was deeply aware of the difficulty of writing a report that was sufficiently specific about terrorist threats to explain how science and engineering might be helpful, yet not providing any information that might aid terrorists in determining new means of attack. In many cases, quite specific information that was available to the committee is presented in the report in a more generic form.

- Identify and repair the weakest links in vulnerable systems and infrastructures;
- Use defenses-in-depth (do not rely only on perimeter defenses or firewalls);
- Use "circuit breakers" to isolate and stabilize failing system elements;
- Build security into basic system designs where possible;
- Build flexibility into systems so that they can be modified to address unforeseen threats;
- Pay attention to the human factors in the design of all systems, particularly those used by first responders; and
- Take advantage of dual-use strategies to reduce vulnerabilities of private-sector targets while enhancing productivity or providing new commercial capabilities.

These general strategies reflect concepts that appear repeatedly throughout this report, in recommendations aimed at different infrastructures and at different phases of prevention and response. In addition to sharing common themes, recommendations in various chapters also repeat some key solutions and programs. There are research and engineering opportunities in crosscutting areas, where new technologies and programs have the potential to mitigate multiple vulnerabilities in different areas. These technologies and programs are described in Chapter 11 and include the following:

- Systems analysis, modeling, and simulation;
- Integrated data management;
- Sensors and sensor networks;
- Autonomous mobile robotic technologies;
- Supervisory control and data acquisition (SCADA) systems;
- Controlling access to physical and information systems using technologies such as biometrics; and
- Human and organizational factors.

Prioritization and Factors Affecting Prioritization

Each of the chapters on society's infrastructures or systems contains a number of recommendations that represent the committee's highest priorities for actions in that area. In addition, in the executive summary, the three or four most important recommendations in each area are summarized, and a list of top short-term actions and long-term research opportunities cutting across all of the areas is provided. However, the final decisions about which measures should be taken first and which programs should be most vigorously pursued will depend on a variety of factors, including the relative likelihood of attacks in each area. The committee did not have access to all relevant information and hence does not claim to offer a definitive prioritization of counterterrorism actions.

BOX 1.1
Reader's Guide to the Report

The list below outlines the structure of the report and lists the topics covered in each chapter. The report includes analyses of vulnerabilities and responses in specific domains (Chapters 2-10) and discussions of general issues affecting the ability to use science and technology for countering terrorism (Chapters 11-13).

Chapter 1 Introduction

- Describes the context of the report and factors that contribute to society's vulnerability to terrorism.
- Provides the committee's working definition for catastrophic terrorism.
- Outlines the structure of the report and describes its scope.

Chapter 2 Nuclear and Radiological Threats

- Outlines the relative threat levels associated with nuclear and radiological weapons.
- Discusses the different issues associated with state-owned nuclear weapons, improvised nuclear devices, and radiological dispersal weapons.
- Explains the methods for control, detection, and interdiction of nuclear weapons and special nuclear materials.

Chapter 3 Human and Agricultural Health Systems

- Explains why new tools need to be developed for surveillance, detection, and diagnosis of bioterrorist agents.
- Outlines the importance of decontamination and bioforensics for responding to attacks.
- Discusses improving models and knowledge of the pathogenesis and genomics of biological agents to facilitate development of therapeutics and vaccines.

Chapter 4 Toxic Chemicals and Explosive Materials

- Outlines how chemicals are used as weapons.
- Discusses ways to mitigate vulnerabilities in a number of areas, including in the production and use of industrial chemicals and in the food, water, and pharmaceutical distribution systems.
- Describes technologies needed to protect from and respond to chemical attacks.

Chapter 5 Information Technology

- Describes IT-only attacks and IT attacks as amplifiers of physical attacks.
- Outlines near-term ways to improve IT security and use IT to respond to an attack.
- Discusses three areas in which IT research investments should be made: information/network security, IT for emergency response, and information fusion.

Chapter 6 Energy Systems

- Covers electric power systems and oil and natural gas systems.
- Describes representative vulnerabilities.
- Suggests how existing technology can be implemented.
- Outlines research and development priorities and strategies.

Chapter 7 Transportation Systems

- Describes transportation system characteristics and their implications for security strategies.
- Discusses research and technology needs.
- Provides advice to the TSA on strategic research and planning.

Chapter 8 Cities and Fixed Infrastructure

- Discusses emergency management and emergency operations centers.
- Discusses water supply and wastewater systems.
- Discusses major and monumental buildings.
- Discusses stadiums and other places for large public gatherings.
- Discusses underground facilities, including tunnels.

Chapter 9 The Response of People to Terrorism

- Outlines how human populations and societies are vulnerable to terrorism.
- Explains factors that contribute to anticipation and preparedness and that influence the effectiveness of warnings.
- Describes the immediate response to the occurrence of attack and the recovery.

Chapter 10 Complex and Interdependent Systems

- Describes how systems analysis and systems engineering should be used in counterterrorism activities.
- Discusses systems management issues, such as governance and decision making, and information systems and tools.
- Explains the importance of threat modeling and infrastructure modeling.

Chapter 11 The Significance of Crosscutting Challenges and Technologies

- Describes seven crosscutting areas where the technologies require multidisciplinary systems approaches or have the potential to reduce vulnerabilities in a variety of domains: systems analysis and modeling; integrated data management; sensors and sensor networks; autonomous mobile robotic technologies; supervisory control and data acquisition (SCADA) systems; biometrics; and human and organizational factors.
- Discusses the need for coordination of programs on crosscutting technologies.

Chapter 12 Equipping the Federal Government to Counter Terrorism

- Discusses issues driving the need for coordination across the federal government.
- Describes the analytic capabilities needed to support OHS.
- Outlines how to strengthen the Office of Science and Technology Policy.
- Illustrates the role of the federal agencies and describes some additional capabilities needed.

Chapter 13 Essential Partners in a National Strategy

- Describes the need for federal agencies to work with states and cities, particularly in technologies for first responders.
- Outlines barriers to and facilitators for the involvement of industry in the development and implementation of counterterrorism technologies.
- Discusses the role of universities, the importance of sustaining the scientific and engineering talent base, and the difficulty in balancing the needs of national security with the requirements for productive and creative research.

A key factor that should affect decisions about counterterrorism priorities is that the nature of the terrorist threats and the targets, weapons, and means of delivery will change over time, often in response to successful countermeasures. Thus it is vital that, as the federal government is setting priorities, decisions be based not only on information about the current threats and ways to limit relevant vulnerabilities but also on an understanding of the impact of deploying proposed protective technologies. To make sound decisions will require threat and risk assessment, systems analysis and engineering, exercises and simulation, red teaming, economic analysis, an understanding of human factors, and other analytic efforts.

Terrorists will adapt to the defenses in place and seek the weakest known spots; overemphasis on particular targets is neither prudent nor desirable.[5] In light of this dynamic nature of the relationship between the threats and the efforts to mitigate vulnerabilities, deployment of new technologies should not be limited to "perfect" systems, but instead should be based on relative effectiveness and advancement of a long-term program to increase the overall security of the system or infrastructure protected. Thus government agencies with homeland security responsibilities will require two capabilities to realize the potential of science and technology. The first is the capacity to use systems engineering and testing to conduct development and procurement of technical systems based on existing technology. The second is the capacity to participate in imaginative research that will produce counterterrorism solutions based on future science and technology.

Realizing the Potential of Science and Technology to Counter Catastrophic Terrorism

This report describes a number of ways in which science and technology could be harnessed to prevent or contain terrorist attacks. Of course, these opportunities are not easily realizable; barriers exist, whether technical or organizational. When they are technical, the committee has recommended research programs designed to develop new capabilities. When possible, the committee has also tried to identify whether a specific government agency has the responsibility for a given area or the capability to lead a given program. When the problem is organizational or institutional, the committee has tried to identify the difficulty (e.g., no government agency has responsibility for the research area in question or no incentives exist for an industry sector to improve its security systems).

However, the recommendations provided in this report should not be judged or acted upon individually. Instead, the federal government needs to define a coherent overall strategy for protecting the nation and should harness the strengths

[5]If the United States invests in hardening security in all airports, for example, terrorists will obviously know this and will likely attack other, less protected targets instead.

of the U.S. science and engineering communities and direct them most appropriately toward critical goals, both short term and long.[6] This task will require an overall investment and research plan, appropriate institutional structures for research on future solutions and for engineering and procuring solutions that are technologically mature, funding allocations that fairly distribute the costs of counterterrorism protections across society, and a renewed population of talented young scientists and engineers to work on these problems. Chapter 12 identifies the steps needed in the federal government (both in the White House and in the agencies that contribute to homeland security) to ensure that today's technological counters to terrorism are fielded and tomorrow's solutions are found. In particular, in recognition of the importance and difficulty of determining goals and priorities, the committee discusses how the federal government might gain access to crucial analytic capabilities to inform decision making and assess risk and the effectiveness of measures to counter that risk.

The proposed budget for federal spending on homeland security programs in fiscal year 2003 is approximately $38 billion,[7] of which less than 10 percent is estimated to be for research and development.[8] While these resources will make a significant difference, they do represent strictly the efforts of the federal government. Yet however well the federal government organizes its own effort in homeland security, the overall national effort cannot succeed without critical contributions from other institutions. Essential partners in utilizing science and technology for countering terrorism will include nonfederal governments (states, counties, and cities), industry, universities, nongovernmental organizations, professional societies, and many other groups. While the bulk of this report is directed toward the federal government and actions it can take, all of these other institutions have vital contributions to make. In Chapter 13, the committee

---

[6]The committee recognizes, and has been greatly informed by, a number of excellent reports published in recent years that anticipated terrorism directed at our homeland and discussed the role of science and technology in countering such terrorism. Among them were reports by the Gilmore Commission, the Bremer Commission, the Hart/Rudman Commission, and the Marsh Commission (see the references for Chapter 12). While the present report is distinct in its scope and in its attempt to integrate science-based responses to terrorism across many disciplines, it is consistent with these earlier studies in its characterization of the country's primary areas of vulnerability and the need to strengthen the federal government's ability to address them.

[7]Of the $38 billion, $21 billion is focused on four missions: ensuring that state and local first responders (firefighters, police, and rescue workers) are prepared for terrorism; enhancing our defenses against biological attacks; securing our borders; and sharing information and using information technology to secure the homeland (*Fiscal Year 2003 Budget of the U.S. Government,* U.S. Government Printing Office, Washington, 2002, p. 17. White House budget documents are available online at <http://www.whitehouse.gov/omb/budget>).

[8]Exact figures are not available but estimates by Kei Koizumi of the American Association for the Advancement of Science predict approximately $2.8 billion for R&D in the FY 2003 counterterrorism budget (personal communication, June 11, 2002).

describes briefly the importance of these partners' roles and touches on some of the issues related to the federal government's ability to productively interact with these groups.

State and local governments have critical responsibilities in homeland security because terrorist incidents are likely to affect first and foremost a particular locality in which a target is located, and the police, fire, emergency management, and other public officials there will be the first on the scene. However, it is not possible for each locality to develop its own comprehensive response to the possibility of terrorism or to engineer protective systems, let alone to conduct research on new techniques and technology. Creating common solutions to counterterrorism challenges, and providing the needed knowledge and engineering base, will therefore fall to the federal government. But the federal government's efforts will be useless unless the design of standards and the development of procedures are informed by the experience and insight of the first responders. Also, the results of the federal programs must then be made available to state and local authorities, directly or through their collective bodies such as police and fire associations.

Industry, too, has crucial contributions to make to increasing homeland security. Many critical infrastructures are largely owned and operated by the private sector, not the government. Much of the needed investment and adaptation to protect these infrastructures will have to be made by private companies. The funds for these investments will come from some mixture of funds provided by the federal government and funds provided by the companies themselves. The private sector's own investments will arise in several ways—for instance, because they are mandated by law or regulation, because incentives are provided (e.g., tax relief), because insurance companies require them, or because competitive business practice recommends them. In any case, it is important that these investments be made in a manner that fully realizes the potential of science and technology to provide solutions. Moreover, since much of the relevant technical expertise about these critical infrastructures resides in the private parties that operate them, it is essential that these parties participate directly in devising solutions to vulnerabilities.

Finally, this report amply demonstrates that America's strength in science and technology is perhaps its most critical asset in countering terrorism without degrading our quality of life. Terrorism is a threat to U.S. security for the foreseeable future, and as our defenses improve, terrorists' abilities to circumvent them will also improve. It is essential that we balance the short-term investments in technology intended to solve the problems that are defined today with a longer-term program in fundamental science designed to lay foundations for countering future threats that we cannot currently define. These long-term programs must involve the nation's immense capacity for performing creative basic research, at universities, government laboratories, industrial research facilities, and nongovernmental organizations.

2

Nuclear and Radiological Threats

THE NUCLEAR AND RADIOLOGICAL THREAT MATRIX

For the purposes of the following discussion, the threats to homeland security from nuclear and radiological terrorism are grouped into the following three categories:

1. *Stolen state-owned nuclear weapons or weapons components,* modified as necessary to permit terrorist use.
2. *Improvised nuclear devices* (INDs) fabricated from stolen or diverted special nuclear material (SNM)[1]—plutonium and, especially, highly enriched uranium (HEU).[2]
3. Attacks on *nuclear reactors* or *spent nuclear fuel* or attacks involving *radiological devices*.

The threat matrix is summarized in Table 2.1 and is discussed in more detail below.

State-Owned Nuclear Weapons or Weapons Components

Several countries possess nuclear weapons that could potentially be turned to terrorist use: Britain, China, France, India, Israel, Pakistan, Russia, and the United States. Other countries have had weapons development programs in the past, and

[1]Special nuclear material includes fissile isotopes such as uranium-233, uranium-235, and plutonium-239 that can be used to make nuclear weapons.

[2]HEU contains ≥20 percent by weight of uranium-235.

one of these (South Africa's) led to the development of nuclear weapons. Iran, Iraq, and North Korea are believed to have active weapons development programs at present, and these countries probably have the technical capabilities to develop nuclear weapons but may not have sufficient quantities of SNM (plutonium or HEU).

The weapons arsenals of Britain, China, France, Israel, and the United States are probably well protected. Indian and Pakistani nuclear weapons are also thought to be adequately protected at present, but the near-term (1- to 5-year) security of Pakistani weapons may be problematical. Theft or diversion of Russian nuclear weapons for terrorist use may represent a significant near-term threat to the United States, especially the theft or diversion of smaller, man-portable weapons. Table 2.1 and the classified annex provide additional details on these threats.[3]

Improvised Nuclear Devices

Improvised nuclear devices are nuclear weapons fabricated by terrorists, with or without state assistance, using stolen or diverted SNM. The basic technical information needed to construct a workable nuclear device is readily available in the open literature. The primary impediment that prevents countries or technically competent terrorist groups from developing nuclear weapons is the availability of SNM, especially HEU.

HEU could potentially be obtained by terrorists from several sources. There are large stockpiles of excess HEU and weapons-grade plutonium in both the United States and Russia, and other countries with nuclear weapons may have smaller stockpiles of these materials. HEU also exists in nuclear fuel from naval reactors, and large stocks of reactor-grade plutonium are contained in commercial spent fuel. Spent-fuel reprocessing programs and separated stocks of reactor-grade plutonium also exist in several countries, and these stocks are routinely transported across national borders. Reactor-grade plutonium can be used to fabricate workable nuclear devices.

Theft or diversion of excess Russian HEU for terrorist use represents a significant near-term threat to the United States. There are estimated to be about 150 metric tons of separated plutonium and 1,200 metric tons of HEU in Russia. The United States has been working with Russia over the past 7 years to secure this material and has made major progress. These safeguards are effective against casual thefts but may not be effective against higher-level threats, especially sophisticated insider threats. Moreover, a complete inventory of Russian materials is not available, so it is impossible to confirm that diversions of materials have

[3]In addition to the unclassified discussion of nuclear and radiological terrorism provided in this chapter, a classified annex containing further treatment of these topics has been produced by the study.

not already occurred. Additionally, there have been more than a dozen seizures of SNM from Russia and surrounding countries since the early 1990s. Most of the seized materials are thought to have been smuggled from Russian civilian nuclear sites.

Stocks of SNM also could be produced clandestinely, either through enrichment of uranium or reprocessing of spent nuclear fuel to recover plutonium. Uranium enrichment is equipment intensive and time consuming, and detection is increasingly likely as the scale of operations is increased. A small-scale program could potentially be hidden through careful facility design, however, and could, in principle, produce sufficient material for a weapon if operated for several years. Reprocessing to recover plutonium also can be carried out in small, difficult-to-detect facilities but requires access to irradiated reactor fuel. Any country with a research reactor has potential access to such fuel, and there are, in addition, large stocks of spent fuel in power reactors in countries of the former Soviet Union and also in foreign research reactors, some of which still operate with HEU. Clandestine production of SNM by states or terrorist groups for use against the United States represents a significant near-term threat to homeland security.

Nuclear Reactors, Spent Nuclear Fuel, or Radiological Dispersion Devices

The threats considered here include attacks on nuclear power plants (both commercial nuclear power plants (NPPs) and research reactors), their spent fuel storage facilities, and spent fuel transportation casks; detonation of conventional explosive devices packed with radioactive materials, so-called "dirty bombs;" and the surreptitious placement of radiation sources in places frequented by large numbers of the public. Attacks on DOE-owned nuclear facilities were not considered because these are generally considered to be hardened and well protected.

Nuclear Power Plants

The United States has 103 operating civilian nuclear power reactors at 65 sites that generate about 20 percent of the U.S. electrical supply (USNRC, 2002; EIA, 2002). The U.S. Nuclear Regulatory Commission (USNRC) regulates NPPs and has had a long-standing concern about security and safeguards. The agency's security and safeguards regulations are extensive and actively enforced.

The USNRC requires that NPPs be protected against a "design basis threat," defined at present to involve a ground attack by a group consisting of several armed terrorists aided by an inside collaborator.[4] NPPs are required to train their

[4]Additionally, some NPPs located near airports have been designed to withstand certain types of low-speed takeoff and landing accidents involving aircraft in common use when the plants were licensed in the 1970s.

TABLE 2.1 The Nuclear and Radiological Threat Matrix

TABLE 2.1A State-Owned Nuclear Weapons

Threat Category	Threat Description	Threat Level	Potential Consequences	Probability of Occurrer
State-owned nuclear weapons	Theft and diversion of state-owned nuclear weapons for use, with or without modification, against U.S. targets or assets	United States: Low—weapons are well protected and tactical weapons have integrated permissive action links to prevent unauthorized use Britain, China, France, Israel: Low—weapons are few in number relative to U.S.-Russian arsenals and are well protected Pakistan, India: Medium—weapons are under secure control of the military, but political situation is unstable Russia: Medium—large numbers of weapons with poor inventory controls	Potentially catastrophic—massive loss of life and severe political and economic destruction possible	Moderate c 5 years, wi potential fo

security personnel against this threat and are periodically tested by the USNRC to ensure readiness to meet this threat.

The current design basis threat for NPPs does not include high-speed attacks with fully loaded civilian airliners or, alternatively, smaller general aviation aircraft loaded with high explosives (HE) or attacks from the ground using HE projectiles. Potential targets for aircraft or ground attacks against an NPP are described in the classified annex.

The USNRC is supporting work at the Sandia National Laboratories, and the nuclear industry's trade association, the Nuclear Energy Institute (NEI), is directing work at the Electric Power Research Institute (EPRI) to assess some of these threats. These studies, which involve modeling aircraft impacts against steel-reinforced concrete structures and investigating the potential effects of aircraft-fuel fires, are proceeding independently of each other and will not be completed until after this report is published.

The details of these studies are classified and/or sensitive, and the results are

ces	Probability of Occurrence	Technical and Policy Challenges	Approaches to Mitigation
ic— ss of life political mic possible	Moderate over the next 5 years, with a high potential for surprise	Theft or diversion may not require state assistance and may go undetected if theft occurs in Russia Stolen or diverted weapons could be converted for terrorist use HEU-based weapons smuggled into the United States could be difficult to detect and recover First responders may be killed or incapacitated by attack	Improve indications and warnings capabilities Improve security of Russian and Pakistani nuclear weapons at storage sites and borders Accelerate deployment of sensor arrays at critical U.S. entry points and targets Develop and announce policies to deter use of weapons by terrorist states Improve attribution capabilities

preliminary. But taken together, these studies suggest that a terrorist attack on an NPP could have potentially severe consequences if the attack were large enough. The severity is highly dependent on the specific design configuration of the NPP, including details such as the location of specific safety equipment. Additional details are provided in the classified annex.

The potential vulnerabilities of NPPs to terrorist attack seem to have captured the imagination of the public and the media, perhaps because of a perception that a successful attack could harm large populations and have severe economic and environmental consequences. There are, however, many other types of large industrial facilities that are potentially vulnerable to attack, for example, petroleum refineries, chemical plants, and oil and liquefied natural gas supertankers. These facilities do not have the robust construction and security features characteristic of NPPs, and many are located near highly populated urban areas. The committee has not performed a detailed examination of the vulnerabilities of these other types of industrial facilities and does not know how they compare to

TABLE 2.1B Improvised Nuclear Devices

Threat Category	Threat Description	Threat Level	Potential Consequences	Probability of Occurrer
Improvised nuclear devices	Theft or diversion of SNM for fabrication of nuclear devices for use against U.S.targets or assets	United States: Low—SNM is well protected Britain, China, France, India, Israel, Pakistan: Low—small amounts of materials are well protected Russia: High—large inventories of SNM are stored at many sites that apparently lack inventory controls ,and indigenous threats have increased	Potentially catastrophic—massive loss of life and severe political and economic destruction possible	Moderate 5 years, w potential f

the vulnerabilities of NPPs. It is not clear whether the vulnerabilities of NPPs constitute a higher risk to society than the vulnerabilities of other industrial facilities.

Research Reactors

Research reactors are used primarily to produce neutrons and gamma rays for research and development, and they provide a testbed for education on reactor physics and operations. As of April 2002 there were 36 operating research reactors in 23 states, an additional 12 reactors were being decommissioned, and 7 had licenses only to possess radioactive material.[5] Most research reactors are

[5]Much of the factual information used in this section is taken from the USNRC Web site. See, particularly, <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/research-reactors.html>, last accessed May 20, 2002.

ces	Probability of Occurrence	Technical and Policy Challenges	Approaches to Mitigation
ic— ss of life political mic possible	Moderate over the next 5 years, with a high potential for surprise	Theft or diversion may not require state assistance and may go undetected Crude HEU weapons could be fabricated without state assistance HEU-based INDs smuggled into the United States could be difficult to detect and recover First responders may be killed or incapacitated by attack	Improve indications and warnings capabilities Consolidate SNM at Russian sites, improve inventory controls, and improve security at sites and borders Accelerate blend-down of Russian HEU Accelerate the development and deployment of SNM sensor arrays at critical U.S. entry points and targets Improve capabilities for remote detection of HEU Develop and announce policies to deter use of INDs by terrorist- states Improve attribution capabilities

located at universities or government laboratories,[6] and many university research reactors operate on a restricted basis and therefore do not generate much radioactive material.

With thermal outputs ranging from about 0.1 to 20 megawatts, U.S. research reactors produce much less radiation, heat, and waste (e.g., spent fuel) than do power reactors, whose thermal output is commonly 2,000-3,000 megawatts. Research reactors also generally have fail-safe shutdown systems, and most do not generate sufficient heat to be vulnerable to core accidents, even in the event of a coolant loss. The potential consequences of terrorist attacks therefore appear to be small relative to power reactors.

[6]In addition, the Department of Energy and the U.S. Army operate research and test reactors at several of their sites. The thermal output of these reactors ranges from 5 to 400 megawatts. These reactors are not licensed by the USNRC and are not considered in this discussion.

TABLE 2.1C Radiological Attacks

Threat Category	Threat Description	Threat Level	Potential Consequences	Probability of Occurrer
Nuclear power plants (NPPs)	Ground or air assaults on civilian NPPs	High—Over 100 potential targets exist in the United States	Variable, ranging from reactor shutdowns to core meltdowns with very large releases of radioactivity	Potential f attacks is l near term
Research reactors	Ground or air assaults	High—there are 36 operating reactors	Little or no release of radioactivity likely	Unclear in
Spent nuclear fuel in wet or dry storage	Ground or air assaults on spent fuel pools or dry storage casks	High—Potential targets exist at all commercial NPP sites	Little or no release of radioactivity likely	Potential f attacks is l next 5 yea would be c locate or s damage
Radiological sources	Attacks with dirty bombs or placement of radioactive sources in public places	Very high—radiation sources are numerous and highly dispersed worldwide	Few deaths likely, but potential for economic disruption and panic is high	High—mat means are available, a few preven in place
Radioactive waste	Same as for radiological sources	Very high—radioactive waste is abundant worldwide and not well protected	Trivial—most types of radioactive waste potentially available to terrorists have low specific activity	High—mat means are available, a few preven in place

Spent Nuclear Fuel in Wet or Dry Storage

All civilian NPPs contain storage facilities for spent nuclear fuel and, with few exceptions, all of the spent fuel produced by those reactors is being stored at the sites where it was produced. Approximately 42,000 metric tons of spent fuel are currently stored under water in large spent fuel storage pools for cooling and shielding purposes. These pools are constructed of steel-reinforced concrete and are typically located adjacent to reactor containment buildings.

At some NPP sites spent nuclear fuel also is being stored outside the power-plant buildings in dry casks on concrete pads. At present, about 3,000 metric tons of spent fuel are being stored in this fashion. The casks are constructed of one or more layers of stainless steel and steel-reinforced concrete. The spent fuel is stored in the casks in an inert atmosphere at low pressure. A consortium of

ces	Probability of Occurrence	Technical and Policy Challenges	Approaches to Mitigation
ranging or to core with very ses of ty	Potential for 9/11-type attacks is high in the near term	Stopping airplane attacks that deliver large amounts of energy directly on target	Perform vulnerability analysis of NPPs Harden vulnerable NPPs and improve redundancies of critical safety systems
o release of ty likely	Unclear in the near term	Providing security against all types of attacks	Minimize the amount of fuel stored onsite
o release of ty likely	Potential for 9/11-type attacks is high over the next 5 years, but targets would be difficult to locate or severely damage	Stopping airplane attacks that deliver large amounts of energy directly on target	Perform vulnerability analysis of spent nuclear fuel storage sites Move vulnerable spent fuel in wet storage to dry cask storage
s likely, ial for disruption is high	High—materials and means are readily available, and there are few preventive measures in place	Training first responders to deal with these types of attacks	Improve first responder capabilities Improve public education
ost types tive waste available s have ic activity	High—materials and means are readily available, and there are few preventive measures in place	Training first responders to deal with these types of attacks	Improve first responder capabilities Improve public education

nuclear utility companies has applied to the USNRC for a license to construct a centralized dry-cask storage facility (the Private Fuel Storage Facility) in Utah west of Salt Lake City. This facility, if licensed and constructed, could house up to 40,000 metric tons of spent fuel contained in up to 4,000 above-ground storage casks on thick reinforced-concrete pads (Private Fuel Storage, 2002).

The threat of terrorist attacks on spent fuel storage facilities, like reactors, is highly dependent on design characteristics. Moreover, spent fuel generates orders of magnitude less heat than an operating reactor, so that emergency cooling of the fuel in the case of attack could probably be accomplished using low-tech measures that could be implemented without significant exposure of workers to radiation. Dry cask storage systems are very robust and would probably stand up to aircraft attacks as well.

Like dry storage casks, spent fuel transport containers are very robust and appear to offer similar protection against terrorist attack. Studies on the vulnerability of spent fuel transport containers to sabotage suggest that relatively little or no radioactivity would be released in the event of a terrorist attack, and the USNRC is now undertaking a package performance study that will examine fuel performance and source terms under a variety of impact situations. That agency is conducting a top-to-bottom review of potential vulnerabilities, including transport vulnerabilities, in the wake of September 11. In the meantime, it has issued advisories to its licensees to take additional precautions until these reviews are completed.

Radiation Sources and Radioactive Waste

A wide variety of radiation sources are used in the civilian economy for, among other things, industrial radiography, radiation therapy, university research, and natural resource exploration. The approximately 2 million sources licensed by the USNRC range in activity from millicuries to tens of kilocuries and typically contain penetrating gamma emitters like cesium-137, cobalt-60, and iridium-192; alpha emitters like radium-226 and americium-241; and beta emitters like strontium-90. Devices in which such sources are dispersed by explosives or other means are called radiological dispersion devices (RDDs).

In the United States, most radioactive sources are regulated by the USNRC or by states under agreement with that agency, and a materials license is required to possess such sources. Licensees are responsible for safeguarding these sources and returning them to the manufacturer or properly disposing of them when the sources are no longer needed. This system is not foolproof, however. For example, according to USNRC records, several hundred U.S. sources are unaccounted for and presumed lost.

Radioactive sources are also used widely in other countries, not all of which have the regulatory controls that exist in the United States. Control of sources may be a particular concern in some central and eastern European countries, which lack strong regulatory or accounting standards.[7]

The United States also produces quantities of radioactive waste that could potentially be used in an RDD. This waste includes high-level spent nuclear fuel and high-level defense waste stored at government or commercial sites; transuranic waste stored at government sites; and low-level industrial, research, and medical waste stored at commercial sites, universities, and hospitals. Low-level waste may be a particularly attractive terrorist target: It is produced by many companies, universities, and hospitals, it is not always stored or shipped under tight security, and it is routinely shipped across the country. Although labeled

[7]See Gonzalez (1999) for a recent review of lost and stolen radioactive sources.

"low-level," some of this waste has high levels of radioactivity and could potentially be used to make an effective terrorism device.

RDD attacks could be carried out in several ways. Nonexplosive sources could be hidden in facilities frequented by large numbers of the public (e.g., sports stadiums, subway systems) or dispersed in building ventilation systems. Additionally, a radiation source could be combined with an explosive to disperse radioactive contamination over areas on the order of hundreds of square meters to a few square kilometers, depending on meteorological conditions. A radioactive waste shipment also could be attacked while in transit. Although such an attack probably would not disperse large quantities of radioactivity, it could cause public panic, especially if the attack took place in a highly populated urban area.

Detailed studies of RDDs suggest that few if any human deaths would be expected from dispersed radiation, although the explosion itself could cause casualties. The presence of dispersed radioactivity in the attacked area could, however, confound rescue efforts. The most severe effects on human health are produced if the material can be efficiently dispersed in respirable form. For optimum particulate sizes, inhaled material can remain lodged in the lungs, leading to either acute or chronic effects, depending on the amount and type of material respired. Although there are methods to construct an RDD to obtain good dispersion of inhalable particles, they require expert knowledge and access to university-level laboratory facilities.

HOMELAND SECURITY CHALLENGES

The threat matrix presented in Table 2.1 and discussed in previous sections suggests that the United States faces several near-term (1-5 year) vulnerabilities to terrorist acts using nuclear and radiological dispersal weapons. Several potential vulnerabilities are described in this section.

State-Owned Nuclear Weapons and Improvised Nuclear Devices

At present, the United States has no evidence that a terrorist organization or nonnuclear state possesses stolen nuclear weapons or INDs. However, this situation could change rapidly over the near term if steps are not taken to better secure nuclear weapons and SNM, especially in Russia. In the future, efforts to develop INDs may involve virtual collaborations among groups of countries and terrorist organizations. These efforts will be harder to detect and interdict because the different materials, facilities, activities, and expertise will be spread across large and unconnected geographical areas. As noted above, the primary impediment to the success of IND development efforts is the availability of SNM, especially HEU. The first challenge, then, for the United States and its allies is to improve security for weapons and special nuclear material wherever they exist, but especially in Russia.

Once a terrorist state or organization is able to procure a state-owned nuclear weapon or SNM, especially HEU, it will be able to fabricate an IND if it has the appropriate technical expertise. In addition to the potential for obtaining SNM from existing stocks in countries like Russia, the technologies for making SNM are ubiquitous, and past experiences, which are discussed in the classified annex, illustrate the difficulty of detecting well-concealed clandestine efforts to produce these materials. Therefore, the second challenge for the United States and its allies is to improve the gathering of indications-and-warnings intelligence on efforts by states or groups to obtain a nuclear capability so that resources can be focused on countering the most significant threats. The third challenge is to improve capabilities for detecting and interdicting stolen nuclear weapons and INDs once they are obtained by a terrorist group or state.

The consequences of terrorist use of a stolen weapon or IND are horrible to contemplate. A successful detonation of a stolen weapon or IND could produce massive casualties and cause substantial damage to the nation's political and economic infrastructure. Although recovery would eventually occur, it would be both expensive and lengthy. While recovery plans should be put into place to deal with such attacks, the main focus of the nation's efforts must be on prevention of attacks by whatever means possible.

Nuclear Reactors, Spent Nuclear Fuel, and Radiological Dispersion Devices

Nuclear power plants may present a tempting high-visibility target for terrorist attack, and the potential for a September 11-type surprise attack in the near term using U.S. assets such as airplanes appears to be high. Such attacks could potentially have severe consequences if the attack were large enough and, were such an attack successfully carried out, could do great harm to the nation's near-term energy security and civilian nuclear power as a long-term energy option.

Complete denial of the means to attack NPPs from the air or ground using U.S. assets such as aircraft is probably not feasible. If important vulnerabilities are identified, however, design and operational fixes exist, some of which are easily identifiable, that could substantially harden the facilities. Some of these possible fixes are discussed in the classified annex.

The private ownership and operation of NPPs present some additional challenges. One involves cost, and another information sharing. Private companies may be hesitant to commit significant resources to reducing vulnerabilities unless they receive clear guidance and leadership from the USNRC. Further, operators may be unable to pass such costs on to consumers in a highly competitive electricity market. This has important ramifications for nuclear energy as a long-term contributor to the U.S. energy supply. Information sharing between government agencies and plant owners and operators on potential vulnerabilities and operational fixes is essential for improving security at the nation's NPPs. Such infor-

mation sharing is currently problematical, however, because much of the information to be shared is classified.

Of course, the development of remedies for reducing potential NPP vulnerabilities to terrorist attack must consider both *costs* and *achieved risk reductions*, especially in view of the potential vulnerabilities of other types of industrial facilities, as discussed elsewhere in this chapter. The nation's resources to address these vulnerabilities are limited and thus have to be expended in a way that achieves the greatest risk reduction at the lowest overall cost to society.

Given the wide use of radiation sources in the United States and other countries, a determined terrorist would probably have little trouble obtaining material for use in an RDD. Fortunately, many radiation sources are strong gamma emitters and, unless heavily shielded, can be readily detected with existing sensor technologies. If an RDD attack were to occur, the casualty rate would likely be low, and contamination could be detected and removed from the environment, although such cleanup would probably be expensive and time consuming.

It is clear that the aim of an RDD attack would be to spread fear and panic and to cause as much disruption to society as possible. Given the public fear of anything "nuclear" or "radioactive," even a minor terrorist attack could have greatly magnified psychological and economic consequences. The ease of recovery from an RDD attack would depend to a great extent on how the attack was handled by first responders, political leaders, and the news media, all of which would help to shape public opinion and reactions.

REDUCING VULNERABILITIES

Several steps can be taken over the near term to reduce the nation's vulnerability to acts of nuclear and radiological terror. Science and technology have an important role to play in this effort but clearly are insufficient in themselves to meet the future challenges. Policy and procedural changes may also be required, as described in the following discussion.

Stolen Nuclear Weapons and Improvised Nuclear Devices

There are no obvious technological silver bullets to reduce the nation's vulnerability to terrorist use of stolen nuclear weapons or INDs. Nevertheless, science and technology can play a central role in an *enduring, multilayered homeland-defense system* that provides for the following capabilities:

- Indications and warnings of terrorist group membership, structure, intentions, and transformational activities;
- Accounting of and security for weapons and SNM inventories at their sources;

- Detection and interdiction, using technology and intelligence, of weapons and SNM moved across national borders, especially Russian and U.S. borders;
- Detection of weapon or IND movements inside the United States;
- Effective responses to nuclear and radiological attacks if they do occur; and
- Attribution to identify weapons and/or SNM characteristics and sources of origin.

Such a system must be structured to overcome the political inertia that inevitably develops over time and that can lead to a slackening of effort. A good example of such inertia is the federal government's reduced willingness to provide funding during the last decade to the Federal Aviation Administration (FAA) for air marshals to guard commercial flights against hijackers. It appears that the FAA's effectiveness in reducing airline hijackings through the 1980s led to a perception that the risk of hijacking no longer existed.

Protection, Control, and Accounting of Nuclear Weapons and Special Nuclear Material

Nuclear weapons and SNM can be most effectively protected, controlled, and accounted for at their sources, which are relatively few in number compared with the many potential points of transit across national borders and are protected by state-run security infrastructures. Therefore, the first line of homeland defense against nuclear and radiological terrorism is a robust system for protecting, controlling, and accounting for nuclear weapons and SNM at their sources.

Technology for weapons and SNM protection, control, and accounting already exists and has been deployed in many nuclear countries. The impediments to more widespread deployment of these technologies in nuclear weapons and SNM states include cultural differences over what constitutes workable and acceptable technologies; funding for procurement, training, and security screening of the necessary personnel; and the willingness of states to accept and deploy such systems.

Of particular concern is the deployment of these systems in Russia, which possesses large stockpiles of weapons and SNM, and Pakistan, whose weapons are controlled in a fashion that may be unpredictable, especially given the potentially unstable governmental situation. The United States can—and should—engage nuclear weapons states, states possessing SNM, and the International Atomic Energy Agency (IAEA) in bilateral and multilateral discussions aimed at improving the protection, control of, and accounting for weapons and SNM. To this end, the following four actions should be taken:

Recommendation 2.1: The U.S. government, working through the Department of Energy, Department of Defense, and Department of State, should

increase the urgency and pace of discussions with states possessing nuclear weapons and special nuclear material with the goal of identifying and implementing more effective safeguards through the wider deployment of protection, control, and accounting technologies.

Although the United States has technically sophisticated capabilities to offer to other nations, other nations have also identified good technical solutions to many of these challenges. Technology sharing is essential for preventing the unauthorized procurement and use of nuclear weapons.

Recommendation 2.2: Concurrently, the U.S. government, working through the Department of Energy and Department of Defense, should reexamine the security of its own nuclear weapons, both within its borders and elsewhere.

Stolen U.S. nuclear weapons represent a very small threat in the universe of threats described in this chapter; nevertheless, protecting these weapons is solely the responsibility of the U.S. government, and a reexamination to determine their security would set a positive example for other nuclear powers to emulate. In particular, the risks and benefits of retaining forward-based nuclear weapons in NATO countries should be reassessed, especially in light of the 2001 Nuclear Posture Review, which emphasizes that the addition of non-nuclear strike forces to the U.S. deterrent capability will reduce U.S. dependence on nuclear forces.[8] Although the presence of forward-based nuclear weapons in NATO countries does not pose an immediate danger given current levels of security and protection measures, the potential for rapid, regional changes in the geopolitical security environment is cause for concern.

Recommendation 2.3: The U.S. government, working through the Department of Energy and Department of Defense, should undertake an internal evaluation of its bilateral Materials Protection, Control, and Accounting (MPC&A) program in Russia and consider ways to accelerate progress in safeguarding nuclear weapons and special nuclear materials, especially to counter potential insider threats. A principal goal of this evaluation should be to identify ways to accelerate deployments of means to safeguard (1) atomic demolition munitions and other small nuclear warheads and (2) special nuclear material, particularly highly enriched uranium.

This program is moving at an irregular and sometimes interrupted rate for a variety of reasons, but there are several actions the United States could take to

[8]Transmittal letter of the 2001 Nuclear Posture Review to Congress, signed by Donald H. Rumsfeld. The classified review was completed in December 2001. There are other technical and diplomatic issues relevant to the nuclear posture that would have to be considered in this reassessment, including binding agreements with NATO countries.

improve its reach and effectiveness. These include (1) encouraging more of the work under this program to take place through direct scientist-to-scientist contacts; this may help to promote a better understanding of workable approaches for both countries and (2) reconceptualizing the program as a fully joint program of technology research, development, and deployment[9] that can serve to improve Russian security and raise worldwide safeguard norms.

The first essential step in a robust MPC&A program is an accurate estimate of SNM inventories, which appears to be lacking in Russia. To address this problem, the United States should work with the Russian government to obtain an accurate inventory of its weapons-usable materials to match the U.S. declaration (DOE, 1994, 1996, 1998) in a way that addresses Russian national security concerns.[10]

Recommendation 2.4: The U.S. government, working through the Department of Energy, should increase the priority and pace of cooperative efforts with Russia to safeguard its highly enriched uranium by blending down this material as soon as possible.

One way to accomplish this objective is to encourage Russia to down-blend HEU in two stages: the first to just less than 20 weight percent to eliminate the proliferation threat, and the second to those levels (typically 4 to 5 percent) required for sale as feed for reactor fuel. This two-stage approach would not require any more time or effort than the one-stage process used at present,[11] and the first stage probably could be accomplished in about 2 years if adequate funding were made available.

Recommendation 2.5: The U.S. government, working through the Department of State, Department of Energy, and U.S. Nuclear Regulatory Commission, should provide encouragement as well as technical and financial assistance to the International Atomic Energy Agency to raise the levels of

---

[9]This effort could involve scientists and engineers from both countries, and one of its explicit goals could be to improve protection, control, and accounting technologies and practices and to share these improvements with other countries and organizations, especially the International Atomic Energy Agency.

[10]For example, the Russian government could make a secret declaration, certify to the United States that such a declaration had been made, and provide the declared inventories to the U.S. government in encrypted form as evidence of this certification. The Russian government would hold the encryption key and might, at some time in the future, make that key public so that the inventory could be verified.

[11]The same uranium hexafluoride (UF_6) gas flow would blend four times as much uranium-235 to 20 weight percent as to 4.4 percent, and the down-blending facility in Russia could handle at least twice the current gas flow. Furthermore, accelerating the pace of down-blending would not disrupt world uranium markets, because the availability of 4.4 percent uranium-235 for nuclear fuel is limited by its rate of sale by Russia to world markets and not by the rate of down-blending. Accelerating the pace of down-blending may require international cooperation beyond that of the United States.

international norms for protecting civilian special nuclear materials, specifically highly enriched uranium from research reactors and civilian plutonium from intact and reprocessed spent nuclear fuel.

The assistance could include technical support and funding for safeguards-technology development and deployment activities. The United States also should encourage other nuclear states to provide support for this effort.

Detection and Interdiction of Illicit Weapons and Special Nuclear Material

An important line of defense in a layered system of homeland protection is the detection and interdiction of illicit nuclear weapons and SNM as well as the detection and disruption of illicit weapons development programs. Science and technology can contribute to this defense effort in at least two ways: (1) by providing technical means for detecting the movement of SNM, especially HEU, either in weapons or as contraband, through border transit points and around critical U.S. assets such as ports, cities, and other high-value facilities; and (2) by providing sophisticated data-mining tools for analysis of intelligence on nuclear smuggling and on illicit weapons development programs.

The presence of certain types of penetrating radiation is a signature of most (but not all) SNM. Passive detection of gamma rays and/or neutrons can be an effective screening technique in some circumstances for revealing the presence of illicit SNM or INDs. In other cases, active interrogation methods may be required. While shielding can reduce these signals, they can serve as a useful first indicator of SNM, as well as other radioactive materials that could pose threats.

The nuclear materials of primary interest in weapons and INDs are plutonium, primarily plutonium-239 and plutonium-240, and HEU. Plutonium can be detected through passive gamma-ray and neutron monitoring, but HEU is difficult to detect passively owing to its low specific activity, low spontaneous fission rate, and low-energy gamma-ray emissions. Passive monitoring of these materials requires large-area detectors and relatively long exposure durations for acceptable sensitivity. HEU can be detected by active monitoring using, for example, neutron detectors and pulsed neutron sources. Additionally, both HEU and plutonium can be detected indirectly by gamma radiography, which is sensitive to high-atomic-number materials. Active systems are more complex and costly than passive detectors, however, and they emit radiation. Consequently, there may be radiological safety issues associated with their use in populated areas.

The full deployment of a national detection network would be an expensive proposition given the large numbers of international transit points, entry points into the United States, and critical U.S. cities and facilities. Although sensor technologies now exist for such deployments, it will be a daunting technical challenge to integrate these technologies into effective and reliable detection systems—in particular, to sort through the thousands of hits that would be re-

ceived each hour from legitimate transport of commercial radioisotopes (including isotopes implanted or injected into people for medical tests and treatments), identify and track suspicious targets while the threats they pose are being evaluated, and dispatch responders to interdict the target if the threat proves credible, all in real time. A poorly designed system would likely be turned off or ignored by frustrated operators and responders once the false alarms reached even moderate levels. The state of the art for such detection systems has not yet advanced to the levels needed to make a national deployment feasible.

A careful analysis of likely SNM transport routes, however, would likely reveal a smaller number of choke points where well-designed detection systems could be effectively deployed. Such choke points might include the following:

- Critical border transit points in countries like Russia;
- Major global cargo-container ports, especially at cargo entry and transfer portals;
- Major U.S. airports with large numbers of international arrivals;
- Major choke points in the U.S. interstate highway system—for example, through the Rocky Mountains; and
- Major roadways, bridges, and tunnels into critical U.S. cities.

The deployment of sensor systems even at a large number of such choke points would not guarantee the detection of SNM in transit—determined terrorists probably could find ways to overcome such systems by using secondary entry points and roads or by using heavy shielding. But the deployment of a well-tested, national integrated detection network would be a powerful component of the layered homeland defense system.

A national detection network could consist of several types of sensors: large numbers of simple counters that indicate the presence of radiation, backed up by smaller numbers of spectroscopic instruments to identify specific isotopic signatures. The technical challenge for the deployment of both types of sensors is the differentiation of signals of interest from the background of naturally occurring radioactivity and medical and industrial radioisotopes. There is a surprising lack of comprehensive data on the normal variations in background and radioactivity in general commerce.

Small hand-held ("pager") radiation detectors are becoming available to customs officials, police, and first responders. These instruments could form the first layer of detection defense for illicit radioisotopes (especially strong gamma emitters) and could also be used by emergency personnel when responding to suspected radiological incidents. At present, most of these instruments have no spectroscopic discrimination capabilities; additional R&D would be needed to develop low-cost instruments of this type with spectroscopic capability and to improve their sensitivity and selectivity. Fixed instruments at airports or other

choke points can provide very useful sensitivity for materials in luggage or carried in truck cargo. R&D to support the innovative design and production of cost-effective detectors to meet these needs could be an important path to progress.

The following actions should be taken to improve the nation's capabilities to detect the illicit movement of weapons and SNM:

Recommendation 2.6: A focused and coordinated near-term effort should be made by the Department of Energy, through its National Nuclear Security Administration, and by the Department of Defense, through its Defense Threat Reduction Agency, to evaluate and improve the efficacy of special nuclear material detection systems that could be deployed at strategic choke points for homeland defense.

The objectives of these evaluations should be to provide (1) technical feedback to system developers that can be used to improve system design and performance; (2) improved definition of background signals at potential monitoring sites and radioisotopes in general commerce that can be used to improve system capabilities to detect illicit materials in transport; and (3) experience in detecting materials in transport that can be used to develop protocols for identifying false positives and evaluating and responding to actual threats.

Recommendation 2.7: Research and development support should be provided by the Department of Energy and Department of Defense for improving the technological capabilities of special nuclear material detection systems, especially for detecting highly enriched uranium.

In the near term, R&D is needed to improve neutron interrogation sources (i.e., neutron generators) and detector systems for HEU. Additionally, some priority should be given to the development of inexpensive portable detectors with spectroscopic discrimination capabilities so that such detector systems could be more widely deployed.

As mentioned above in this chapter, future efforts to develop INDs may be harder to detect and disrupt because such efforts are likely to involve multiple organizations spread across the globe. Detection of such efforts will require the ability to assemble intelligence data from many disparate sources and to find patterns and connectivity among large amounts of seemingly unrelated data. This will require the development of new databases, for example, databases that can be used to track and attribute smuggling efforts; enhancements to the connectivity of various kinds of databases (e.g., intelligence, immigration, law enforcement, signals intelligence, and imagery) to enable searching for relevant data; and the development of sophisticated data-mining tools and techniques that can identify transnational patterns and connections in the acquisition of know-how, technology, and materials for fabricating illicit weapons.

Effective Responses to Nuclear and Radiological Attacks

Responses to nuclear and radiological attacks fall into two distinct categories that could require very different types of governmental actions: (1) attacks involving the detonation of a nuclear weapon or IND and (2) attacks involving RDDs. The first type of attack would likely involve massive property destruction and loss of life, making it difficult to mount an effective emergency response, at least over the short term. An emergency response action lasting months to years might be required in the wake of such an attack. The second type of attack would likely involve localized loss of life and no immediate danger to surrounding populations or property, but the potential for misinformation and public panic would be high. An emergency response action lasting weeks to months might be required, although longer-term cleanup might be needed for large RDD attacks. The worst scenarios involving nuclear power plants fall somewhere between these two categories, but, as noted in the classified annex, studies have not yet determined how credible these scenarios are.

Responses to nuclear and radiological attacks are governed by the Federal Radiological Emergency Response Plan,[12] which establishes authorities and procedures for responding to "peacetime" radiological emergencies such as accidents at nuclear power plants. This plan devotes only three paragraphs to radiological sabotage and terrorism, giving the Federal Bureau of Investigation the lead for investigating such acts and calling on other agencies, especially the designated lead federal agency, to assist the bureau in its investigative mission. The plan concludes that acts of sabotage and terrorism should not be treated as separate types of emergencies but are simply a "complicating dimension" of the other types of emergencies.

The correctness of this conclusion seems questionable given the attacks that might be envisaged in light of September 11. A terrorist attack could be much larger in magnitude than other events anticipated under this emergency plan. Such an attack could require large numbers of rescuers and medical personnel trained to deal with radiological emergencies; the ability to manage large populations in contaminated urban areas for long periods of time, potentially years; the ability to predict in real time the spread of radioactive contamination in debris clouds and provide this information to potentially affected populations in real time so that appropriate actions can be taken; and timely and effective cleanup capabilities. The current plan does not appear to provide the guidance needed to ensure this type of response in the case of nuclear terrorist attack.

---

[12] *Federal Radiological Emergency Response Plan—Operational Plan,* published by the Federal Emergency Management Agency in the *Federal Register* on May 1, 1996, with a correction published on June 5, 1996. The plan is available online at <http://www.au.af.mil/au/awc/awcgate/frerp/frerp.htm>. Accessed on April 22, 2002.

Recommendation 2.8: Immediate steps should be taken by the Federal Emergency Management Agency to update the Federal Radiological Emergency Response Plan, or to develop a separate plan, to respond to nuclear and radiological terrorist attacks, especially an attack with a nuclear weapon on a U.S. city. This plan should, at a minimum, address the following needs: (1) rapid mobilization of nationwide medical resources to cope with burns, physical trauma, and poorly characterized outcomes of exposure to radiation; (2) rapid airlift of field hospitals to the affected area; (3) means to provide the affected public with basic information on protection against radiation and fallout; (4) technical procedures for decontaminating people, land, and buildings; and (5) protection of citizens and foreign nationals from vigilante attacks. This plan should be mock exercised and, if required, incident site monitoring capabilities should be enhanced. Steps also should be taken to ensure that federal decision makers are familiar with this plan.

Should a nuclear or radiological attack occur, response effectiveness could be enhanced through public education efforts carried out well in advance of a nuclear or radiological attack. These efforts could include the stocking of potassium iodide pills by individuals to reduce the potential for thyroid cancers from releases of radioactive iodine. Such efforts may increase the public's willingness to accept market-based recovery approaches for land use and permitted activities in regions that are contaminated at levels just a few times above background radiation levels.

Attribution to Identify Characteristics of Weapons and Special Nuclear Material and Their Sources of Origin

As the history of the Cold War has shown, the most effective defense against attacks with nuclear weapons is a policy of nuclear retaliation. This past success suggests that the United States may be able to deter some future state-supported or state-sponsored nuclear and radiological terrorist acts by announcing in advance that it will retaliate by whatever means deemed appropriate, including the use of nuclear weapons, against states and terrorist groups responsible for nuclear or radiological attacks against U.S. citizens or assets.[13] To be a useful deterrent, however, this doctrine would have to be formulated and announced in advance, and its credibility would depend in large part on the ability of the United States to demonstrate to the rest of the world that it has the technical means to attribute such attacks to states or terrorist groups.

---

[13]The analogy between the Cold War and post-September 11 worlds is imperfect in that terrorist activity is dispersed geographically and may not be politically motivated. A doctrine of assured retaliation probably would not deter fanatical terrorist groups, but it may discourage states from providing such groups with aid and comfort.

Attribution is a difficult technical challenge—ideally, one would want to know both the characteristics of the weapon used in the attack and its country of origin. The former can be determined through careful analysis of blast debris; the latter might be determined by linking this information with intelligence on thefts, smuggling, and weapons development efforts by states and terrorist groups developed through the data-mining techniques discussed above.

Efforts are under way by national laboratories to develop an attribution capability under the Defense Threat Reduction Agency (DTRA). The goal is to develop the capability to perform a postdetonation debris analysis and to draw conclusions on the design and performance after an attack. The technology for developing this capability exists but needs to be assembled, an effort that is expected to take several years.

Recommendation 2.9: Given the potential importance of attribution to deterring nuclear attacks, the Defense Threat Reduction Agency's efforts to develop a capability for identifying perpetrators of an attack should continue to declared operability as quickly as practical.

Reactors

The events of September 11 suggest that physical and operational changes at some NPPs may be needed to mitigate vulnerabilities to attacks from the air using a large commercial airliner or a smaller aircraft loaded with high explosives and, possibly, attacks from the ground using HE projectiles. The technical analyses that are now being carried out by the USNRC and EPRI to understand the effects of such attacks on reactor containment buildings and essential auxiliary facilities are critical to understanding the full magnitude of this threat to the nation's NPPs.

Recommendation 2.10: The ongoing U.S. Nuclear Regulatory Commission and Electric Power Research Institute assessments of nuclear power plant vulnerabilities to airliner attacks should be completed as soon as possible, and follow-on work to identify vulnerabilities on a plant-by-plant basis, including vulnerabilities to air attacks by small craft loaded with high explosives or to ground attacks by high-explosive projectiles, should be undertaken as soon as these initial studies are completed. This "completion" should not stand in the way of early actions to address significant plant vulnerabilities that are identified in the course of the ongoing Sandia National Laboratories and EPRI assessments. If these assessments continue to show that important vulnerabilities exist, then steps should be taken to reduce such vulnerabilities as soon as possible.

If the USNRC discovers significant vulnerabilities at its licensees' reactors as a result of these analyses, it could mandate a number of physical and opera-

tional changes to reduce vulnerabilities to and the consequences of attacks. Some possible changes are listed in the classified annex. This list is by no means exhaustive, and an effective remedy can be applied at a particular reactor only after a careful analysis of risks and benefits, taking into account the comparative risk reduction that could be achieved by devoting resources to hardening nuclear plants versus other large industrial facilities.

Radiological Dispersion Devices

Although the damage potential of RDDs is far less than that of stolen nuclear weapons, improvised nuclear explosives, or successful attacks on reactors, the terror/panic potential of RDDs warrants increased attention to the control and use of radiological sources by regulatory agencies and materials licensees.

Recommendation 2.11: The U.S. Nuclear Regulatory Commission and the states with agreements with that agency should tighten regulations for obtaining and possessing radiological sources that could be used in terrorist attacks (i.e., large sources containing long-lived isotopes), including requirements for securing and tracking these sources. Additionally, licensees possessing large sources should be encouraged to substitute nonradioactive sources (compact accelerators, electron beams, and x-ray generators) when economically feasible.

Other important counters to RDDs are public education, emergency responder training, and preparation of leaders to deal quickly and effectively with terrorist acts. As noted above, the likely aim of an RDD attack would be to spread fear and panic and cause disruption. Recovery would therefore depend on how such an attack is handled by first responders, political leaders, the media, and general members of the public.

In general, public fear of radiation and radioactive materials appears to be disproportionate to the actual hazards. Although hazardous at high doses, ionizing radiation is a weak carcinogen, and its effects on biological systems are better known than those of most, if not all, toxic chemicals. Federal standards that limit human exposure to environmental ionizing radiation, which are based on the linear, nonthreshold dose-response relationship,[14] are conservative and protec-

[14]That is, mutagenic (cell mutation) and carcinognic (cancer) effects are assumed to increase linearly with radiation dose, with no threshold at low doses below which there is zero effect. A recent report by the National Council on Radiation Protection and Measurements concluded that "there is no conclusive evidence on which to reject the assumption of a linear-nonthreshold dose-response relationship for many of the risks attributable to low-level ionizing radiation . . ." (NCRP, 2001, p. 7).

tive, and the government continues to fund R&D[15] to improve scientific understanding of radiation effects on biological materials.

Education and training can serve as an effective counter to future RDD attacks. To this end, the committee recommends that the following actions be implemented:

Recommendation 2.12: Training should be provided to emergency responders (police, fire, and other emergency service personnel) on how to assess on-the-ground hazards from radiological attacks. As part of this training, responders should be provided with simple but effective radiation-monitoring devices, trained in their use, and told whom to contact for expert assistance, if needed. The Office of Homeland Security should take the lead for this effort in cooperation with the National Nuclear Security Administration and the Federal Emergency Management Agency.

Recommendation 2.13: Prepackaged kits of written materials on basic radiation science and effects should be developed for the media and national, state, and local leaders to help them respond appropriately to radiological attacks. The Office of Homeland Security should take the lead for this effort and should work with independent credible organizations to develop these kits.

Recommendation 2.14: A technically credible spokesperson at the national level who is perceived as being outside the political arena—for example, the President's Science Advisor, the Surgeon General, or their designated spokespersons—should be prepared to provide accurate and usable information to the media and public concerning public health and safety risks and appropriate response actions in the aftermath of a nuclear or radiological attack.

Such a response needs to be prepared and rehearsed in advance to avoid the kind of national leadership confusion that followed the anthrax attacks on Washington, D.C., in 2001.

---

[15]The Department of Energy sponsors research on low-dose radiation effects within the Office of Science and also supports the Radiation Effects Research Foundation, which is conducting a long-term longitudinal study of Japanese atomic bomb survivors. Additionally, the federal government provides funding to the National Research Council's Biological Effects of Ionizing Radiation (BEIR) Committees for periodic reassessments of low-dose health effects. The BEIR-VII study is currently in progress, and its objective is to determine the mathematical relationship between health risks and radiation dose for low levels of ionizing radiation.

CONCLUDING DISCUSSION

Many of the recommendations offered in this chapter call for an organized, focused, and adequately funded R&D effort to counter nuclear and radiological terrorism, as well as additional scientific, technical, and policy actions to reduce the nation's vulnerability to terrorist attacks, sometimes in cooperation with other national governments. To be effective, these efforts must bring to bear the best scientific and technical resources available to the federal government and must be well coordinated with other federal R&D and counterterrorism activities.

Important progress is already being made by the R&D and policy communities to reduce the nation's vulnerability to nuclear and radiological terrorism. There is not much evidence, however, that the R&D activities are being coordinated, that thought is being given to prioritizing these activities against other national counterterrorism needs, or that effective mechanisms are in place to transfer the results of these activities into application. Presumably the newly established Office of Homeland Security will take a lead role in the national counterterrorism effort, but that office does not have the expertise or budget to oversee a broad R&D effort.

The effectiveness of the nation's counterterrorism efforts could be improved if one agency were given the lead responsibility for coordinating and prioritizing, in consultation with other interested agencies, nuclear and radiological counterterrorism R&D. Several federal agencies have R&D responsibilities and could potentially take the lead: DOE's National Nuclear Security Administration (NNSA) already has a large R&D effort on many of the issues addressed in this chapter and is carrying out that work at the three national laboratories under its control.[16] The DOD's DTRA is carrying out R&D work to reduce threats from chemical, biological, and nuclear weapons of mass destruction. This work is being carried out primarily by DOD contractors, including NNSA national laboratories. The USNRC also sponsors R&D on NPP safety and vulnerabilities, and some of this work is carried out at NNSA national laboratories.

Given its large budget and broad scope of current work, it appears that DOE-NNSA is best positioned to take a lead role for R&D on nuclear and radiological terrorism. The committee, however, has not had an opportunity to study this issue in detail, especially to examine the current R&D portfolios of NNSA and DTRA or their strategic planning documents. The President's science advisor, working with DOE, DOD, USNRC, and other agencies with a stake in this decision, may be in the best position to develop a recommendation to the President regarding which agency should take a lead role in this important R&D effort. The designation of a lead agency also will require approval from the U.S. Congress.

---

[16]Lawrence Livermore National Laboratory, Los Alamos National Laboratory, and Sandia National Laboratories.

Recommendation 2.15: A single federal agency, possibly the Department of Energy's National Nuclear Security Administration, should be designated as the nation's lead research and development agency for nuclear and radiological counterterrorism. This agency should develop a focused and adequately funded research and development program to fulfill this mission and should work with other federal agencies, the President's science advisor, and the director of the Office of Homeland Security to coordinate this work and ensure that effective mechanisms are in place for the timely transfer of results to the homeland defense effort.

The centralization of lead R&D responsibilities into a single federal agency is no guarantee of success absent commitments to certain operating principles. Among these are commitments to appoint a technically capable staff to manage the R&D work; to provide sufficient and sustained funding to carry out an adequate program; and to reach across agency boundaries and outside government to obtain the expertise needed to execute the work and to ensure that results are moved expeditiously into application. While the events of September 11 appear to have produced a renewed sense of cooperation among federal agencies, the challenge for whichever agency is selected to lead this important R&D effort will be to nurture and sustain this spirit.

REFERENCES

Department of Energy. 1994. *Openness Press Conference Fact Sheets*, Office of the Press Secretary, Washington, D.C.

Department of Energy. 1996. *Plutonium: The First 50 Years,* Washington, D.C., 82 pp.

Department of Energy. 1998. *Commercial Nuclear Fuel from U.S. and Russian Surplus Defense Inventories: Materials, Policies, and Market Effects,* DOE/EIA-0619, Energy Information Administration, Washington, D.C., 115 pp.

Energy Information Administration. 2002. *U.S. Nuclear Generation of Electricity*. Available online at <http://www.eia.doe.gov/cneaf/nuclear/page/nuc_generation /gensum.html>.

Gonzalez, A.J. 1999. "Strengthening the Safety of Radiation Sources and the Security of Radioactive Materials: Timely Action," *IAEA Bulletin*, Vol. 41, No. 3, pp. 2-15.

National Council on Radiation Protection and Measurements. 2001. *Evaluation of the Linear-Nonthreshold Dose-Response Model for Ionizing Radiation*, Report No. 136. Bethesda, Md., 287 pp.

Private Fuel Storage. 2002. *The PFS Facility Specifications*. Available online at <http://privatefuelstorage.com/project/facility.html>.

U.S. Nuclear Regulatory Commission. 2002. *List of Power Reactor Units*. Available online at <http://www.nrc.gov/reactors/operating/list-power-reactor-units.html>.

3

Human and Agricultural Health Systems

INTRODUCTION

Biological pathogens (for example, anthrax bacteria or the smallpox virus) or toxins produced by biological organisms (for example, botulinus toxin or staph enterotoxin) that are released intentionally or accidentally—or that occur naturally—can result in disease, fear, disruption to society, economic harm, diminished confidence in public and private institutions, and large-scale loss of life.

People or livestock can be exposed to these agents from inhalation, through the skin, or by the ingestion of contaminated food, feed, or water. After exposure to a pathogen or toxin used as a biological weapon, physical symptoms can be delayed and prove difficult to distinguish from naturally occurring illnesses. Similarly, crops can be exposed to biological weapons in several ways—at the seed stage, in the field, or after harvest.

The deciphering of the human genome sequence and elucidation of the complete genomes of many pathogens, the rapidly increasing knowledge of the molecular mechanisms of pathogenesis and of immune responses, and the development of new strategies for designing drugs and vaccines offer unprecedented opportunities for using science to counter bioterrorist threats. But these advances also allow science to be misused to create new agents of mass destruction.

Two kinds of biological terrorist threats must be envisioned. The first is the release of communicable infectious agents—like smallpox, Ebola, or foot-and-mouth disease—that can spread rapidly within communities and farmland through contact and have the potential, as does influenza, to spread around the world and cause epidemics. The second kind of threat consists of biological agents that may cause disease or death in individuals but generally may not be transmitted *between*

individuals—the most familiar example being anthrax. In either case, some agents may persist in the environment, as do anthrax spores, and continue to cause problems long after their release.

In addition to naturally occurring pathogens, biological agents used offensively can be genetically engineered to resist current therapies and evade vaccine-induced immunity. Though it is vital that the molecular mechanisms by which classes of organisms cause disease (pathogenesis) be elucidated in order to understand and counter their effects, this is no simple matter. Preparedness for a biological attack against people, crops, or livestock is complicated by the large number of potential agents, the long incubation periods of some agents, and their potential for secondary transmission.

Biological agents do not need to be weaponized for effective dissemination. Deliberate contamination of food looms as perhaps the easiest method, despite the recent focus on release of these agents as small-particle aerosols or volatile liquids. Moreover, because of its size and complexity, the U.S. food and agriculture system is vulnerable to deliberate attacks, particularly with foreign diseases that do not now occur domestically. Even without actual attack, plausible threats to infect populations or poison the food supply could, in and of themselves, damage the U.S. economy and reduce public confidence in the government's ability to safeguard health and security.

Recent experiences with the West Nile virus and anthrax spores in the United States, and with foot-and-mouth disease in the United Kingdom, offer practical lessons in human and agricultural outbreak detection, laboratory diagnosis, investigation, and response that might be useful in planning for future attacks involving biological terrorism (Fine and Layton, 2001). The experience with the West Nile virus outbreak highlighted the importance of communication and coordination between responding agencies (U.S. General Accounting Office, 2000). The GAO study noted that although the system worked, there were several obvious places for improvement. A single alert physician at a local hospital initiated the investigation early enough that an effective intervention was possible before the outbreak became widespread, but the investigation subsequently found many other cases, which were either not properly diagnosed or not reported to the health department. The GAO report concluded that much more systematic surveillance and reporting at the local level is needed. Similarly, improved communication among public health agencies, including those dealing with animal health, is needed. Increased laboratory capacity will also be important to an efficient and effective response to disease outbreaks (at first only one public health laboratory in the country was equipped to diagnose West Nile virus) (IOM, 2002). Moreover, these events raise vexing concerns about how many outbreaks could be managed at one time.

The attacks of September 11, 2001, and the intentional release of anthrax spores shortly afterward also revealed vulnerabilities that are the results of long-term declines in the nation's public health and agricultural infrastructures. The

decline in the U.S. public health system is the result of its systematic dismantling over time by Congress and the executive branch. In fact, the response of the Centers for Disease Control and Prevention (CDC) to the anthrax attacks was admirable given its limited resources and outdated communications system. CDC, together with state and local health departments, has provided this nation with an outstanding cadre of people who understand how to perform surveillance, prevention, and detection of infectious agents, whether they are endemic, emerging, or a result of bioterrorism. These agencies must be supplied with the tools and resources taken away from them in the past. Restoring the public health system of the United States should be the first order of business in the efforts to defend the nation against bioterrorism.

The Need for Approaches with Multiple Benefits

Bioterrorism poses a unique challenge to the security of the U.S. population. A state-sponsored enterprise, or just a few individuals with specialized scientific skills and access to a laboratory, could easily and inexpensively produce a panoply of lethal biological weapons, although it is no trivial matter to disseminate or disperse such agents across large populations. Such operations may be difficult to detect because, in contrast to nuclear weapons, biological agents can be manufactured with ordinary pieces of equipment that are listed in commercial catalogues and are legitimately purchased for producing such things as chemicals, pharmaceuticals, or even beer.

Fortunately, investments made to protect the country against bioterrorism will help protect the public's health and the U.S. food supply from naturally occurring threats as well. Although it may be difficult to distinguish an introduced infectious disease from a naturally occurring one, the strategies to protect against either—requiring preparation and new scientific and technological approaches to surveillance, prevention, response, recovery, decontamination, and forensics—must be the same. Similarly, investments made to protect the country's food supply against bioterrorism have the potential, and are even necessary, to protect it from more routine threats as well. Because the most likely breakthroughs will come from the study of both pathogenic and nonpathogenic bacteria and viruses, they should be studied together—indeed, the study of bioterrorism agents alone is likely to give a low return on investment.

There are also indirect benefits associated with investments in protecting ourselves from bioterrorism. Money spent on research to develop new types of sensitive detectors and related monitors for biowarfare agents will almost certainly carry over to the public health sector in the form of rapid, improved diagnostics for disease. Money spent on coordinating and developing emergency response teams at the federal, state, and local levels will also bring better mechanisms for dealing with natural outbreaks of emerging diseases. Money spent on innovative surveillance approaches for detecting biowarfare attacks should improve

medical epidemiology. Money spent on vaccine research and delivery may help to buttress our limited capacity to protect civilian and military populations.

Changing Research Paradigm

While this report was being prepared, the National Institute for Allergy and Infectious Diseases (NIAID) released a bioterrorism research agenda for rapidly addressing the most threatening biological agents (NIAID, 2002).[1] Though important and commendable, this agenda lacks several major components—such as surveillance strategies, epidemiology of transmission, and the entire range of agricultural threats—needed for a comprehensive plan to counter bioterrorism. Consideration must also be given to preparing for still-uncharacterized threats and to assuring investment in long-term, broad-range strategies. These gaps must be filled, where not appropriate for NIAID action, by other federal agencies. CDC is the logical place for surveillance efforts, given its expertise, and therefore it will require additional resources.

NIAID's expanded role in bioterrorism research demands a focused effort to coordinate activities with other agencies—CDC, the Department of Defense (DOD), the Department of Energy (DOE), the Environmental Protection Agency (EPA), the U.S. Department of Agriculture (USDA), and the very recently proposed new Department of Homeland Security, for example. All of the governmental entities must seek expertise from private organizations, such as industry and professional societies with relevant expertise, for example, the Infectious Diseases Society of America and the American Society for Microbiology. It also demands that NIAID's parent, the National Institutes of Health (NIH), find new mechanisms to fund research in this area, particularly for taking on long-range, highly managed, higher-risk projects and for moving the research at a faster pace. Likewise, CDC's role is critical to the nation's preparedness, but it must have the resources to improve its focus, strengthen its extramural capacity, and extend its international collaborations. National security also depends on public-private sector cooperation and communication and on an increased willingness to collaborate.

Organization of This Chapter

This chapter is organized into three sections: (1) intelligence, surveillance, detection, and diagnosis; (2) prevention, response, and recovery; and (3) policy and implementation. Each section describes the desired capabilities that could soon exist through better application of existing science and technology (and that might therefore have a near-term payoff) as well as desired capabilities that

[1]See March 14, 2002, press release "NIAID Unveils Counter-Bioterrorism Research Agenda" at <http://www.niaid.nih.gov/newsroom/releases/biotagenda.htm>.

cannot now be provided through existing science and technology (S&T) but might be available in the future, given longer-term research and possibly more innovative funding and organizational approaches. The chapter focuses on research needs related to both human and agricultural health. Many of the recommendations apply equally to both areas while others are specific to one area or the other. In general, recommendations focus on R&D goals or organizational goals. The chapter concludes with recommendations about education and information dissemination, strengthening the public health and agriculture infrastructures, and organizing the research and development effort through improved policies, new funding models, and public–private partnerships.

INTELLIGENCE, DETECTION, SURVEILLANCE, AND DIAGNOSIS

A comprehensive approach to coping with bioterrorism must incorporate efforts to prevent the proliferation of biological weapons; methods for detecting covert biological weapons programs; strategies for deterring their use if biological weapons do proliferate; and mechanisms for protecting civilian and military populations if deterrence fails. The emphasis in this multitiered approach should be on defense, simply because the proliferation of biological weapons is difficult to control (biotechnology equipment and expertise are now available globally), covert biological weapons programs (e.g., those of the former Soviet Union and Iraq) are difficult to detect, and deterrence will likely be less effective against suicidal terrorist groups than against states. Consequently, in addition to improving intelligence and information management, the S&T community should be focused on improving defenses against biological weapons. The means to do so include environmental detection of biological agents together with preclinical, clinical, and agricultural surveillance and diagnosis.

Intelligence and Information Management

Increased awareness in the S&T community could reduce the inadvertent spread of knowledge that may aid terrorists, although there is a fine balance that must be achieved so as to not quash legitimate exchange of scientific information. Voluntary international and national efforts to share biotechnology information could improve security and safety in the handling, storage, and transport of sensitive biological material and equipment. Information technology could help monitor international trafficking in biotechnology products.

Detection of covert programs will involve technical intelligence (e.g., remote sensing and environmental sampling) as well as human intelligence, which has special importance because it can distinguish the benevolent use of biotechnology from the malevolent. Understanding intent in the area of biotechnology, which requires familiarity with S&T culture, processes, and procedures, is an expertise that scientists and technologists can offer the intelligence community.

Meanwhile, there is a need to teach, reinforce, and strengthen ethical standards of the S&T community against the production and use of biological weapons; this will reduce the likelihood of scientists working in covert programs and increase the chance of them helping to abort malevolent efforts.

Although much has been written about the potential efficacy (or inefficacy) of ways to deter biological attacks, the S&T community has yet to fully explore means for strengthening deterrence. An obvious option is biological forensics (discussed later), because without reliable attribution, most deterrence strategies are likely to fail. Nucleic acid sequence databases for pathogen strain types and advances in chemical-trace analysis and the use of taggants will help the process of attribution, thus discouraging terrorism, but they will by no means guarantee that perpetrators can be identified.

The greatest potential benefit of a counterterrorism strategy might derive from preemptive efforts at earlier points in the bioterrorism-attack timeline—that is, the evolution of a bioweapons program from inception through weapon deployment, before any biological agent is released. The S&T communities have had relatively little input into detection and characterization of terrorist activities during this early stage, yet they could offer significant untapped resources. Opportunities for their involvement in the area of human intelligence should be explored (see Box 3.1).

BOX 3.1
Opportunities for Integrating the Intelligence and S&T Communities

Short Term

- Recruit members of the S&T community for assistance and advice on the collection and early analysis of relevant human intelligence in bioterrorism activities.
- Promote collaborative research programs that enhance contact between members of the S&T community and scientists from former or current biowarfare or bioterrorism research programs (e.g., cooperative research programs).
- Develop a database for locating bioterrorism or related expertise in academic and industrial laboratories.

Long Term

- Recruit and train intelligence analysts in state-of-the-art biology, microbiology, and bioinformatics.
- Train or sensitize working scientists to recognize malevolent intent, as well as signatures of offensive bioweapons programs, and develop a plan for sharing this information with appropriate parties.
- Facilitate the development of tools for aiding in the recognition of such signatures.

Recommendation 3.1: All agencies with responsibility for homeland security should work together to establish stronger and more meaningful working ties between the intelligence, S&T, and public health communities.

Identification of Biological Agents in the Environment

At the present time, efforts to identify biological agents in air, soil, and water samples have had only limited success. Ideally, one would hope to be able to collect air samples, for example, and identify a pathogen in those samples in near real time, allowing the population to be warned of the pathogen's presence. However, existing technologies for rapid and reliable detection (collection and identification) of bioagents have not been widely evaluated or well validated in real-world settings. Much greater attention must therefore be given to the transition between basic laboratory research and field application.

Traditional laboratory approaches include microbial cultivation, immunological (e.g., antibody-based) assays, and nucleic acid detection schemes, especially amplification methods such as the polymerase chain reaction (PCR). The last two approaches seek molecular evidence of agent components, such as characteristic immunological markers and genome sequences. A fourth broad approach relies upon the response of a surrogate host—such as cultivated cells from humans, animals, or plants.

Each of the four approaches has its advantages and disadvantages. It is important to note, however, that even though cultivation is slow, limited in scope (by ignorance of appropriate growth conditions in the test tube and in human tissues for many pathogens), and the least technologically sophisticated approach, it provides the most ready assessment of complex microbial phenotypes (behaviors), such as drug resistance. It also is the most widely used approach in laboratories throughout the world, especially in developing nations, and hence is currently the most common identification method for international surveillance.

A number of challenges must be addressed in order to develop and implement effective methods of environmental identification. An improved understanding of natural background is needed, regarding both the agent (including genetic, antigenic, geographical, and temporal variations) and the setting (including related agents and inhibitors). Additionally, standards must be established by which sampling and detection methods can be rigorously evaluated, validated, and standardized (see Recommendation 3.16 and surrounding discussions). Centralized repositories of diverse, high-affinity binding and detection reagents (e.g., antibodies, peptides, oligonucleotides) should be established, as well as repositories of genomic material and control samples. There are dozens of ways to identify bioterrorism agents that are sensitive and accurate. However, agreement on how a few well-developed platforms are implemented would allow the data to be broadly understood and make the limitations of the test used apparent to all.

For example, whether one is identifying anthrax on the farm, from the environment, or in a patient's blood stream, the identification can be quickly made using a fairly easily agreed upon set of standard genomic and immunological reagents. Subsequently, there must be cultures of microorganisms grown in the laboratory using agreed upon standard methods. The identification should be based on uniform standards and not a free-for-all depending on program officers or agencies with differing views.

To date, a disproportionate amount of the effort in the bioagent detection arena has been focused on the development of technology platforms. Efforts on standardization or validation of sample collection and sample processing procedures, as well as on test validation in a real-world setting, have had much lower priority. But the use of genomic and proteomic information, as well as the development of robotic sensing devices that can communicate signals from many environmental sites, offers new possibilities for the early detection of biologic agents in the environment. It also increases the risk of false alarms when sophisticated analysis and decision-making systems are lacking.

Another challenge involves creating broad-spectrum detection tools and methods. Currently a large number of tests rely on a small number of specific antibodies or microbial genomic sequences. This reliance creates vulnerabilities—for example, with respect to bioagents having modified antibody epitopes (binding sites) or sequences. Rather than relying on methods that target specific, known organisms, one would like to have detection methods that target groups of organisms (i.e., all members of these groups) and that can identify specific members of the group, including recognition of those that may not yet have been characterized. Although there are experimental challenges, the expertise exists to immediately begin addressing these problems (Cummings 2000, 2002; Nikkari et al., 2002).

A further challenge is the need for highly sensitive systems, as some highly infectious pathogens require the inhalation of only 1 to 10 organisms to cause disease. In general, much greater attention is needed to translate basic laboratory research into field applications and clinical validation (standards will play an important role; see Recommendation 3.16 and surrounding discussion). Finally, because no test is perfect, it is important to be able to anticipate false-positive test results in a reliable and quantitative fashion. One potential strategy for minimizing the impact of false-positive test results is to create a system of multiple, parallel, independent technical platforms so as to avoid dependence on any one testing procedure. This requires crosscutting, interdisciplinary science (e.g., combining environmental microbiology, cell biology, biophysics, electronics, materials science and microfabrication, microfluidics, and bioinformatics/statistics) and would require collaboration between several federal agencies and industry. However, even the currently available tests could be made significantly more useful by adopting a quality assurance index that would be applied to any positive test result. For example, single positives in tests with high false-positive rates, such

as ELISA, would receive a low ranking, whereas successful culture of a known biological agent from a sample would receive the highest ranking. Informed decisions on public action could be made based on the quality of the result rather than simply on the presence of a positive result.

Recommendation 3.2: Federal agencies should work cooperatively and in collaboration with industry to develop and evaluate rapid, sensitive, and specific early-detection technologies.

The types of identification systems needed are likely to be developed by industry, not in an academic laboratory. Federal funding agencies can speed this process by supporting the early stages of the work. The same kind of milestones should be applied to this kind of work as are used in industry to ensure that the technology is valid and meets the expected specifications. There is a role for the mobilization of established detection procedures and for those that might be second-generation detecting devices sometime in the future. The immediate need is acute and very attainable.

Surveillance and Diagnosis of Infection and Disease

Early diagnosis of patients infected with potential biological warfare (BW) agents is complicated by the lack of relevant medical experience with most of these agents in the United States and by the nonspecific symptoms of their associated diseases (e.g., many cause flulike symptoms in the early stages). Systems for effective surveillance and diagnosis of biothreat agents, as well as of many naturally occurring and emerging pathogens, are either unavailable at present or inadequate.

Many of the current challenges in surveillance and diagnosis are quite similar to those described above for identification of pathogens. Surveillance and diagnosis must also address the important distinction between infection and disease—that is, between the colonization or contamination of a host with a potential biothreat agent and the actual manifestation of pathology (disease). Sensitive and specific diagnostic tests are important adjuncts to clinical diagnosis; however, such tests cannot substitute for astute clinical recognition of symptoms to raise the suspicion of a particular diagnosis. Equally vital is the role of classical epidemiological analysis in assessment and recognition of human- and animal-disease patterns.

Preclinical Surveillance and Diagnosis

It would be critical, in the event of a biothreat agent attack, to be able to recognize or identify infected persons, animals, or plants before they develop overt disease. Great benefit could be achieved by rapid intervention in those persons, animals, or plants known to be infected, while avoiding unnecessary

intervention in those who are not. It is at this stage that the difficulties and challenges of diagnosis are greatest as well. In recent years, novel biotechnological and biological approaches have opened up new opportunities in this area.

In the interim, while new approaches are developed and refined, assessment of white blood count, fever, and relatively simple observations will remain the first line of defense in protecting human health. A primary focus of diagnostic strategy will continue to be the continuing education of physicians and health-care workers.

An example of a plausible new technological approach is the host-genome-wide gene-expression profile. The availability of a nearly complete human-genome sequence and the power of DNA microarray technology have been harnessed to create an approach for surveying the responses of nearly all known human genes to various infectious agents. Cells are programmed to recognize pathogenic agents and foreign life forms, and they respond with changes in host-gene expression; microbial agents, meanwhile, have evolved strategies for manipulating and subverting these programmed responses. The result is an intricate, choreographed, and time-dependent set of induced and repressed gene-expression patterns that can be detected in small blood samples (Cummings and Relman, 2000).

Although the dominant features of these patterns are common to virtually all infections, regardless of the particular infectious agent, other features may be more specific to the agent or disease. With further research and refinement, one might actually be able to distinguish infections by different pathogens and generate signatures that allow early identification. These patterns reflect how the host "sees" the pathogen, and they also reflect (and perhaps predict) the outcome of the host-pathogen interaction. Research exploring the potential usefulness of this approach is still in its early phases, however.

Host-gene expression patterns are just one complex biological pattern that might lend itself to this kind of diagnostic and prognostic approach. Others include patterns of secreted proteins in host fluids, volatile compounds in breath (analyzed, for example, with mass spectroscopy), and spectral features of host cells and fluids (studied using spectrometers and hyperspectral analysis). The enormous advantage of such technology, should it be able to fulfill researchers' expectations, is that it could distinguish genuine infection from hysteria or terror, either at the emergency room or in the clinic.

Human Disease Surveillance and Diagnosis

In this country and elsewhere, the recognition of almost all emerging infectious diseases—both naturally occurring and intentional—has depended on an astute clinician contacting a public health agency after suspecting an unusual serious illness (e.g., hantavirus in the Southwest or anthrax in Florida). This traditional system of notifiable human disease surveillance depends on the train-

ing of physicians and other health care providers, in terms of both disease awareness and their responsibilities to public health. In addition, the important systems linking hospitals around the country with CDC, known as sentinel surveillance systems, need to be enhanced; they can establish whether a common cause of disease is being seen simultaneously in multiple regions. Research should be conducted on the strategies likely to be most useful in enhancing the notifiable human disease reporting system for the broad range of potential threat agents (strategies such as education, animal sentinels, changes to the surveillance systems, and the use of infection control specialists). Mathematical models of disease transmission and distribution using simulations of a covert release of various agents could be helpful in assessing the potential and relative value of different surveillance systems. An integrated national system that can report diseases electronically in real time is needed to support these networks. Information technology advances should be explored both to automate required reporting (e.g., laboratory reporting of pathogens) and to develop new surveillance tools (e.g., the automated scanning of electronic media, such as that utilized by the Global Public Health Information Network).

Systems of syndrome surveillance—that is, screening for changes in the frequency of cases of flulike illness seen in hospital emergency rooms across a city or town—should be developed to identify outbreak patterns. Relevant computer programs are being developed, but there are known fluctuations in emergency room admissions from season to season and day to day, and it will be important to determine their potential predictive value, specificity, and usefulness. Syndrome surveillance has allowed early recognition of some respiratory and diarrheal disease outbreaks, but it is not clear whether it will be useful for early detection of key threat agents such as smallpox, anthrax, and tularemia.

Because infectious diseases do not respect national borders, international cooperation is vital in the sharing of epidemiological and clinical data, both on emerging infectious diseases and on outbreaks caused by potential bioterror agents. A global network for surveillance of infectious diseases in humans and animals would be strengthened by augmenting the numbers and capabilities of U.S. overseas laboratories and by providing enhanced support for current initiatives on international surveillance (e.g., DOD's Global Emerging Infectious Diseases program and corresponding Department of Health and Human Services (HHS) initiatives).

Increased support for the development and expansion of public health and agricultural laboratories in other countries, particularly in their capacity to diagnose threat agents, would yield dividends for recipient and donor alike. This means that CDC and other agencies must reach out to educate, train, and collaborate with scientists from many countries on aspects of surveillance and identification of threats. The World Health Organization could play a critical role in building and strengthening international capabilities.

Recommendation 3.3: Create a global network for detection and surveillance, making use of computerized methods for real-time reporting and analysis to rapidly detect new patterns of disease locally, nationally, and—ultimately—internationally. The use of high-throughput methodologies that are being increasingly utilized in modern biological research should be an important component of this expanded and highly automated surveillance strategy.

Another important area for applied research is the development of improved clinical diagnostics—rapid assays for the detection of common pathogens and BW agents—that could be used in primary care settings as well as referral laboratories. In addition, the kinds of needs that were described above for preclinical detection also apply to the field of clinical diagnostics. Standards are needed by which diagnostic methods and technology can be rigorously evaluated and validated, and centralized repositories of standardized reagents and samples are needed as well. Because the development and evaluation of diagnostics require interdisciplinary applied research, it is currently difficult to find targeted sources of support for these efforts. NIAID, CDC, and USDA should consider providing extramural funding programs to stimulate research in this area.

Because of the low likelihood of infections with BW agents compared to common, widely circulating agents like influenza viruses, routine application of rapid diagnostics for potential BW agents in a primary care setting *in the absence of clinical suspicion* will face problems with false-positive and false-negative results, for which rapid adjunctive standards do not exist. A triage system could be applied in which patients with relevant symptoms who test negative for a panel of expected pathogens would be sent to a referral laboratory for a second round of diagnostic tests, which could include suspected BW agents and broad-range methods.

High-throughput automated laboratory technology can now be applied to assist in these efforts. Positive samples could be forwarded to central public health laboratories for more comprehensive characterization. A laboratory designed, for example, to address influenza surveillance (Layne et al., 2001) could be dual use: Not only would it enhance public health by providing more accurate and timely information about the emergence of novel influenza strains, but it could also provide surge capacity to detect other agents if outbreaks occurred as a result of a terrorist attack. Continued development of effective networks of such referral laboratories (private, academic, local, state, and federal) is thus vital.

It should be noted that the first suspicion of the outbreaks of anthrax and of West Nile virus came not from sophisticated computer technology but from thoughtful and perceptive physicians. Tools to help all health professionals make the appropriate inferences from small numbers of patients must be developed so that the likelihood of missing a new outbreak is markedly reduced. Principal responsibility for this work should rest with CDC, NIH, and DOD.

Recommendation 3.4: Use knowledge of complex biological patterns and high-throughput laboratory automation to classify and diagnose infections in patients in primary care settings.

Agricultural Surveillance and Diagnosis

The protection of the nation's food supply presents several unique challenges related to surveillance and diagnosis of disease. The U.S. livestock industry, with revenues of approximately $150 billion annually, is extremely vulnerable to a host of highly infectious and often contagious biological agents (insects and other pests, viruses, and microbes) that have been eradicated from the United States. Unlike traditional biological agents that can be used against humans, many of these animal-targeted agents need not be weaponized to cause an outbreak. Their simple point-introduction into herds could immediately halt all movement and export of U.S. livestock and livestock products.

Although most agents that affect animals are not human pathogens, introduction of any of the agents on the A List of the World Organisation for Animal Health would have wide-ranging and devastating impacts on the U.S. economy—not to mention psychological effects on the country's human population—from which it could take years to recover. These disease agents are readily available in many countries. Although USDA's Animal and Plant Health Inspection Service (APHIS), as currently constituted, has proven adequate for naturally occurring disease, it would probably be unable to help eradicate intentional introduction, especially if this were done at multiple sites. There is a need for USDA to develop a research and surveillance capability for plant and animal diseases comparable to the one that CDC oversees for human diseases.

Animal agriculture would seem to be increasingly vulnerable to intentional biological attacks, given recent trends toward concentration and specialization in the livestock industries (MacDonald et al., 1999). For example, tens of thousands of animals can be housed in relatively close quarters in concentrated feedlots prior to slaughter. If the introduced agent is highly contagious, as is the foot-and-mouth disease virus, this concentration creates the potential for greater impact from a single infected animal, as aerosol transmission of pathogens is common within herds. Likewise, animals move across great geographic distances. For example, during September 2001, nearly a million of the swine imported into Iowa came from 24 states and Canada (communication from the Iowa State Department of Agriculture).

Given these vulnerabilities, there is a need to recognize an infected animal immediately. At present, however, although there are well-operated state and federal animal diagnostic laboratories, there is no integrated national system that can report diseases and infestations electronically in real time. In addition, there are no rapid field diagnostic assays for most animal pathogens and pests.

Crops, too, are vulnerable. They are grown over very large areas (e.g., some 75 million acres for soybeans) and there is very little surveillance or monitoring. Likewise, plant diagnostic laboratories are scattered across the country and are underresourced and understaffed. In addition, great variability exists in the capabilities of these laboratories from state to state. This situation means that a long time could elapse from the introduction of a crop pathogen to its detection. Remote sensing, particularly satellite imagery, may have value in monitoring crops for disease outbreaks, including those resulting from bioterrorism.

Other factors heighten the vulnerability of U.S. crops: (1) many hybrid crop species exhibit low levels of genetic diversity; (2) there are few restrictions on trade, and large volumes of agricultural products are imported and exported each year; (3) a substantial proportion of the seed used for growing U.S. crops is produced in other countries, presenting a possible route for the introduction of dangerous plant pathogens as well as contaminated fertilizers and pesticides; (4) fungi, viruses, and bacteria cause more than 50,000 diseases of plants in the United States; (5) for any given crop, there are several pathogens that are not yet found in the United States but that cause major losses elsewhere; and (6) the biological agents that could affect crops are more numerous than the pathogens that affect humans, making it more difficult to focus the research funding available for efforts to counter agricultural bioterrorism.

Threats to crops intersect with threats to livestock in the case of animal feed, and there is a particular concern about the timing of ultimate effects. The delay between the time at which a bioterrorist contaminates animal feed and the time the human food product becomes adulterated would cause more uncertainty about the source of the contamination and could minimize the possibility of apprehending the terrorist. The less obvious and the more natural the source of biological contamination, the greater the likelihood that the contamination of the animal feed will be mistaken as a natural phenomenon. Rapid testing of feed and separation of contaminated feed are important steps, followed by the more specific identification of the contaminant to determine the source of adulteration and the possibility of decontamination. The development of specific antibodies for the production of sensitive and specific test kits is the key to identifying contamination. This would allow one to deal effectively with the disposal or decontamination of the animal feed and, ultimately, to prevent the contamination of animal-derived human food products (Von Bredow et al., 1999).

Rapid containment of agricultural pathogens is dependent on an effective system for diagnosis and the coordinated action of various state and federal agencies. Although these agencies, including USDA's APHIS, have dealt successfully in the past with the natural introduction of several foreign pathogens of plants and animals, they are not properly organized to deal with the massive, multiple introductions that terrorists are likely to attempt. In essence, the game has changed, and this requires a substantial restructuring of the nation's agricultural response systems.

Recommendation 3.5: USDA should create an agency for control and prevention of plant disease. This agency should have the capabilities necessary to deal effectively with biothreats.

For animal disease, USDA operates several laboratories—Plum Island and Ames among them—that perform diagnoses, carry out research, and provide training for veterinarians. CDC is the central agency for the control and prevention of communicable human disease, but no center currently exists to serve the same function for plant disease. Such a center is desperately needed.[2] Departments of plant pathology at various state universities, APHIS, and a wide variety of other agencies, all of which often depend on outside experts, currently deal with new and unusual plant pathogens as best they can.

A major research, development, and training center is called for that would address fungal, bacterial, and viral diseases of plants. Programs would focus on genomics and proteomics, databasing and informatics, forensics, pathogenesis, host-parasite interactions, diagnostics, sensors, food safety, analytical methods, epidemiology, modeling of disease outbreaks, intervention, and management. Other efforts could include outreach, technology transfer, collections of pathogens, and epidemiological intelligence and response. Close linkages could be established with other federal and state agencies, as well as with academic institutions, international agencies with responsibilities for surveillance of plant diseases and bioterrorism, and industrial, extension, and professional organizations. These collaborators could, among other functions, provide advice on containment and control procedures.

PREVENTION, RESPONSE, AND RECOVERY

We can never create a perfect system to safeguard against terrorist use of a biological agent. But conscientious preparation—to the greatest extent that budgets and available methods allow—will reduce anxiety and greatly mitigate the consequences of an actual attack. Part of that preparation should involve research and development on needed tools and approaches. These include modeling techniques, bioforensics, methods for defining threats, specific and broad-spectrum antibiotic and novel antiviral agents, and means for rapid vaccine fielding. Once an attack has occurred, a better prepared and reinforced health and agriculture response system will be needed, as will be a reliable and consistent communications plan. For those exposed, protocols for treatment and decontamination must be available. And for animal and plant exposures, an effective disposal and decontamination plan must be in place.

---

[2]A similar recommendation was made in February 2002 by the American Phytopathological Society. The white paper "American Phytopathological Society: The First Line of Defense—Biosecurity Issues Affecting Agricultural Crops and Communities: Genomics, Biotechnology, and Infrastructure" is available for review at <http://www.apsnet.org/media/ps/BiosecurityWhitepaper2-02.pdf>.

For communicable diseases in particular, given the potential for initial exponential growth in the number of cases from a single diseased individual, it is crucial that a variety of methodologies, both prophylactic and reactive, be developed for limiting spread. These include vaccination, treatment, quarantine, movement restrictions, isolation and, in the case of nonhuman populations, culling. Because the potential for spread is determined by the number of secondary infections per primary infection, success in management can be achieved by a combination of reducing the infectious period and reducing transmission.

Studies must be done to develop decision rules and procedures for quarantine. These studies must be conducted with the goal of ultimately involving active participation of communities well before any event occurs. This will help reduce panic and irrational behavior in the case of an actual or suspected bioterrorism event. Quarantined communities must know where they will get medical care, antibiotics and vaccines, clean water, food, and mortuary service if the need arises.

A systems-level approach to dealing with bioterrorism threats, especially those involving communicable diseases, is needed. This approach must consider the integration of multiple modes of management, risk analysis in the face of inherent uncertainties concerning what agents will be introduced, and potential interactions among multiple biological agents. Such research is likely to rely heavily on the techniques of operations research, especially models that can be used for scenario development and training, for rapid response following detection of infected individuals, and for redesigning current systems (including possible patterns of movement) in order to make societies less susceptible to catastrophic outbreaks. Indeed, all of this argues for major development of modeling capabilities.

Uncertain Understanding of the Effects of Biological Weapons

Modeling the likely outcomes of different bioterrorism attacks is important for two reasons. It provides insight into the severity of the threat posed by the proliferation of biological weapons, and it allows one to estimate the effectiveness of different defensive responses (and hence the priority one should assign to each). Modeling efforts over the past decade, at least those publicly available, tend to emphasize worst-case scenarios—broadscale attacks involving millions of human casualties, if not fatalities. While such scenarios may be possible under the right circumstances, they probably are less likely than localized threats. In any case, a wider range of simulations is required to capture the range of possible outcomes. Here there is a major need for training; a critical mass of competent scientific expertise in epidemiological modeling has not to date been adequately supported. Such efforts should become major responsibilities of NIH, CDC, and DOD.

Constructing models may be easier, however, than supplying them with

meaningful data. There are gaps in our understanding of the factors that affect biological agents' dispersal and uptake by humans, animals, and plants. For example, uncertainties of a factor of 10 or more in the LD_{50} values and a factor of 2 or more in the probit slopes (i.e., the dose-response curves) for different agents are common. These uncertainties are even greater if strain type is not known or the mechanism and magnitude of environmental decay rates for different agents are not well understood. Moreover, the incubation period (and its dose dependence) for different agents can vary by factors of 2 or more; and diurnal and weather variations can easily affect the contaminated area by an order of magnitude or more for open-air releases (typically the highest-casualty scenarios). Finally, uncertainties surrounding the amount and purity of the agent, the aerosolization efficiency for 1- to 5-micron particles, reaerosolization for agents that have settled onto the ground versus other surfaces, protection factors associated with buildings, and breathing rates can easily affect the inhaled dose by an order of magnitude or more.

These factors produce an irreducible uncertainty of several orders of magnitude in the number of people who will be infected in an open-air release. Moreover, the onset of disease may occur several times faster or more slowly than predicted, and this can have a significant impact on the efficacy of medical prophylaxis administered at a specific time after release. When bounds on these uncertainties are taken into account, the mean and variance of different attack outcomes may yield a different picture of the magnitude of the medical response required to cope with attacks—it is possible, in other words, that response options may be relatively insensitive to these uncertainties. However, the psychosocial consequences of a biological warfare attack (i.e., the disruption and terror caused by the event) will likely remain very large and difficult to quantify. Other transmission modes (water, food, animal vectors) create similar uncertainties, as do attacks directed at livestock or crops. Nonetheless, modeling and scenario building will be essential for cities and states to evaluate and improve their capacity to respond.

Recommendation 3.6: Agencies with relevant expertise (such as NIH, CDC, and DOD) should develop and support the development of models—taking into account a range of incubation periods, transmission dynamics, and variables of climate, population, and migration—to simulate the release of contagious and noncontagious agents. Such modeling may resolve many of the uncertainties about the effects of biological weapons.

Substantial uncertainties regarding mechanisms of pathogenesis would still remain, however; the only way to resolve them is through new experiments that involve virulent organisms and animal models of human disease. This fundamental work, which has been neglected in the age of molecular biology, underlies much of what must be done to develop new vaccines, broad-spectrum antibiotics and antivirals, and preclinical and traditional diagnostics. And, work must

proceed in parallel on nonpathogenic bacteria and viruses, where many of the molecular mechanisms essential to our understanding of pathogenic organisms can most readily be deciphered. For example, new antibiotic discovery is dependent on an understanding of fundamental cellular mechanisms that are held in common among bacterial pathogens and nonpathogens. Careful oversight of experiments with pathogenic organisms is essential to ensure that they are not in violation of the Biological Weapons Convention of 1972.[3]

Recommendation 3.7: Expand investigations into the pathogenesis of infectious agents. Review the state of knowledge on the mechanisms of pathogenesis of all bioterrorist agents and of host responses to them, and initiate an action plan to conduct laboratory research using the latest molecular biology tools. This research will enhance understanding of the points at which these threats are most susceptible to useful intervention and will help identify new targets for developing diagnostics, drugs, and vaccines.

Microbial Forensics and Analysis of Trace Evidence

The overall lack of knowledge about how to respond to a given attack, together with the lack of intelligence information to help identify the organisms or chemical agents used in an attack, presents major vulnerabilities. But the importance of microbiological forensics in reducing these vulnerabilities was largely overlooked until the recent outbreak of anthrax. Its importance is that the sophisticated scientific and organizational mechanisms of forensics can be the means for determining the states or persons responsible for the attack and for formulating strategies to deter future attacks (Cummings and Relman, 2002).

The U.S. criminal justice, national security, public health, and agricultural communities have more than adequately demonstrated that physical evidence and subsequent forensic investigations are crucial to the investigation of a crime. Similarly, preventing the use of biological weapons, responses to their use, and adequate defenses against them depend in large part on the ability of forensic analyses to attribute (or exclude) the source of a material with a high degree of scientific certainty. The ability to characterize biological weapons might also contribute to deterrence. But although advances have been made in forensics for specific biological agents that may pose a threat, a far more aggressive, compre-

[3]From the Web site of the Harvard Sussex Program on CBW Armament and Arms Limitation: "The Harvard Sussex Program on CBW Armament and Arms Limitation, with advice from an international group of legal authorities, has prepared a draft convention that would make it a crime under international law for any person knowingly to develop, produce, acquire, retain, transfer or use biological or chemical weapons or knowingly to order, direct or render substantial assistance to those activities or to threaten to use biological or chemical weapons." More information is available online at <http://www.fas.harvard.edu/~hsp/cbwcrim.html>.

hensive, and coordinated R&D program is needed. Such a program could then lead to fully tested forensic capabilities for all known biological agents that might be used in an attack.

Lessons should be drawn from the forensic community's experience with human DNA over the past few decades, and alternative approaches to microbial forensics should also be explored. For example, knowledge of microorganisms, the methods used to profile them, and the responses of mammals (particularly humans, domesticated species, and sentinel species) to infections with these microorganisms can be used to determine whether an attack with a biological agent can be effectively correlated with a particular place, event, process, or time. Biological trace evidence, microchemical analysis (analysis of information about the agent carried along with the biological weapon during manufacture, storage, handling, and release), and the feasibility of using tagged organisms should be comprehensively investigated to determine their value in the characterization and comparison of the biological agents used in different weapons. Many in the biological warfare defense community believe that it should be possible to use a combination of DNA sequence information (occurring naturally) and/or deliberately introduced additional DNA sequences (stegnographic tags) to uniquely mark and identify all known pathogenic species. In this way, it may eventually prove possible to assign a unique code to every strain and variant, which would help in forensics, attribution, and defense. Such tags might even be encrypted.

Recommendation 3.8: Develop and coordinate bioterrorism forensics capabilities. Federal agencies with missions in defense and national security should lead in establishing this new multidisciplinary, multilayered field. A comprehensive study should be performed to determine the capabilities of and needs for bioterrorism forensics, and an integrated national strategy and plan formulated.

Investments and outcomes in the new field of bioterrorism forensics should be fully coordinated among agencies, with the program design, implementation, management, and oversight involving those agencies that actually have expertise in relevant sciences—including, of course, forensic science. The new field should cover human, animal, and plant pathogens. The information resident in the genomes and proteomes of organisms should be fully exploited, as should trace materials and chemical evidence associated with those organisms.

The strategic objective of a bioterrorism forensics program is to establish systems for the high-resolution analysis and specific identification of all materials and substances used (or intended for use) in bioterrorism. Although the committee recognizes the extreme difficulty of the task, the desired outcome is the absolute attribution of a biological weapon to its source—the identification of persons, places, processes, or instruments involved in the attack. The ability to substantially reduce the number of possible sources or individuals involved in bioterrorism, and the ability to completely exclude the possibility of an act of

bioterrorism, are equally important. So is the ability to understand the limits of the bioterrorism forensics process at any given moment and to accurately interpret and communicate results.

An Approach to Defining Bioterrorist Threats

Pathogenic microorganisms and the toxins produced by living organisms pose a threat to national security whether they occur in their natural state or are released in bioterrorism attacks. In either case, the greatest threats to human health in the United States come from emerging and reemerging infectious agents that sporadically occur in nature. The population is highly susceptible to such infectious agents, and the mortality rates among infected individuals can be high. Such agents in a bioterrorism attack could easily be spread to large numbers of individuals (Peters, 2002).

As part of a risk analysis, one can classify infectious agents and diseases in relation to these sorts of factors. Thus an eradicated disease agent to which there is currently a high degree of susceptibility, for which there is a high rate of mortality among infected individuals, that can be spread as an aerosol, and that can continue to be spread via contagion—in effect, a worst-case disease—could inflict the most casualties. Smallpox is such a disease, and it is at the top of the list of biological agents that may pose a threat. Once measles is eliminated (Hilleman, 2001) it will join smallpox in this category if immunization against measles is halted (as was done for smallpox) and the population becomes highly susceptible. This has important policy implications for the continuation of immunization against a disease agent after elimination of its natural occurrences.

Previously circulating pandemic influenza strains, most notably the 1918 Spanish influenza (Taubenberger, 2000) and the 1957 Asian influenza (Cox and Subbarao, 2000), and influenza strains of novel subtypes—e.g., the 1997 H5N1 strains from Hong Kong—have pandemic potential in humans. Ebola and hemorrhagic fevers (the causative viruses of which, however, are less easily spread from person to person than influenza viruses) would also have the characteristics of rare diseases that are communicable, to which there is a high degree of susceptibility, and for which there is a high rate of mortality among infected individuals. A genetically engineered pathogen could also have these characteristics and would need to be viewed as being among the most serious potential biological threats. The difficulty is that such genetically engineered pathogens could be created from virtually any biological pathogen or even vaccine strain; thus it will be challenging to develop vaccines or therapeutic antimicrobial agents in advance of a bioterrorism attack.

Because eradiated or genetically engineered agents often do not occur naturally or are difficult to obtain from nature, the best source for terrorists is a research facility. It is thus appropriate to impose significant restrictions in terms of oversight and apply stringent security precautions for biological agents that

pose high-level risks. Security guards, surveillance systems, personnel checks, and testing of personnel can be used to ensure that such biological agents are not removed from research facilities.

In contrast, biological agents with the potential to damage U.S. agriculture most often occur naturally in some part of the world. These agents can easily be obtained (domestically or overseas) and can readily be released, given the general lack of security on farms and fields and their formidable size. For example, foot-and-mouth disease was widespread in the United Kingdom in 2001. A shoe from someone who walked on an infected farm would have been able to carry enough of the agent into the United States to cause an outbreak. Although U.S. border inspections for such potential introductions were heightened during the outbreak in the United Kingdom, the methods used were heavily dependent on the honest answers and voluntary compliance of the traveling public. It is likely that a determined terrorist could circumvent such an interdiction approach.

Similar issues arise for plant pathogens and pests. For example, citrus canker is a bacterial disease of woody perennials that is endemic in several parts of the world where citrus is grown. It has recently been reintroduced into the United States, in Florida, and has had significant adverse impacts on the state's citrus industry. For agriculture, given that would-be terrorists have access to various naturally occurring threats, it will also be important to consider the possibility of the intentional release of multiple types of agents at multiple sites.

For biological agents that may be used by terrorists and that occur naturally, it is appropriate to use lower levels of security and less direct oversight. The level of such oversight may still be significant and should be designed to offer real protection against the acquisition of biological agents that may be used as weapons. Significantly higher levels of security should be applied to any weaponized biological agents—for example, anthrax spores that have been treated to make them easily aerosolized.

Developing Antimicrobials and Antivirals

The diversity of existing biological weapons and the ever-increasing number of possibilities through use of genetic recombination preclude simple therapeutic countermeasures to bioterrorism. The Soviets are known to have developed at least 30 biological agents. While it might only take 1 to 3 years to develop a new biological weapon, the average development time of a new drug or vaccine is 8 to 10 years. Thus with respect to development of countermeasures for biological weapons, a great need exists for broad-spectrum antibiotics and antivirals. Based on current knowledge, technology, and genomic databases, the goal of broad-spectrum anti-infectives is achievable.

Existing countermeasures for known threats are limited. For the potential biological weapons on the CDC "A" list, there are only two vaccines available or in production (anthrax and smallpox), one antiviral, and a limited number of

classes of antibiotics. Supplies of both vaccines are currently limited. While smallpox vaccination is effective, it elicits dangerous and potentially lethal complications in a number of individuals, and because it is a live-attenuated vaccine, it poses a significant risk for all immunocompromised individuals. The limited antibiotic armamentarium is an even greater concern with respect to future threats, especially in light of an increase in the number of new and reemerging infectious diseases and a marked rise in resistance to existing antibiotics. When the issue of resistance is laid against the dearth of new classes of antibiotics being developed and commercialized today, it becomes clear that no public health response to bioterrorism is likely to prove effective without a wider range of antimicrobials to draw on.

Work must proceed in parallel on nonpathogenic bacteria in the same class as the pathogen. New antibiotic discovery is dependent on an understanding of fundamental cellular mechanisms that are held in common among pathogens and nonpathogens. In most cases, the nonpathogenic cousin has far superior genetics and a deeper database of gene function and regulatory networks allowing discovery and development to proceed at a faster pace. Most antibiotic discovery is, in fact, based on work in nonpathogens that is then directly applicable to the pathogens on the list of biological warfare agents.

An Interagency Task Force on Antimicrobial Resistance has set forth recommendations for judicious use of existing antibiotics; they appeared in the *Federal Register* almost 2 years ago.[4] Although the recommendations were widely endorsed, funds have yet to be appropriated by Congress to implement the plan. Given the long lead time required for development of new antibiotics, we must preserve those we have. Thus it is essential that the recommendations of the task force be implemented without further delay.

Unfortunately, the complacency associated with infectious diseases in the 1960s and the general confidence in existing antibiotics largely arrested the production of new classes of antimicrobials. There has been only one new class in the past three decades, and resistant strains emerged prior to its launch. But the situation may be changing for the better. The public attention to the antibiotic crisis in the early 1990s, coupled with the potential for discovering new antibiotics using genomics, high-throughput screening, microarrays, combinatorial chemistry, and structural biology, has resulted in industry's reinvestment in antibiotic research.

At first glance, the current antibiotic pipeline looks encouraging. There are more than 18 antibiotics in Phases I through III of clinical development. However, there are no new classes or targets for antibiotics. In particular, there are no new classes of broad-spectrum antibiotics, and the outlook for antivirals, particu-

---

[4]*A Public Health Action Plan to Combat Antimicrobial Resistance* appeared in the *Federal Register* on June 22, 2000 (Volume 65, Number 121). The report is available online at <http://www.cdc.gov/drugresistance/actionplan/html/index.htm>.

larly broad-spectrum agents, seems even more distant. These deficiencies are critical, as the chances for use of a multi-drug-resistant recombinant organism in future attacks is high. Here again, the deciphering of the genomes of major pathogens and the analysis of their function by the new field of bioinformatics will reveal new potential drug targets—most notably, targets that are present only in bacteria or viruses and not in human cells (such that broad-spectrum drugs can be developed that are likely to have few adverse effects on the human host).

The need has never been greater for research, in both the public and private sectors, aimed at development of novel antimicrobials. However, recent analysis indicates that most, if not all, major pharmaceutical companies have over the past 3 to 5 years *decreased* their investments in drug discovery related to antibiotics, and few are exploring antiviral agents. These changes have resulted from higher regulatory hurdles, competing priorities, and a shrinking market. Thus, new classes of antimicrobials will not emerge in the next decade without a major strategic shift.

Rapid Vaccine Development

Bioterrorism attacks might not be restricted to the dissemination of known pathogens. Variants that have been engineered by current molecular-biology-based methods to alter or mask surface antigens—so as to avoid detection by the immune system—could also be used in such attacks. The following question arises: How quickly and by what means could a new vaccine be developed and deployed to protect against a novel pathogen?

Before that need is upon us, we should act now to tackle several challenges to overcome the critical shortfall of research in vaccinology:

- The genome sequences of all plausible organisms that could potentially be used in a bioterrorism attack, including naturally occurring variants, need to be determined. This information will greatly facilitate the identification of any engineered variations in a weaponized strain.
- DNA-based vaccines (including vaccines that use defective viruses as carriers) should be more fully investigated for human application, as their use represents a potential quick path from determination of the genome sequence to the availability of a vaccine. Recombinant human antibody technologies should be explored, including novel delivery systems.
- Recombinant protein expression provides another pathway for the development of relevant antigens, but more research is needed to determine ways to make recombinant proteins as effective as immunogens.
- More effective adjuvants are needed.
- The development of vaccines against toxins, as opposed to pathogenic organisms, should also be explored.

- Better surrogate animal models are needed for testing vaccines against novel pathogens.
- Improved vaccines against known agents (like smallpox virus) are necessary if immunocompromised subjects are to be safely protected.
- A low cost per dose and stability at ambient temperature are important goals if vaccines are to be shipped to troops in remote locations or to populations in developing countries.
- Antibodies produced for medical use may provide an effective way to ameliorate the effects of a toxin or an infectious agent.
- The regulatory, legal (liability), and ethical issues associated with new vaccines are complex and must be addressed. Could vaccines developed by certain standard protocols be preapproved by the Food and Drug Administration (FDA) to streamline vaccine deployment, even if only at times when a certain high threshold of infection or mortality had been surpassed?
- Vaccines must be produced and stored in multiple secure locations, as the vaccine itself could be a target in a terrorist attack to disable our ability to respond.
- The possibility of using vaccines effective against combinations of antigens from different viral pathogens needs to be investigated.
- Further work in basic immunology needs to be done to obtain an understanding of whether it will be possible to develop drugs that will up-regulate an immune response to pathogens, including organisms used for bioterrorism (immune modulation).

The application of microbial genomics to the development of a novel meningococcal vaccine is one instructive model to consider here (Pizza et al., 2000). In addition, over the past several decades there has been an explosion of basic knowledge about virus structure, the genetic organization of viral genomes, and the mechanisms of viral replication. This knowledge presents us with many potential targets for antiviral therapy. Only a tiny fraction of such targets has been exploited to date. An informative example of success in this area is development of protease inhibitors, such as anti-HIV drugs. The discovery that processing of certain HIV proteins by the protease is essential for virus multiplication came out of basic research on viral proteins. The demonstration that the protease is essential for infectivity was published in 1988. The first protease inhibitor was approved by FDA in 1995. It is highly likely that similar approaches would result in useful therapeutics to counter viruses that might be used for bioterrorism.

Recommendation 3.9: Increase research and development on therapeutics and vaccines. Support basic and clinical research to discover molecular targets in bacteria and viruses, develop broad-spectrum antivirals and antibiotics, and devise treatments that enhance or stimulate protective host responses (both innate and acquired). Similarly, continue to expand and

deploy the capability to use genomics to rapidly identify engineered mutations or altered virulence factors, create a generic platform to develop a vaccine against recombinant pathogens, and employ streamlined testing and regulatory processes to assure adequate efficacy and safety while expediting delivery.

Improvement and Testing of Environmental and Personal Protective Equipment

As described in *Chemical and Biological Terrorism* (IOM, 1999), personal protective equipment (PPE) includes clothing and respiratory apparatus designed to shield an individual from chemical, biological, and physical hazards. Availability (and even knowledge of availability) of such devices can reduce anxiety among first responders, health-care providers, and potential victims. In general, PPE is more effective against chemical agents, because biological agent incidents are not likely to be evident until well after release of the agent.

Protective methods aimed at preventing the pathogen from entering the body are usually physical rather than biological and do not depend on the detailed structure of the pathogen. Available filtering methods depend only on particle size. Like most physical methods, filtering methods available today have the characteristic that they are not 100 percent effective, but they are able to sharply reduce the number of casualties. What is remarkable is that a capability exists based on existing products that can be put into service rapidly. HVAC filters in large buildings can be upgraded at minimal cost (see Chapter 8); other similar filtering devices can be used in the home. Simple cheap masks, about the size of a folded handkerchief, are available and probably provide a high degree of protection. These devices must be tested by government agencies and information must be provided to citizens about their effectiveness.

An array of equipment currently exists (e.g., gloves, gowns, masks, eye protectors, respirators, protective suits), but technical problems remain—for example, heat stress in suits, permeable respirators, and difficulty of use. Also, there is no uniform testing standard for some of this equipment. In particular, testing is needed for antipathogen devices in order to distinguish personal protective equipment that is truly protective from items that generate a false sense of security (and that could increase people's risks by unknowingly putting them in harm's way).

There is also a need for research on environmental protection devices that safeguard buildings and homes from biological and chemical-aerosol threats. For example, less expensive HEPA (high-efficiency particulate-arresting) filters for heating, ventilating, and air-conditioning systems could provide a real defense against terrorist attack on buildings and landmarks; they could also *prevent* exploitation of ventilation systems by terrorists. Such research might have non-

counterterrorism application as well; it could provide knowledge about the use of filters for reducing the current epidemic of asthma in U.S. cities, particularly among children.

Recommendation 3.10: Improve environmental and personal protective equipment. Agencies such as EPA, NIOSH, CDC, DOD, and DOE should perform and support research on new technologies that increase the protection factors of such equipment, and ensure uniform testing oversight to certify efficacy.

Approaches to Preparing the Health Care System for Response and Recovery: The Need for Surge Capacity

The U.S. health care system has focused on efficiency in the past decade. Redundancies have been eliminated through hospital closures, decreases in the numbers of physicians in many specialty practices, and consolidation of traditional public health activities within health care delivery organizations. Furthermore, the budgets of many agencies that could deal with significant epidemics have been curtailed because no such incidents have occurred in the United States in recent years.

Efficient systems use resources to deal with predictable health problems, but almost by definition they lack the resilience (in the form of excess capacity) to deal with unusual episodes of disease, particularly large-scale outbreaks or those that may result from an act of bioterrorism. The challenge is to devise a system that would create capacity on demand to cope with sporadic and potentially very large demands on the health care infrastructure without destroying the efficient use of resources that characterizes the current situation.

It is probable that the given medical capacity in any community can respond immediately to a terrorist attack, providing the following two conditions are met:

- *The attack does not destroy the hospitals and emergency departments in that community.* A chemical attack might destroy multiple hospital emergency departments or contaminate them so completely that they could no longer be used; a biological attack could quickly spread to medical personnel, thereby effectively destroying their capacity to respond.
- *The attack is short-lived and can be handled within a short time frame (less than 24 hours).* For example, during the attack with sarin on the Tokyo subway in 1995, there were few fatalities and a small number of serious cases. Yet the total number of patients (of all types) created an overwhelming workload for the emergency departments of Tokyo hospitals, though only for a short period of time. Had the attacks continued on a daily basis (as in the case of a biological agent that would spread over time, such as the plague bacterium or smallpox virus), there would have been a need to divert some capacity to care for the usual

daily workload—thereby reducing the number of staff medical professionals for handling the bioterrorism-related workload.

In most urban communities of the United States, a bioterrorism attack could pose major problems for the hospital emergency departments, which are already close to their maximum utilization capacities. Some capabilities do exist for reducing the usual workload under such circumstances: patients with marginal cases of illness or minor injuries could be quickly discharged from specialty-care units; elective cases of treatment or surgery could be delayed; and incoming emergency patients could be triaged. However, a large number of patients would continue to need care so that they did not deteriorate into a more serious state. Numerous off-duty medical personnel could be pressed into longer hours of service in a crisis, but the amount of time during which they could respond without relief is still finite. Thus, although the prehospital care agencies might be able to gear up quickly into a disaster mode and accommodate a sudden influx of patients with illnesses related to an acute attack, there is not high confidence that emergency departments in most cities could do the same.

The initial symptoms of the illnesses caused by virtually all infective agents, be they bacterial, viral, or fungal in nature, are very similar. In fact, in everyday clinical practice it is common to confuse a serious bacterial infection with a trivial viral infection, with a loss of opportunity for effective intervention and curative treatment. If individuals or government agencies outside the medical community have knowledge about a pending attack with a specific agent, they may still not be able to dispel such confusion; no mechanism currently exists for the transmission of that information to the medical community so that it can recognize infected individuals and respond to their needs more quickly.

The federal government already has systems in place for responding to disasters. HHS coordinates Disaster Medical Assistance Teams, Disaster Mortuary Operational Response Teams, Veterinary Medical Assistance Teams, and other medical specialty teams located throughout the country. These units can be deployed immediately in the event of natural disasters. In addition, HHS coordinates the National Medical Response Teams for Weapons of Mass Destruction—weapons of mass destruction include chemical, biological, radiological, nuclear, or explosive (CBRNE) agents—to deal with the medical consequences of such incidents, and it is helping metropolitan areas across the nation prepare to deal with such incidents through the Metropolitan Medical Response System.

The Metropolitan Medical Response System emphasizes enhancement of local planning and response capabilities, as well as that of local hospital capacities, tailored to each jurisdiction so that it can best apply local resources to care for victims of a terrorist incident involving a weapon of mass destruction. The resulting systems are characterized by a concept of operations; specially trained responders; a special stockpile of pharmaceuticals; equipment for the detection of biological, chemical, and nuclear agents along with personal protective equip-

ment; decontamination capabilities; communications equipment, medical equipment, and other supplies; and enhanced emergency-medical-transport and emergency-room capabilities. The program focuses on responses to a biological attack, including early warning and surveillance, mass-casualty care, and plans for the management of mass fatalities. The concept of operations also includes the local jurisdiction's plan for augmentation of health and medical assistance by the federal, state, and neighboring governments, including the movement of patients (when local health-care systems become overloaded) via the National Disaster Medical System (NDMS). Each major medical center in cities across the nation must have response plans in place. These should include designated hospital areas that can be converted into isolation zones and decontamination areas, triage plans, and ongoing training sessions for disaster response teams among the medical personnel.

The Office of Emergency Preparedness leads the NDMS, a partnership of four federal agencies (HHS, DOD, the VA, and FEMA) and the private sector. The system has three components: direct medical care, patient evacuation, and nonfederal hospital care. NDMS also includes more than 7,000 private sector medical and support personnel organized into 80 disaster-assistance teams. These teams provide immediate medical attention to sick and injured individuals during disasters, as well as mortuary and veterinary care when local emergency-response systems become overwhelmed.

All of these systems (e.g., NDMS and the Metropolitan Medical Response System) should be supplemented with additional local capacities for responding to attacks on humans, animals, and plants. A national, regional, and local planning process should identify human and other resources that could be brought out of reserve during such times. In addition, public health laboratories need to build surge capacities as well as expertise in containment. Microbiology laboratories are the first lines of defense for the detection of new cases of antibiotic resistance, outbreaks of food-borne infection, and a possible bioterrorism event. Maintaining high-quality clinical microbiology laboratories on site or near the institutions and communities that they serve is the best approach at present for managing infectious diseases and detecting resistance to antimicrobial agents. However, a public health reserve system, consisting of certified laboratory personnel with the ability to provide expertise when the health care system becomes overloaded, needs to be created. In addition, before a crisis occurs, it is critical to have in place agreements between public health and emergency response agencies across jurisdictions. Drills using both threats and scenario models can test the full range of capabilities and assure the availability within a short distance of Level 4 public health laboratory capability.

Recommendation 3.11: Create a public health reserve system and develop surge capacity. As part of a broader planning process, create a health reserve system of health care professionals (modeled on the military reserve

system), and prepare local and regional laboratories for deploying surge capacity to supplement and enhance disaster-response capabilities.

Approaches to Preparing the Food and Agriculture System for Response and Recovery

The U.S. food and agriculture system has undergone profound changes since World War II that have increased the vulnerability to plant and livestock diseases and to widespread human illnesses caused by food-borne pathogens. Food processing and distribution have become increasingly concentrated. For example, four companies now slaughter and process 85 percent of the domestically produced meat, livestock is raised in large, centralized feeding operations, and vast amounts of land are devoted to one or two crops, such as corn and soybeans.

Meanwhile, government support for agricultural research has remained flat (in constant dollars) for nearly 25 years. The private sector supports more agriculture research than the state and federal governments combined, but most of these industry initiatives are in the development of biotechnology products, pesticides, and other inputs to agricultural production.

A USDA-state system of laboratories that investigates outbreaks of livestock diseases does exist, but it varies somewhat in structure from state to state, with some relying on state laboratories and others on colleges of veterinary medicine or agriculture, usually located at land-grant universities. Within USDA, the Animal and Plant Health Inspection Service (APHIS) leads efforts to prepare for and respond to outbreaks of crop and livestock diseases, both indigenous and exotic. APHIS develops the basic emergency-response plans, while state agriculture departments extend the plans to apply to the conditions and administrative structures within their domains.

Recommendation 3.12: Create an agricultural health reserve system and develop surge capacity. As part of a broader planning process, create a reserve system of veterinarians and plant pathologists (modeled on the military reserve system), and prepare local and regional laboratories for deploying surge capacity to supplement and enhance disaster-response capabilities.

Communicating Risks and Responses to the Public

In 2000, a workshop cosponsored by the Defense Threat Reduction Agency (DTRA), the FBI, and the U.S. Joint Forces Command was held on the communication of risk resulting from a weapons of mass destruction (WMD) attack. A report published in March 2001 describes the results of the workshop and recounts lessons learned from past experiences, addresses unresolved issues that were identified by the expert participants, and presents prioritized recommendations for future research, analysis, and other activities (DTRA, 2001).

A disaster response program should include many elements if it is to be successful in dealing with the effects of a WMD attack and restoring public order. In the United States, several agencies at the federal, state, and local levels have been assigned to handle contingencies such as natural disasters, chemical spills, and nuclear mishaps. The Federal Response Plan, a signed agreement among 27 federal departments and agencies, and including the American Red Cross, provides a mechanism for coordinating delivery of federal assistance and resources to augment state and local efforts in major disasters or emergencies. This plan, however, does not describe an integrated, comprehensive blueprint for crisis/risk communications in the event of a large-scale disaster such as a WMD attack. It should be noted that in the 1918 pandemic of influenza, there was a severe lack of mortuary services and facilities, which must also be provided for by the plan.

To help fill the gap, research and analysis on communication and awareness campaigns, and training and preparation, are needed (see Chapter 9). However, it is essential that all federal agencies involved in response develop, through a panel of outside experts, a plan for analyzing data, developing a response, coordinating the response with other agencies and the Office of Homeland Security, and communicating with the public.

Development of Treatment Protocols

In most cases, there is insufficient research and information on which to base a sound public health protocol and medical response in the event of a biological attack. We cannot, for example, answer the following questions with confidence: How long should individuals continue antibiotic treatment after exposure to biological agents? How long after exposure will vaccination be effective? What other types of interventions will increase survival rates and decrease spread of the disease?

Sound protocols are a necessary prerequisite for communicating information about appropriate postattack responses to the public, physicians, and public health officers. The anthrax attacks of 2001 illustrated the lack of preparedness in this area.

Recommendation 3.13: Develop protocols for public health responses to bioterrorist attack. OHS should develop a plan for achieving this objective, and HHS, through its various agencies, should support the necessary research.

Development of Decontamination Protocols

At present there are few data on which to base decontamination procedures, particularly for biological agents. A review of the literature shows that dose-response information is often lacking or controversial, and that regulatory limits

or other industrial health guidelines (which could be used to help establish the maximum concentrations of such agents for declaring a "decontaminated" environment) are generally unavailable or not applicable to public settings (Raber et al., 2001). Moreover, the correct means for identifying the presence of many biological agents are not known, nor is the significance of the presence of biological agents in the natural environment (e.g., anthrax spores are found in the soil in some parts of the United States). Research is therefore needed to determine what level of cleanup will be required to meet public health needs in the aftermath of a bioterrorist attack.

Although the lack of dose information, cleanup criteria, and decontamination protocols presents challenges to effective planning, several decontamination approaches are available. Such approaches should be combined with risk-informed decision making to establish reasonable cleanup goals for the protection of health, property, and resources. Efforts in risk assessment should determine what constitutes a safety hazard and whether decontamination is necessary. Modeling exercises are needed that take into consideration the characteristics of a particular pathogen, public perceptions of the risk that the pathogen poses to their health, the level of public acceptance of recommendations based on scientific criteria, levels of political support, time constraints in responding to the threat posed by a pathogen, and economic concerns (Raber et al., 2001). Specialized robots may have to be developed and used in highly contaminated or extremely hazardous situations.

Agricultural Decontamination

For agricultural biological threats, critical components of the response include quarantines, disposal of contaminated plant or animal material, and decontamination of products, facilities, equipment, and, in some cases, soil (especially for agents that are persistent and can survive in the environment) (NRC, 2002). The disposal or decontamination procedures used, as well as their effectiveness and acceptability, are highly specific to each biological agent: They depend on the nature of the agent, the commodity affected, and the extent of disease or infestation. For example, foot-and-mouth disease (FMD) is so highly contagious that large numbers of infected and potentially exposed animals may need to be slaughtered and disposed of at the farm of origin. Mass burial and burning are the major alternative means for disposal. Both methods are expensive, repugnant to many people, and raise environmental concerns. Novel methods for carcass disposal, for inactivation of FMD virus in and on carcasses, and alternatives to mass slaughter during FMD outbreaks are urgently needed. Decontamination of products, equipment, or facilities is less of a problem because FMD virus is inactivated by heat, irradiation, or treatment with chemicals at high or low pH.

Similar issues apply to plant pests and pathogens. In general, decontamination of seeds and combines, trucks, or other field or handling equipment is pos-

sible by fumigation with appropriate chemicals, but this is costly, from both an economic and environmental perspective. Eradication, especially of soil-borne spores of plant pathogens, is virtually impossible. Methyl bromide, one of the few standard chemicals used for fumigation of soil and containers, will be banned after 2005 in developed countries and 2010 in developing countries as the result of an international agreement made in response to evidence that the chemical depletes the ozone layer. Live steam can be used to clean up facilities and handling equipment, but its cost and damage to the equipment can make this method unappealing. Alternative methods for decontamination and eradication of biological threats to plants are needed (NRC, 2002).

Recommendation 3.14: Develop methods and standards for decontamination. Develop standards for levels of decontamination and certification of products to ensure safety.

Research is needed on chemical fumigation and irradiation as methods for decontamination of buildings and mail; development and evaluation of novel decontaminants; disposal of crops and livestock carcasses; and decontamination of trucks, railroad cars, container ships, and warehouses used to transport and store contaminated crops, livestock, food, and feed. This effort will require collaboration among all agencies with expertise and a mission in this area, including HHS, EPA, USDA, the Coast Guard, and DOD. Because cross-agency collaboration is often challenging, the Office of Homeland Security should designate a lead agency on these issues and ensure that collaborating agencies provide the necessary resources to identify and support research efforts in this area.

POLICY AND IMPLEMENTATION

Effective preparedness for countering bioterrorism will not only require focused and sustained efforts to build the nation's public and agricultural health infrastructures (including the training of health care professionals in detection, surveillance, prevention, and response); it will also require substantial changes in the way government-supported research is executed. Several overarching strategies are needed to provide the necessary funding for research and development (R&D), mechanisms for response, integration of efforts, and translation of findings into application. The recommendations listed below, which support and facilitate the R&D priorities outlined in previous sections of this chapter, are offered in that spirit.

Develop Scientific and Technological Human Resources

The public and private sectors should explore new funding mechanisms that select for the best ideas and the most productive scientists, that offer great flexibility, and that provide the freedom to pursue bioterrorism-related research in a

protected environment (i.e., not subject to 1- or 2-year budget fluctuations or constraints). The traditional system of reviewing and funding grants and contracts can be lengthy and averse to highly focused, highly managed research initiatives. Although basic and discovery science will continue to be a critical underpinning of all research in countering bioterrorism, a more focused, outcomes-based approach is also warranted. Balance between basic and applied research approaches will be crucial.

One model worth considering is a central organization that directs R&D projects whose risks and payoffs are very high—that is, whose successes may provide dramatic advances—and that pursues these projects with both flexibility and speed. There is a real need for NIH, particularly NIAID, to adopt an approach like this for funding the kinds of high-payoff, high-risk projects that might create innovative scientific tools for addressing bioterror threats.

Recommendation 3.15: Create special research organizations to build expertise in countermeasures to bioterrorism. Federal agencies must build human resources in threat-agent characteristics, pathogenic mechanisms, and responses to bioterrorism-induced disease. Protected environments that foster innovation must be developed to support a cadre of leaders, scientists, engineers, policy experts, and strategic thinkers. These designated research organizations should address both classified and unclassified issues, and special mechanisms for rapid funding should be created to support external research efforts as the needs and opportunities emerge. New mechanisms for funding high-risk, long-term, high-payoff projects should be created in NIH.

Ideally, the new organizations recommended above would be small but have strong interactions with universities and government agencies. They would work in basic and applied science—specifically, to understand pathogenic (virulence) factors at the molecular level and how they affect mammalian systems. And they would also work in product development—specifically, in diagnostics, antiviral and antibacterial drugs, and all stages of vaccine manufacture, from development to pilot production. Clearly, drugs and diagnostics should have dual use, and the range of pathogens studied will inevitably have dual-use spinoffs. As a companion to this initiative, a mechanism for rapid funding should be established for bioterrorism-related research conducted extramurally; this mechanism would select for creative ideas quickly, with a minimum of bureaucracy.

Need for Standards and Standardization

The goals for research on surveillance and clinical diagnostics include rapid diagnostic assays for common pathogens and biological warfare agents. These assays could be used in primary-care settings (point of care) as well as referral laboratories. But standards are needed by which they may be rigorously evalu-

ated and validated, and centralized repositories of standardized reagents and samples are needed as well. Because the development and evaluation of diagnostics require interdisciplinary applied research, however, it is currently difficult to find targeted funding sources and mechanisms.

Recommendation 3.16: Establish laboratory standards. Set up an oversight standards laboratory to evaluate diagnostic and detection tools; to ensure the availability of standard reagents for academia, industry, and government; and to develop appropriate standards on a continuing basis.

The National Institute of Standards and Technology (NIST) is one agency where these sorts of efforts might appropriately be undertaken.

It is to be expected that many new products will be introduced for detecting and responding to bioterrorist threats, but no mechanism currently exists for evaluating them and comparing their effectiveness. An oversight standards laboratory would have the capacity to evaluate biosensors and diagnostic systems for infectious diseases, develop taxonomies of syndromes and data classifications, improve the quality of the expanding DNA and protein databases, validate methods, develop reagents, create internal standards for diagnostic comparisons for the scientific community, and evaluate methods and standards for personal protective equipment and decontamination.

Facilitate Development of Therapeutics and Vaccines: Engagement of Industry

Government has a vital role to play in basic research on countering biological warfare agents through its own institutions, many of which have enormous expertise that has long been brought to bear in the fight against infectious diseases. It would be inefficient, however—and ultimately ineffective—for government to go it alone, without actively engaging private industry in the race to deploy needed biomedical countermeasures. Indeed, the greatest efficiency in this urgent effort is likely to come from working the broadest possible network of synergy among all institutions of established expertise—public sector entities, academic laboratories, private research institutes, biotechnology start-up ventures, and pharmaceutical companies. The fight is big enough and difficult enough to demand that the entire spectrum of available talent and resources be productively engaged. To build this network, a new partnership model for industry and government is needed that goes beyond the current models of government contracting.

Existing mechanisms for government interactions with the private sector cover a wide range: from simply acting as a customer in the marketplace, through NIH grants, to the comprehensive R&D contracting done by DOD. There seems to be no one best way among these mechanisms, nor any clearly better way

beyond them. They all have valid applications, and, in practice, different cases will probably require different solutions. However, there is one principle that must serve as the foundation for any partnership aimed at developing countermeasures for bioterrorism. It is the principle of risk sharing.

Drug and vaccine development is an incredibly high-risk business. Front-end costs start big and grow bigger as development proceeds. The total is often something like $800 million by the time a successful drug is launched—10 years or more from the day it was discovered. The odds against success are long—one compound in 5,000 makes it all the way from the test tube to the pharmacy shelf. And even among newly launched products, only one in three earns back its development costs. Public policy makers must consider whether drugs and vaccines could be developed more cheaply, given the compounds that are languishing in the developmental pipeline because bioterrorism is a small and uncertain market.

At the front end, government could help defray some of the costs associated with discovery and early-stage development. Grants and other forms of direct investment might help, especially with smaller organizations. But given the current needs related to antibiotic resistance in naturally occurring pathogens and to the decline of innovation in antibiotic-drug discovery, risk sharing may need to be considered more broadly.

Government could further reduce the risk to industry by providing some form of legal relief from the product-liability issues associated with new countermeasures. Risk sharing could also help to lower the costs of purchasing and storing biodefense drugs—whether existing or to be developed.

The government's current practice is to determine what quantity of a given material it may need, issue a contract to purchase that quantity, and then stockpile it until needed. This process works well for some products, but it is a very expensive way to purchase pharmaceuticals. A more cost-effective approach would be to contract with drug manufacturers for assured access to the necessary quantities. The manufacturers would have to be able to prove beyond doubt that they could deliver the requisite quantities within the needed time frame. It is essential that production capability occurs at more than one facility and that these facilities be based within the United States. The government would reimburse the cost, build and maintain the inventory, and add a modest profit. In the event of an attack, the government would take control of the inventory at no additional cost. Meanwhile, responsibility for addressing such additional risks as unforeseen spoilage would rest with the manufacturers.

Recommendation 3.17: Facilitate vaccine and therapeutics production. Through public-private partnerships, create research, development, and manufacturing capacities to produce diagnostics, therapeutics, vaccines, and devices to counter terrorism and an oversight laboratory to evaluate, prepare, and standardize methodologies.

Traditional market mechanisms for the development of new diagnostics and vaccines are failing with regard to pubic health generally and response to bioterrorism in particular, where the principal market is likely to be federal and state governments. National orphan vaccine centers, perhaps created as government-owned, contractor-operated (GOCO) facilities, are needed to help bring vaccines for otherwise rare diseases to the stages of mass manufacture. Such centers could help coordinate extramural R&D activities in the public and private sectors as well as perform critical research. In particular, national orphan vaccine centers could coordinate the clinical trials and studies with animals on which licensing would be based, and could serve as conduits for production at industrial facilities (including development of surge vaccine-manufacturing capacity and the training of personnel to produce vaccines that meet FDA standards). Such collaboration would require the establishment of new relationships between the public and private sectors.

For development of broad-spectrum antibiotics and antivirals, federal funding should encourage the large pharmaceutical and biotechnology companies to enter the field with the expectation that at least some drugs developed for bioterrorist threats will have dual use—that is, they may be applicable to common infectious diseases as well. Such encouragement for undertaking R&D on new drugs against bioterrorism agents could take the form of streamlined grant mechanisms, financial incentives, and regulatory changes.

Regulatory Reform

Maintaining public confidence in vaccines, and in medical products in general, is critical to assuring overall confidence in the nation's public health programs. But bioterrorism is a moving target, not a single disease of predictable epidemiology, and all potential product uses may not be anticipated. This complicates many decisions about product use.

Current biodefense-related activities at the FDA include meeting with sponsors and sister agencies to encourage interest in developing safe and effective new products, performing research that ultimately facilitates the development of these products, and intensively interacting with product sponsors to expedite availability.

Other steps that the FDA has employed in an attempt to safely speed up the licensure process include the following:

- *Emergency use under investigational new drug (IND) status* allows rapid access to products that have not yet completed requirements for licensure. While IND status makes available potentially lifesaving items, a disadvantage of emergency use under this rule is that the product is not licensed, which not only reflects the true scientific limitations of the data but also raises important issues about public perception.

• *Fast-track processes* can speed up the review procedure so that the FDA can evaluate information as it becomes available and as soon as the sponsor submits it.

• *Accelerated approval* uses surrogate end points to demonstrate benefit. For bioterrorism agents, this might include protective-antibody levels for vaccines. The use of CD4 cells for assessment of antiviral treatment for HIV was one of the first surrogates to be approved under this rule.

• *The "Animal Rule"*[5] is extremely important with respect to bioterror agents. It states that where human efficacy trials are not feasible or are unethical, the use of animal-efficacy data may be accepted as they relate to the desired benefit in humans—usually a significant outcome such as mortality or major morbidity. Clinical studies are still required for establishing pharmacokinetics and for assessing safety. The Animal Rule has postmarketing and labeling restrictions, however, and it does not apply if the product could be approved on the basis of any other standard under the FDA's regulation.

Much more research is needed to establish acceptable criteria for reduction in morbidity and mortality. Human diseases caused by many of the CDC Category A agents are so poorly understood at present that meaningfully defining such criteria for the Animal Rule will be difficult. For some agents—for example, smallpox—appropriate animal models are lacking, and many existing animal models are poorly characterized with respect to lesion character and disease progression.

Animal models (with the exception of those for anthrax) remain poorly characterized with respect to aerosol challenge and disease characteristics in animals receiving sublethal challenge doses. Criteria need to be established with respect to end points that will be acceptable to the FDA for reduction in morbidity and mortality and similarity to human disease—i.e., route of inoculation, challenge doses and strains of organisms to be used, strain and species of animals, and duration of observation periods for reduction in morbidity according the FDA's Animal Rule regardless of route of challenge.

Recommendation 3.18: Allow regulatory exceptions for development of therapeutics and vaccines against bioterrorism threats. The FDA should convene a broadly based conference to consider options and plausible mechanisms for expedited approvals under specific emergency conditions. In addition, for new drugs and vaccines that cannot be tested in humans, mechanisms for indemnification in the case of adverse effects will need to be

---

[5]The Animal Rule is Code of Federal Regulation (CFR) Title 21, Parts 314 and 601: "New Drug and Biological Drug Products; Evidence Needed to Demonstrate Effectiveness of New Drugs when Human Efficacy Studies Are Not Ethical or Feasible." The final version of this rule was published in the *Federal Register* on May 31, 2002, and will take effect June 30, 2002. The final rule can be viewed at <http://www.fda.gov/OHRMS/DOCKETS/98fr/98n-0237-nfr0001-vol1.pdf>

developed. The possibility of encouraging collaboration between pharmaceutical companies in this area by waiving antitrust restrictions—in specific cases justified by the national interest—must also be considered. Thus, in addition to the FDA, the Departments of Commerce, Treasury, and Justice should also be involved in these discussions.

Clearly, in an emergency, someone or some agency has to be authorized to decide, for example, that INDs may not be required, that the informed consent process can be modified, that companies might have to be indemnified, or that companies might have to exchange information or work together, which would require a waiver of antitrust law. The factors that go into such decisions should be discussed by government and industry, and possible approaches recommended to federal agencies.

CONCLUDING REMARKS

Understanding of biological agents as threats to human, livestock, and crop health, as well as to the U.S. economy, must be improved. Special emphasis might be placed on an urgent short list of recognized agents, including *Bacillus anthracis* (the agent responsible for anthrax), variola virus (which causes smallpox), and a few others, for obvious reasons; but much of the preparation should target a broader list and effectively prepare the nation for the unknown.

Appropriate government agencies and scientific organizations must evaluate emerging viruses and the genetic modification of existing viruses. Similarly, they need to consider the impact of genetic manipulations of pathogenic bacteria that enhance their virulence, particularly manipulations that render them resistant to the available antibiotics.

Although there are gaps in the scientific understanding of many potentially deadly biological agents and in the technological advances needed to anticipate and respond to their release, reliance on purely scientific or technological solutions is misguided. A much more inclusive effort is needed to build a seamless system of preparedness and response—one that can exercise the best available tools to counter biological threats.

This task depends first and foremost on rebuilding the public health infrastructure of the United States, which has been allowed to decay as the nation conquered some of the more common infectious and other disease challenges of the past century. The terrorist events of September and October 2001 should serve as a wake-up call to those in the position of setting science and health policies in the United States. Many of the scientific goals described in this chapter cannot be achieved in the absence of trained and well-equipped public health officers, educated and prepared first responders, and clear communication among leaders, the medical community, and the public.

HHS, CDC, and other federal agencies, along with state departments of

health, have begun to consider the best ways to educate health care professionals for effectively responding to bioterrorism. This country's public health schools and professional societies have a major role to play both in training individuals and in researching ways to build a more responsive public health system. Various entities with some knowledge of bioterrorism, such as medical associations, have already prepared educational materials. The American Medical Association, for example, has produced an excellent primer to help physicians recognize and treat diseases likely to be caused by acts of bioterrorism. Regular updating of physicians and other health care professionals, perhaps through mandatory continuing education courses on the agents that pose the greatest threats, would be prudent. Meanwhile, training in this area should be part of the basic curricula for all aspiring health care professionals. Agencies and other institutions also face a major challenge in training first responders, such as firefighters and police, as well as in educating leaders and influential nonhealth professionals, such as teachers, on the realistic threats of bioterrorism and the ways in which they can be empowered to protect themselves and their communities.

But countering terrorism is not the only incentive for such actions. In 1992, the Institute of Medicine published a groundbreaking report, *Emerging Infections: Microbial Threats to Health in the United States* (IOM, 1992). It pointed out that "pathogenic microbes can be resilient, dangerous foes. Although it is impossible to predict their individual emergence in time and place, we can be confident that new microbial diseases will emerge" (p. 32). Thus, preparedness is essential not only for countering bioterrorism but also for facing the constantly evolving threat of infectious diseases, particularly the widespread escalation of bacterial pathogens resistant to all known antibiotics.

In reality, humans and the livestock and crops that sustain them are in a perpetual contest with microorganisms and the diseases that they cause—a contest that requires an armamentarium of knowledge gained from research, surveillance, and improved health practices. Humans and animals are not immune to the threat of infectious diseases just because they have been immunized or eat food and drink water that is regulated and evaluated for their safety. Serious, sometimes deadly, outbreaks of infectious diseases continue to occur naturally around the world. Even when they are treatable, these diseases take their toll in pain and suffering, inconvenience, disability, lost time from work and lost wages, and cost to the health-care system and the economy.

But preparing for the once unthinkable—a biological attack—should also prepare the U.S. population for the inevitable: the natural occurrence (or recurrence) of diseases that can affect all living things. Efforts that protect humans, animals, and plants from bioterrorism will also help us prevail in that never-ending contest with natural threats.

The reader is referred to Box 3.2 for Web sites with additional information on bioterrorism.

BOX 3.2
Resources on the Internet with Bioterrorism Information (Accessed May 2002)

- Centers for Disease Control and Prevention: <http://www.bt.cdc.gov/>
- U.S. Army Medical Research Institute of Infectious Diseases: <http://www.usamriid.army.mil/education/bluebook.html>
- Johns Hopkins Center for Civilian Biodefense: <http://hopkins-biodefense.org/>
- New York City Department of Health: <http://NYC.gov/html/doh/html/alerts/wtc8.html>
- American Medical Association: <http://pubs.ama-assn.org/bioterr.html>
- National Institute of Allergy and Infectious Diseases, NIH: <http://www.niaid.nih.gov/publications/bioterrorism.htm>
- International Society for Infectious Diseases: <http://www.promedmail.org/>
- Biohazard News: <http://biohazardnews.net/>
- American Society for Microbiology: <http://www.asmusa.org/pcsrc/bioprep.htm>
- Wake Forest University Baptist Medical Center: <http://wfubmc.edu/intmed/id/links_biot.html>
- National Academy Press Web resources for first responders on bioterrorism and public safety: <http://www.nap.edu/shelves/first/index.html>

REFERENCES

Anderson, R.M. 2001. "The Application of Mathematical Models in Infectious Disease Research," *Firepower in the Lab: Automation in the Fight Against Infectious Diseases and Bioterrorism,* S.P. Layne, T.J. Beugelsdijk, and C.K.N. Patel, eds., Joseph Henry Press, Washington, D.C.

Barbera, J., L. Gostin, T. Inglesby, T. O'Toole, C. DeAtley, K. Tonat, and M. Layton. 2001. "Large-Scale Quarantine Following Bioterrorism in the United States," *JAMA,* Vol. 286, pp. 2711-2717.

Bradley, R.N. 2000. "Health Care Facility Preparation for Weapons of Mass Destruction," *Prehospital Emergency Care,* Vol. 4, pp. 261-269.

Brinsfield, K.H., J.E. Gunn, M.A. Barry, V. McKenna, K.S. Dyer, and C. Sulis. 2001. "Using Volume-Based Surveillance for an Outbreak Early Warning System," *Academic Emergency Medicine,* Vol. 8, p. 492.

Centers for Disease Control and Prevention (CDC). 2001. "Updated Guidelines for Evaluating Public Health Surveillance Systems: Recommendations from the Guidelines Working Group," *Morbidity and Mortality Weekly Report,* Vol. 50, No. RR-13, pp. 1-35.

CDC. 2000. "Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response, Recommendations of the CDC Strategic Planning Working Group, *Morbidity and Mortality Weekly Report,* Vol. 49, No. RR04, pp. 1-14.

Committee on Emerging Microbial Threats to Health, Institute of Medicine, National Research Council. 1992. *Emerging Infections: Microbial Threats to Health in the United States,* Joshua Lederberg, Robert E. Shope, and Stanley C. Oaks, Jr., eds., National Academy Press, Washington, D.C.

Cox, N.J., and K. Subbarao. 2000. "Global Epidemiology of Influenza: Past and Present," *Annual Review of Medicine,* Vol. 51, pp. 407-421.

Cummings, C.A., and D.A. Relman. 2000. "Using DNA Microarrays to Study Host-Microbe Interactions," *Emerging Infectious Diseases,* Vol. 6, No. 5, pp. 513-525.

Cummings, C.A., and D.A. Relman. 2002. "Microbial Forensics—When Pathogens Are "Cross-Examined," *Science,* May 9.

Defense Threat Reduction Agency. 2001. *Human Behavior and WMD Crisis/Risk Communication—Final Report from a Workshop*, March. Available online at <http://www.dtra.mil/about/organization/finalreport.pdf>.

Fine, A., and M. Layton. 2001. "Lessons from the West Nile Viral Encephalitis Outbreak in New York City, 1999: Implications for Bioterrorism Preparedness," *Clinical Infectious Diseases*, Vol. 32, pp. 277-282.

Gust, I.D., A.W Hampson, and D. Lavanchy. 2001. "Planning for the Next Pandemic of Influenza," *Reviews in Medicine Virology 2001,* Vol. 11, pp. 59-70.

Hilleman, M.R. 2001. "Current Overview of the Pathogenesis and Prophylaxis of Measles with Focus on Practical Implications," *Vaccine,* Vol. 20, pp. 651-665.

Institute of Medicine. 1992. *Emerging Infections: Microbial Threats to Human Health,* National Academy Press, Washington, D.C.

Institute of Medicine. 1999. *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response,* National Academy Press, Washington, D.C.

Institute of Medicine. 2002. *Preparing for Terrorism: Tools for Evaluating the Metropolitan Medical Response System Program,* National Academy Press, Washington, D.C.

Interagency Task Force on Antimicrobial Resistance. 2000. *A Public Health Action Plan to Combat Antimicrobial Resistance*. Available online at <http://www.cdc.gov/drugresistance/actionplan/html/index.htm>.

Layne, S.P., and T.J. Beugelsdijk. 1998. "Laboratory Firepower for Infectious Disease Research," *Nature Biotechnology,* Vol. 16, No. 9, pp. 825-829.

Layne, S.P., T.J. Beugelsdijk, and C.K.N. Patel, eds. 2001. *Firepower in the Lab: Automation in the Fight Against Infectious Diseases and Bioterrorism,* Joseph Henry Press, Washington, D.C.

Layne, S.P., T.J. Beugelsdijk, J.K. Taubenberger, N.J. Cox, I.D. Gust, A.J. Hay, M. Tashiro, and D. Lavanchy. 2001. "Global Laboratory Against Influenza," *Science,* Vol. 293, p. 1729.

MacDonald, J.M., M.E. Ollinger, K.E. Nelson, and C.R. Handy. 1999. "Consolidation in U.S. Meatpacking," *Agricultural Economics Report*, No. 785. Available at USDA-ERS Web site.

Murch, R.S. 2001. "Forensic Perspective on Bioterrorism and the Proliferation of Bioweapons," *Firepower in the Lab: Automation in the Fight Against Infectious Diseases and Bioterrorism,* S.P. Layne, T.J. Beugelsdijk, and C.K.N. Patel, eds., Joseph Henry Press, Washington, D.C.

National Institute of Allergy and Infectious Diseases. 2002. *NIAID Biodefense Research Agenda for CDC Category A Agents: Responding Through Research,* National Institutes of Health, February. Available online at <http://www.niaid.nih.gov/dmid/pdf/biotresearchagenda.pdf>.

National Research Council. 2002. *Countering Agricultural Bioterrorism* (in press).

Nikkari, S., Lopez, F.A., Lepp, P.W., Cieslak, P.R., Ladd-Wilson, S., Passaro, D., Danila, R., Relman, D.A. 2000. "Broad-Range Bacterial Detection and the Analysis of Unexplained Death and Critical Illness," *Emerging Infectious Diseases*, Vol. 8, No. 2, pp. 188-194.

Peters, C.J. 2002. "Many Viruses Are Potential Agents of Bioterrorism," *ASM News,* Vol. 68, pp. 168-173.

Pizza, Mariagrazia, et al. 2000. "Identification of Vaccine Candidates Against Serogroup B Meningococcus by Whole-Genome Sequencing," *Science,* Vol. 287, pp. 1816-1820.

Raber, E., A. Jin, K. Noonan, R. McGuire, and R.D. Kirvel. 2001. "Decontamination Issues for Chemical and Biological Warfare Agents: How Clean Is Clean Enough?" *International Journal of Environmental Health Research,* Vol. 11, pp. 128-148.

Taubenberger, J.K., A.H. Reid, and T.G. Fanning. 2000. "The 1918 Influenza Virus: A Killer Comes Into View," *Virology,* Vol. 274, pp. 241-245.

U.S. General Accounting Office. 2000. *West Nile Virus Outbreak: Lessons for Public Health Preparedness*, HEHS-00-180, Washington, D.C.

Von Bredow, J., M. Myers, D. Wagner, J.J. Valdes, L. Loomis, and K. Zamani. 1999. "Agricultural Infrastructure Vulnerability," *Annals of the New York Academy of Sciences,* p. 894.

4

Toxic Chemicals and Explosive Materials

INTRODUCTION

Toxic, explosive, and flammable materials provide a wide range of potential terrorist weapons for attacking targets of high value and visibility and for grabbing media attention and causing public panic. These materials can themselves serve as targets during their production, storage, transportation, and use in our highly concentrated manufacturing and transportation systems. Chemical weapons, and chemicals used as weapons, can also be introduced through a variety of ready-made distribution systems, such as those for food, water, and pharmaceuticals.

Nevertheless, we are not without resources for countering these threats: Our current capacity to respond to chemical attacks is substantial. The military is trained and equipped for chemical warfare; industrial and academic chemists have significant expertise in dealing with toxic chemicals; and cities and industries have broad capability in responding to their accidental releases. While this collective know-how is not organized to deal with the threats of chemical terrorism within the United States, it is an excellent starting point for building a reasonable level of preparedness.[1]

This chapter describes some of the vulnerabilities associated with toxic, explosive, and flammable materials as weapons of terrorism and suggests ways to reduce these vulnerabilities with existing technology as well as through research

[1]Because plausible chemical attacks do not have the same potential for national-scale disaster posed by nuclear and some biological threats, and because a substantial number of people are already trained and equipped to deal with toxic chemicals, building a capability to deal with chemical attacks is more tractable than doing so for nuclear and biological attacks.

initiatives that could lead to new counterterrorism technology. It is divided into five sections: how chemicals can be used as weapons; the general capabilities that are needed to help mitigate vulnerabilities; possible approaches to protecting some key systems (such as food distribution); and responding to terrorist attacks, both for first responders and the medical system. Finally, the value of a dual-use strategy for developing counterterrorism technologies that are also economically viable is briefly discussed.

BACKGROUND: CHEMICALS AS WEAPONS

Chemicals continue to be weapons of choice for terrorist attacks. They are readily available and have the potential to inflict significant casualties (from a few to perhaps many thousands in technically possible, if improbable, high-end attacks). And they have characteristics that make them attractive for deployment against an open society: easily concealed, undetectable at a distance, and visually indistinguishable from materials in everyday use. Moreover, the potential for their use causes anxiety. While chemical agents may not have the potential to produce the widespread casualties and destruction that could be caused by epidemic biological agents or nuclear weapons, they are more readily available and can cause significant deaths and injuries and disruption in a local area. Historically, problems of delivery were considered a serious barrier to the use of chemical weapons in warfare, and this has been assumed to be a significant constraint on their use by terrorists. But improvements in the technology for disbursing the agents, the willingness of terrorists to commit suicide, and their focus on killing as many people as possible rather than on targeting a specific person or persons, make the danger of attacks with chemical agents a serious threat.

The most plausible use of chemicals as weapons is in attacking aggregations of people in enclosed spaces (e.g., in subways, airports, and financial centers) in ways that would cause disruption to crucial infrastructure services or render them unusable (closing down transportation or financial systems, for example) and potentially causing widespread loss of confidence in the government's ability to protect its citizens. Small quantities of chemicals would usually be all that would be needed (for nerve agents, a few hundreds of grams would suffice). Use of a chemical agent in a nonenclosed space, however, is perhaps of less concern, because a toxic cloud would be subject to the vagaries of wind direction and thermal currents, thereby requiring large amounts (many kilograms) of the agent to cause numerous casualties.

Other ways to use chemicals as weapons include attacking people indirectly by contaminating facilities. Nonvolatile chemicals can be very persistent and thus able to taint their targets—and interfere with critical services—for long periods of time.

Harmful agents could also be delivered through existing systems already designed for rapid and widespread distribution, such as the postal system or the

food and water supply networks (the latter two are discussed in more detail later in this chapter). The anthrax attacks in the fall of 2001 demonstrated the effectiveness of using such systems both to harm people and disrupt an important service. A concerted attack from multiple locations could have resulted in widespread contamination of many of the automated centers where mail is sorted and distributed, resulting in large numbers of infected mail workers and recipients—and possibly even shutting down the U.S. Postal Service. Countless businesses could also have been contaminated. Other mass-distribution systems—currency, newspapers, and junk mail, for example—might also be used to expose large numbers of people to the effects of infectious or toxic substances or to interfere with the functioning of society.

A wide variety of chemicals—including many in common use—could be used as weapons. There are three major classes of such chemicals:

1. Chemical weapons (CW), developed by states for military use; [2]
2. Toxic industrial chemicals that are produced, transported, and stored in large quantities in the civil economy; and
3. Explosives and highly combustible materials.

These three classes of chemicals are discussed below.

Military Chemical Weapons

Chemical weapons were first used in World War I and drew on existing industrial chemicals (chlorine, phosgene). In the period after World War II, a number of countries (especially the United States and the Soviet Union) continued to develop chemicals specifically designed as weapons: The most important of these are the so-called nerve agents and blister agents (e.g., sarin and mustard gases). A number of such chemicals have been produced, and they can be delivered in a variety of ways, including sprays, rockets, mortar shells, mines, and other explosive devices. Several of these chemicals were designed to have very high toxicities (Table 4.1).

Chemical weapons were not used in World War II, and the United States discontinued its CW programs in the 1960s, at least partly on the grounds that CW were not militarily effective. The Soviet Union reached a different conclusion and continued, up to the 1990s, to develop chemical weapons for military use. In fact, chemical weapons appeared to be a standard part of Soviet operational doctrine, with special utility in slowing and blunting offensive operations,

[2]Some biological and radioactive agents are occasionally considered in this chapter along with chemical agents because the responses to attacks with them would be similar. Such biological agents include botulinum toxin, staph enterotoxin, and ricin. Radioactive agents, in this context, mean dispersible radioactive materials (as distinct from nuclear weapons); they are discussed in Chapter 2.

TABLE 4.1 Approximate Toxicity[a] of Selected Chemical Agents

Type	Agent[b]	LCt_{50}[c]	ICt_{50}[c]
Choking	Phosgene	3,200	1,600
Blistering	Mustard (HD)	900	450
Blood	Hydrogen cyanide	2,000 to 4,500	Varies[d]
Nerve	Tabun (GA)	270	200
	Sarin (GB)	35	20
	Soman (GS)	70	35
	VX	15	8

[a]For respiratory exposure to vapor or aerosol; other forms of exposure are also possible (e.g., skin exposure or ingestion).
[b]Abbreviations in parentheses are common military designations.
[c]Dosages expressed as concentration × time (Ct) in units of mg-min/m^3. LCt_{50} refers to a dosage that is lethal to 50 percent of the exposed population; ICt_{50} refers to a dosage that is incapacitating to 50 percent.
[d]The incapacitating dosage depends on the concentration.

SOURCE: NRC (1999), p. 69.

damaging logistics systems, and attacking the cities of adversaries. Large portions of the Soviet technology are now presumed to be widely available to other countries and to an unknown but probably growing number of nonstate groups.[3,4]

The Chemical Weapons Convention, ratified by more than 160 nations (including the United States) in 1997, has the objective of eliminating chemical weapons from state production, storage, and use. It was not specifically designed to reduce terrorist activities. However, it is likely to have some impact because it reduces the availability of CW, as they are destroyed under the observation of the Organization for the Prohibition of Chemical Weapons (OPCW). In addition, certain chemicals and equipment that could be used to produce CW must be routinely reported, and facilities producing them must be inspected. These requirements present a terrorist with obstacles to producing and concealing the production of CW. Further, nations that are members of the OPCW are prohibited from trading with nonsignatory nations—which currently include Iraq, Libya, North Korea, and Syria, among others—in certain chemicals used as precursors.

[3]At least one Middle Eastern country hostile to the United States—that is, Iraq—possesses and has used chemical weapons in military operations and against its own people.

[4]The technology of designed chemical weapons has been relatively static for a decade (since the collapse of the Soviet effort). There is, however, the potential for development of new classes of chemical weapons. The Soviet Union experimented extensively with a variety of agents, and the results could provide starting points for new programs. Some of these could be developed rapidly if significant financial resources and technical expertise were applied.

Despite some protection afforded by the Chemical Weapons Convention, military chemical weapons—and chemicals that can be used as weapons—must still be assumed to be relatively available. Dedicated and trained terrorists might obtain chemical weapons from nonsignatory and noncompliant nations, or synthesize the agents themselves (*Scientific American*, 2001). Making chemical weapons requires some technical skill, but over time much of the information required to make these materials has drifted into the public domain. The most toxic of the common weapons—the nerve agents—can be made using relatively unsophisticated facilities and in quantities sufficient for terrorist attacks (although large-area attacks requiring tons of agents would require large-scale facilities available only to states or large corporations, not to individuals). There are a number of sources that a terrorist might use to get the information needed to make chemical weapons, including the Internet.

The Aum Shinrikyo attack on the Tokyo subway system in 1995—using sarin—proves that fabrication and use of chemical weapons by nonstate groups is now possible and can inflict significant casualties. Twelve people were killed and more than 5,000 injured in this attack (Kawana et al., 2001), and many more would have died if the terrorists had been more sophisticated in their use of the chemical agent. The deployment of chemical weapons is now more a question of the attacker's objectives and competence than of the effectiveness or availability of the technology. In the hands of skilled terrorists, especially if they are willing to die in the effort, CW attacks could be devastating.

Industrial Chemicals

Every industrialized country is heavily reliant on chemicals. The United States is no exception; it produces, stores, and transports large quantities of toxic industrial agents. Certain of these (such as chlorine and phosgene) have actually been used as chemical weapons, as noted above; others (volatile acids, certain industrial chemical intermediates) could cause numerous casualties if released in cities in large quantities.[5] Although the safety record of the chemical industry is very good, these chemicals nevertheless pose inherent risks.

Over the last 20-30 years, significant changes in the chemical and petroleum-refining industries have taken place, driven both by economic and regulatory factors; some of these changes have inadvertently helped to reduce the risks that hazardous materials might be used by terrorists. For example, the movement toward just-in-time supply of materials, while made to reduce costs, has also

[5]A good example is the accidental release of methyl isocyanate from a chemical plant in Bhopal, India, in 1984; over 2,500 people died and more than 100,000 required medical treatment. Although a number of toxic chemicals (such as insecticides) are readily available and might be used in small-scale attacks, they are not likely to cause many casualties and are not the focus of this report.

reduced inventories of hazardous chemicals stored at manufacturing sites. Innovations involving less-toxic starting materials, intermediates, products, and by-products have lowered intrinsic dangers to workers, the public, and the environment and at the same time reduced the availability of materials that might fall into the wrong hands. Over-the-fence manufacturing—whereby the supplier builds a plant immediately adjacent to the customer's plant, or even on the customer's site—provides a reliable source of materials while minimizing transport and storage. Probably the most significant change has been the ability to monitor and control reactions on a real-time basis; real-time control reduces the chances for accidental or intentional releases. These trends show that many technical changes intended to increase efficiency, reduce environmental impacts, and improve safety can also reduce the threat of terrorist attacks.

Despite these advances, the volume of toxic materials in production, transport, and storage is still enormous, and as a result there are still many hard-to-protect targets. Chemicals could be released from industrial facilities or pipelines, for example, using explosive charges or simply by cutting pipes or opening valves. Under some meteorological conditions, release from production and storage facilities could permit a toxic plume to pass over heavily populated areas. Transportation systems (e.g., railroad tank cars, ships and barges, and trucks) allow rapid transport of hazardous chemicals, and terrorists could take advantage of these vehicles' frequent proximity to potential targets (e.g., trains that travel under cities or barges located in harbors) (see also Chapters 7 and 8).

Thus new technologies or further incentives to reduce the amount of toxic materials being moved around the country would be very useful. Taxes placed on transport and storage of highly toxic chemicals, combined with public-private research partnerships, perhaps managed by EPA, could be used to encourage the development of new approaches to on-site and just-in-time production. For example, new process technologies to allow small-scale production of chlorine at water-treatment plants could greatly reduce shipments of this hazardous material.

Explosives and Flammable Agents

Explosives, having many legitimate purposes and being relatively accessible, pose a significant terrorist threat (NRC, 1998). They can be used in large quantities to produce mass destruction, as in the attack on the Murrah Federal Building in Oklahoma City, and in smaller quantities to destroy sensitive or symbolic targets such as airplanes, bridges, or key components of critical infrastructures (e.g., telecommunications networks, electric-power grids, and water supplies). Legally mandated controls apply to industrial and civil engineering explosives, but the quantities in use are large and the control mechanisms imperfect. More important, as the Oklahoma City attack shows, very powerful explosives can be readily assembled from such otherwise innocuous ingredients as agricultural chemicals and fuel oil.

Flammable materials include gases and volatile liquids that could be formed into a vapor cloud and ignited to cause a fire or detonation. They are in common use across the United States for fuel, industrial feedstocks, and a variety of other applications and could be released from production, storage, or transport facilities.

As with industrial chemicals, the distribution systems for explosives and flammable agents are vulnerable to attack. These systems include trucking and shipping networks (especially liquefied natural gas tankers and their shore facilities), railroad lines, pipelines that carry natural gas or other gaseous or liquid hydrocarbons, and underground sewers or utility tunnels. These systems are all susceptible to hijacking and use of explosive or flammable materials as weapons, or to physical damage, with consequent disruption of service. In some cases, injuries and environmental damage may occur near where a pipeline is breeched.

Underground sewers or utility tunnels could be used as conduits for releasing toxic, flammable, or explosive materials. Chemicals could disperse through these systems and eventually emerge from manholes, drains, and other openings, or they could ignite or explode under streets and near buildings (see Chapter 8). Another potential dispersal mechanism is a subway system. Materials in the subway tunnels could be "pumped" through the city by the trains—a particularly effective method for delivering powderized materials like anthrax, but it might also work for spreading chemical agents.

GENERAL CAPABILITIES NEEDED TO HELP MITIGATE VULNERABILITIES

Sensors and Operational Systems for Detecting and Characterizing Chemical Agents

Improved and expanded use of sensors must play a major role in preventing catastrophic terrorism or, if attacks do occur, in minimizing their impacts. Sensors have the potential to thwart terrorist activities in the planning stage, or before or during attempted attacks, and to help identify individuals with malicious intent. They may also be useful in forensic analysis to identify perpetrators after an attack.

Possible applications include the following:

- Improved sensors to detect explosives in luggage and enhance airport security (see Box 4.1 and Chapter 7);
- Sensors to help provide sensitive and rapid warning for the protection of fixed sites (subways, airports, government buildings, financial centers, high-value industries). For example, sensors for ventilation systems capable of detecting deviations from normal conditions and monitoring for chemical and biological agents could be coupled to rapid-shutdown procedures, especially at the final vent (see Chapter 8);

BOX 4.1
Sensors for Airport Security

Development of new and improved sensors should provide many security benefits, but perhaps none is so visible and immediate as the need for increased airport security with minimal passenger inconvenience. Until recently, security at U.S. airports was limited to metal detectors and x-ray imaging. But over the past few years, explosives detectors have been installed that use stationary ion mobility spectrometers (IMSs) or chemiluminescence sensors, both of which are capable of detecting a number of explosives, including RDX (1,3,5-trinitro-1,3,5-triazacyclohexane), PETN (pentaerythritol tetranitrate), TNT (2,4,6-trinitrotoluene), and nitroglycerin. However, given the limited sensitivity of deployed detectors (detection limits of 1-10 picograms) and the low volatility of most explosives, these systems generally require the collecting of particles of explosive for detection. Particle collection requires tedious swabbing of luggage, and careful cleaning of the exterior of a package by a terrorist can greatly reduce the chance of detection. Another limitation of conventional technologies is that particles can be picked up from one object by another, causing a false positive.

However, new and emerging techniques could augment existing detection capabilities. A number of new technologies appear to hold promise for explosives detection, including x-ray diffraction, which detects several types of explosives; microwave/millimeter wave scanners; and nuclear quadrupole resonance (NQR) (NMAB, 2002). The use of NQR spectrometry or neutron capture for explosives detection is based on the unique physical nature of the ^{14}N nucleus (99.6 percent natural abundance) in the nitro groups in the explosive materials. New detection-coil technologies have improved NQR considerably, and the U.S. Army is developing vehicles that use it for landmine detection. However, NQR still suffers from limitations. It has sizeable power and computational requirements, making it unsuited for a portable system. The long relaxation times of the ^{14}N in TNT restrict the number of pulses that can be applied and thereby limit sensitivity for this explosive; there is also a reluctance to expose people to strong radio frequency fields. Neutron capture methods require a neutron source, such as a radioisotope or a particle accelerator, and present other complexities.

Methods to detect explosive vapors have many advantages: Vapor collection from people and luggage can be rapidly accomplished and is minimally invasive. Such detection needs considerable sensitivity, as is provided by mass spectroscopy, and may require new sensor advances. It will also be important to have high-sensitivity systems—unlike IMS, chemiluminescence, NQR, or neutron capture—that are portable and can be used as a handheld wand.

Additional support is needed for research to develop improved methods for detecting explosives at airports.

- Sensors to detect chemical agents or nuclear materials in shipments (see Chapters 2 and 7);
- Sensors to check food, water, currency, and mail for contamination;

- Portable sensors to allow first responders to assay levels and types of hazard at a distance—that is, to allow them to make correct initial assessments without themselves becoming casualties (see Chapter 8);
- Mobile sensors to be used in mapping the extent of a cloud of a volatile agent and to guide civil authorities in controlling population movements;
- Sensors to assist physicians in determining the extent of exposure of patients presenting at hospitals (see Chapter 3); and
- Sensors to assess the level of contamination following an attack and, more importantly, to determine when a site is safe and can be returned to normal function.

As can be seen from the above list, the use of sensors is not limited to the detection of chemical agents; the detection of biological agents and of fissile and radioactive materials is discussed in Chapters 2 and 3. Current sensor capabilities are fairly limited; in many cases, the best "technology" for practical use continues to be trained dogs. Manufactured sensors are often designed for use in specific environments and to be selective for only one or two chemicals. Yet because there is a spectrum of possible threats, sensor systems are needed that can detect a large number of possible chemicals. And, given the ultrahigh toxicity of some of these chemicals, detection systems' sensitivities must be significantly increased. In addition, sensor systems will need a number of different subsystems, including sample collection and processing, presentation of the chemicals to the sensor, sensor arrays with molecular recognition, sophisticated signal processing, and amplification of the transduction events.

Sensor programs funded by the government have not yet produced significant increases in counterterrorism capabilities, in part because the focus has been on the sensor itself and not on the overall system for detecting threats. There is a strong need to focus on systems approaches here—to explicitly consider how the sensor system will be used, by whom, for what purpose, and at what cost. While the common goals for virtually all sensors are that they be less expensive, more versatile, more reliable, and more compact, each of the potential applications listed above will have a different set of most-desired characteristics for a sensor *system*, and development efforts should recognize what trade-offs (between, say, size and versatility) each application demands (see Chapter 11).

One example of a factor that needs to be considered in sensor development is the relevant time scale. Chemical agents have a broad range of times required for their toxic effects to appear. One of the most plausible types—nerve agents—acts rapidly; evidence of toxicity can appear in seconds to minutes, depending on concentrations, exposures, and agent. Similarly, many industrial chemicals (e.g., chlorine, hydrochloric acid) that might be used as improvised chemical weapons are immediately apparent through smell or effects on eyes or mucus membranes at concentrations well below that required for serious toxicity (but if escape from them is not possible, the resulting damage to lungs becomes evident over time).

Some chemical agents, such as mustard gas, for example, have symptoms that appear much more slowly (NRC, 1999). Unconventional agents (e.g., aflatoxins, which can induce cancer in some exposed individuals) might not have observable effects for years. Effective responses to chemical attacks, and to biological attacks as well, need to be tailored to the specific agent involved; thus the choice of the right sensor(s) for the job at hand—whether with respect to the time scale or to other factors—is crucial.

In the United States, government-supported research on sensors is now mainly funded through DOD (DARPA), NSF, and DOE and has produced some significant advances in the sensitivity and other characteristics of the sensors themselves. In particular, sensors with medical applications have reached the market fairly rapidly, even though the DOD programs have focused mainly on military problems (e.g., standoff and point detection in field operations) and military customers. Development of sensors is heavily supported by industry as well, and industrial production facilities are routinely equipped with instrumentation that can detect and identify releases of toxic materials. However, none of these technologies has had any real impact on emergency preparedness, as the market for such applications is small and fragmented. For sensors to be effectively implemented for homeland security, they will need to be inexpensive, widely deployed, and networked.

Thus, although improved detection does not rely on sensors alone, research on sensors being conducted by many agencies, companies, and universities—including, but not limited to, work on sensors to detect explosives—should certainly continue. There are rich opportunities for discovering new technological principles on which sensors might be based.

Recommendation 4.1: A broad-based research program should continue to look for promising new principles on which better sensors might be based.

Presently, trained dogs represent the best broad-spectrum, high-sensitivity sensory systems. Dogs are capable of detecting many more items of interest, including people, explosives, drugs, fuels, and disease, and at lower concentrations than currently manufactured sensors. But the precise chemical signals that provoke responses in dogs remain uncertain; it is likely that the signals are not from a single compound but rather from multiple compounds. In the short term, the use of dogs could be expanded, and dogs could be trained to detect a wider array of targets. In the longer term, however, detailed studies to better understand the abilities of dogs could be useful in designing more broadly effective *manufactured* sensor systems.

Recommendation 4.2: Basic research to study how animals accomplish both detection and identification of trace chemicals should be pursued. These efforts could yield new concepts for better automated systems to reduce our dependence on the use of dogs for detection.

If sensor research is to move forward efficiently, mechanisms to focus and exploit the highly fragmented array of existing programs will be needed. In addition, there should be increased emphasis on converting demonstration systems into practical, commercially available products that can increase the ability of responders to do their jobs safely and efficiently. Model mechanisms for helping to bridge the gap between sensor research and the development of implementable systems include the NIST Advanced Technology Program (ATP), the Small Business Innovation Research (SBIR) programs in place at several agencies, and the DARPA Advanced Concept Technology Demonstration program. Such programs could decrease the commercial risk of developing new types of sensors; government-sponsored purchases of sensor/detector systems to test their utility with first-responder groups would also be of value.

Recommendation 4.3: A new program—with sustained funding—should be created to focus and coordinate research and development on sensors and sensor networks, with an emphasis on the development of fielded systems.

This program should build on the sensor research under way at many agencies and should also include plans for commercialization (favoring dual-use systems) and be backed by exercises, simulations, and testing to establish reliability.

New technologies that offer significant advances need to be constantly evaluated. But evaluating sensor systems is difficult because their effectiveness depends on the operational environment and on who will be using them. Attention must be paid to the way systems are deployed and how alerts from sensors are displayed; people with less specialized training, such as emergency responders, would need different system performance characteristics and require different kinds of information than those with more experience, such as chemical professionals and plant operators.

Recommendation 4.4: Because a bewildering array of counterterrorism technologies (including various kinds of sensors) is coming onto the market, the federal government should oversee a technology testing and verification program that could guide federal research investments and advise state and local authorities on the evolving state of the art.

Data Networks and Processing

In many cases, efforts to prevent terrorism will involve large data streams—from arrays of sensors, for example. It is important to be able to efficiently process and mine the data for useful information, so as to quickly distinguish patterns of actual threats from noise or natural events and to make the information systems accomplishing these tasks secure. These issues are discussed in Chapters 5 and 11.

Improved Filters, Absorbents, Scrubbers, and Membranes for Chemical Decontamination and Restoration of Function

In most cases, the impact of a chemical attack would not be limited to the harm done at the time of the attack. Afterward, it could take a long time to decontaminate the site, as well as to restore public confidence. Restoring the Hart Senate Office Building after it was contaminated by anthrax exemplified the difficulty of decontamination in the wake of a biological attack. Comparable efforts following a chemical attack would be different, but not necessarily easier. Contamination by a volatile agent (e.g., sarin) presents the problem of removing a toxic vapor without releasing it into the outside environment. Contamination with a persistent agent (e.g., VX) poses an additional concern—much of the agent may deposit on surfaces, and the chemicals used in decontamination, such as hypochlorite solution, are generally incompatible with electronic equipment and paper. Regardless of the type of contamination, however, persuading the occupants of the building to reenter and go back to work will require credible technical evidence that it is safe to do so.

Research is needed to identify more effective technologies for removal of contaminants from different media (air, water, and solid surfaces) and to quantify their effectiveness so that appropriate decontamination measures can be developed. These technologies are likely to be specific for the contaminants involved and for the media in which they are dispersed. Contaminants in air or water—chemical, biological, or nuclear—may be present as aerosols (particles of solid or liquid) in air or as particles in water, or they may be homogeneously dispersed, as gaseous contaminants in air or dissolved contaminants in water.

Particles may be removed by filtration, with the specific technology depending on particle size (Accomazzo et al., 1988; Ensor, 1988). Several filtration technologies are available: micro-, ultra-, and nanofiltration membranes for treating contaminated water and HEPA (high-efficiency particulate air) filtration for contaminated air. Improved high-efficiency and low-pressure-drop filter systems could be useful in rapidly treating large volumes of particle-contaminated water or air.

Homogeneously dispersed contaminants may be removed by absorption,[6] adsorption,[7] chemical reaction/neutralization, or selective membrane filtration (Ho and Sirkar, 1992; Majumdar and Sirkar, 1988; Prasad and Sirkar, 1987; Way et al., 1982). Absorbers and filters can be used both to prevent toxic chemicals

[6]Absorption is a process in which a material extracts one or more substances present in a mixture of gases or liquids, accompanied by changes in the material's physical or chemical properties.

[7]Adsorption involves surface adherence, in which a material extracts one or more substances present in a mixture of gases or liquids, unaccompanied by changes in its physical or chemical properties. Commercial adsorbent materials have enormous internal surface areas, typically several hundred square meters per gram.

from entering a facility through the ventilation system and to decontaminate a building after an attack. Carbon adsorbents and molecular sieves (zeolites) are conventional adsorbents; their effectiveness for specific contaminants must be determined and documented. Special adsorbents may need to be developed for hard-to-remove contaminants. Absorption techniques may be used for removing gaseous contaminants from air in conventional scrubbers/packed columns using appropriate solvents. Reactive packed-sorbent (reagent) beds may also be used for removing contaminants from water or air by chemical reaction/neutralization. A need exists to identify appropriate contaminant/sorbent combinations and possible interference factors, e.g., humidity. Some dissolved contaminants may be removed from water with selective membrane filtration; however, membranes require a concentration gradient that may not be available for rapidly dispersing dilute contaminants. Membrane techniques based on preferential diffusion of contaminants will thus be highly specialized for specific contaminants. Microporous membranes may, however, be combined with an appropriate reactive absorbent/adsorbent for the removal of contaminants by facilitated transport.[8] In such an application the membrane simply provides a large surface area for effective and efficient removal of dilute contaminants.

Another area of need is for better methods to contain and neutralize clouds of airborne toxic materials such as ammonia, chlorine, hydrogen fluoride, hydrogen sulfide, and sulfur dioxide. Work to date has shown that large quantities of water must be sprayed in the air to "knock down" any significant portion of such airborne chemical clouds (Dandrieux et al., 2001; Petersen and Diener, 1990). The use of reactive foams in existing fire-suppression systems to counter chemical and biological agents should also be explored.

Recommendation 4.5: Universities, companies, and federal agencies should work together to improve existing technologies and develop new ones for removing chemical contaminants from air and water. Research is especially needed on filter systems capable of treating large volumes, novel media that can help prevent toxic materials from entering facilities through ventilation systems, and methods to contain and neutralize clouds of airborne toxic materials.

The problem of decontamination has been studied for many years at DOD, the national laboratories, and universities. While new approaches may be found in areas already being explored, it is possible that better solutions could lie in

[8]A facilitated transport membrane contains a complexing agent that exhibits an affinity toward one species in a mixture. A reversible interaction between the two selectively enhances the solubility and transport rate of the one species relative to others that do not interact. This transport mechanism can achieve higher separation factors than simple (passive) transport, where species diffuse down a concentration gradient but have little or no interaction with the membrane.

some entirely new direction—e.g., chemically "hardened" surfaces that are non-adsorbing and easily cleaned.

Recommendation 4.6: Under the lead of DARPA, DOE, and NSF, exploratory programs should be initiated in new approaches to decontamination, including hardened structures, protective systems for microelectronics and other expensive equipment, and environmentally acceptable ways of disposing of contaminated material that cannot be cleaned.

In addition to new and advanced technologies for decontamination and filtering, attention must also be paid to low-technology approaches for the protection of both people and buildings. In a large-scale chemical attack, timely warning and advice about appropriate countermeasures could make a significant difference to those potentially exposed. Such countermeasures often involve passive protection (masks, sealed rooms) when levels of contamination are relatively low, yet there are currently no U.S. standards for such protection.

Recommendation 4.7: Working in coordination with others as needed, NIST should take the lead on developing standards and technologies for the passive protection of individuals, rooms, and buildings against chemical, biological, and radiological threats. The developers of such technologies should consider factors such as cost and accessibility to all sectors of society.

Robotic Technologies

Many of the tasks involved in counterterrorism, such as the assessment of attack sites, inspection of containers at borders, and routine surveillance of facilities, are potentially dangerous and dauntingly labor-intensive. Robotic technologies could spare humans from dangerous work, substitute machine time for human time in surveillance, and perform other important functions. Robotic technologies have matured substantially in recent years, but the prospect of robots as autonomous systems, performing complex tasks without human supervision, seems somewhat remote. However, the idea of robots (and especially networks of robots) as *helpers* for emergency responders does seem plausible, given sufficient investment.

Robots could assay damage and rescue casualties in a contaminated environment, carry out decontamination (especially if the process used in decontamination is itself hazardous), and inspect spaces inaccessible to humans (e.g., the interiors of shipping containers). Cities, where terrorist attacks are most likely to occur, provide an ideal environment for robots: There is ample power, the topography of the landscape is predictable, and other resources that might be needed (e.g., decontamination solutions, supervision by human specialists) are readily available (see Chapter 11).

Recommendation 4.8: Agencies with experience in robotics, such as DARPA, should support research on all elements of robotic systems—including sensors, networks, and data communication and analysis. The aim would be to develop robots to assist in chemical (and biological or radiological) defense, thereby reducing hazards to humans and increasing the capabilities of defensive systems.

MITIGATING VULNERABILITIES OF SPECIFIC SYSTEMS

Technology to Secure Industrial Chemicals and Chemical Production and Storage Sites

The chemical industry and the government have been making substantial efforts since September 11 to increase security preparedness. Industry is carrying out joint assessments with the FBI, EPA, Coast Guard, FEMA, the Bureau of Alcohol, Tobacco, and Firearms (ATF), and the Office of Homeland Security. Aspects under examination include security checks of personnel, controlling access to sensitive areas and materials, increasing surveillance, reviewing and changing distribution routes, and reducing quantities of hazardous materials in storage and transit. The experience of large companies in preventing and responding to accidental releases of chemicals is relevant to defense against chemical terrorism; these companies are highly regulated with respect to the reporting and inspection of processes, products, record keeping, shipments, storage, and use, and they have much of the infrastructure required. But smaller companies lack such broad infrastructure for increased security and response; mechanisms by which the government or larger companies could provide expertise and advice might therefore be helpful.

The cast of players is even larger. In the past, security issues were primarily the purview of those who produced hazardous materials; now, transporters and users (including private and government laboratories and educational institutions) must be included in the security chain. This means that industries dependent on hazardous materials (such as mining, construction, electronics, manufacturing, food processing, agriculture, the medical industry, and transportation) will need to pay attention to security concerns as well.

The best defense against misuse of chemical, explosive, and flammable materials is adequate security around the facilities that handle them and in the transportation systems that distribute them. Heightened surveillance and improved techniques for detection and identification of leaks or illegitimate use will help prevent hazardous materials from being acquired, released, or rerouted. But progress beyond the immediate tightening of security will require systematic assessment of vulnerabilities in the complex systems by which we produce, store, and transport chemicals.

Issues requiring careful analysis include the following:

- Industrial plants have not been designed to withstand well-executed attacks involving a number of people, nor is there thorough understanding of (or protection from) the damage that might be done by a well-placed, knowledgeable person within a facility.
- Many industrial operations are controlled by supervisory control and data acquisition (SCADA) systems—computer systems designed to automate and control plant functions. These systems stress interoperability more than security, and a better understanding of how to improve their ability to resist cyberattacks is needed (see Chapters 5 and 11).
- Large quantities of hazardous industrial chemicals are shipped daily in the United States—by truck, rail car, and barge. These shipments often pass through cities or are stored in (or close to) cities. Understanding how to secure these shipments—either by protecting them or by routing them around cities—is important in preventing them from being hijacked and used as weapons (see Chapter 7).

Recommendation 4.9: The Departments of Transportation and Commerce, working with industry and with federal and state law enforcement agencies, should be tasked with developing plans for regulating the movement of hazardous materials through and near cities. These plans should incorporate technologies that allow detection of anomalies in handling and movement.

Ammonium nitrate and urea are used in very large quantities for agriculture and can also be used as explosives—ammonium nitrate was used in the truck bomb that brought down the Murrah Federal Building. British scientists and others have worked for some years to find a way to alter this chemical so that it retains its agricultural benefits but is no longer an effective explosive. This research has not been successful to date, and practical, new approaches to this problem would certainly be welcome (NRC, 1998).

Protecting Food Supplies

Consumers in the United States are very sensitive to suggestions that the food supply might not be perfectly safe. Widely publicized episodes, such as the concern about the pesticide Alar on apples, debate about the safety of genetically engineered food, and ripple effects caused by the association of beef with mad cow disease, exemplify this highly charged social environment, and a good deal of attention is being paid to ensuring safety and purity throughout the various stages of food production, processing, and distribution.

However, protecting the food supply from *intentional* contamination has not been a major focus of the U.S. food industry. Three characteristics of this industry create vulnerabilities to terrorist attack: the concentration of primary produc-

tion in large, monoculture farms; the concentration of commodity food-processing in large centralized facilities; and a tendency to adhere to rigidly defined patterns of quality control that may not detect unanticipated contaminants.

Food production and processing offer many potential avenues for terrorist attack. Protection of the U.S. food supply is generally the responsibility of the Food and Drug Administration (FDA), which is progressively replacing old quality control (QC) and quality assurance (QA) programs with a new methodology called hazard analysis and critical control point (HACCP).[9] In earlier QA/QC methods, samples were drawn from food lots according to a statistical protocol. These lots were then held, pending the results of testing, and released only after each lot passed all tests. HACCP is a system designed to enhance food safety by identifying sources of possible contamination and specifying ways to control them—through changes in source, process, procedure, or structure. HACCP was designed to prevent unintentional contamination, however, and not to deal with *intentional* contamination. Extending the existing HACCP program so that it can be effective against deliberate tampering will require a multidisciplinary reassessment.

Recommendation 4.10: The FDA should act promptly to extend hazard analysis and critical control point (HACCP) methodology to enable it to deal effectively with deliberate contamination of the food supply.

Primary food-production facilities need to be secured from contamination with toxic or infectious agents, but only to an extent commensurate with the hazard—that is, the number of people that might be involved, their likely rate of consumption of the contaminated food, and the time delay from contamination to consumption should all be considered. The time delay is especially important, because contaminated foods consumed slowly over time (such as canned goods) would cause few illnesses or deaths per unit time. Thus, there would be an opportunity to determine the source of the contamination and the lots affected and to accomplish a recall—thereby reducing the consequences of such an attack. By contrast, foods consumed quickly (such as milk, bread, and fresh meats and vegetables) would be less effectively removed by recall, so their production facilities require more security.

Recommendation 4.11: The FDA should develop criteria for quantifying hazards in order to define the level of risk for various kinds of food-processing facilities. The results could then be used to determine the minimal level of protection required for making each type of facility secure.

---

[9]So far, HACCP regulations have been established only for juice (FDA, 2002a) and seafood products (FDA, 2001); those for dairy products are voluntary (FDA, 2002b). In addition, HACCP guidelines have been issued for retail food (FDA, 1998).

This approach, sometimes called "graded security," would define the extent of security measures needed, with the severity increasing in proportion to the risk. It might be conceptually similar to the classification system created by NIH for laboratories working with biohazardous agents.

Recommendation 4.12: The FDA should convene panels of experts in major areas of food production to assess vulnerabilities and recommend corrective actions. This effort should be pursued with as much cooperation as possible from industry, but it should not be left to industry alone.

Protecting the Pharmaceuticals System: Excipients and Unregulated Diet Supplements

Following the 1982 poisoning incidents in which cyanide-laced Tylenol was placed in retail stores in the Chicago area, tamper-evident packaging became required for all over-the-counter medications. As a result, deliberate contamination of distributed nonprescription drugs has become far more difficult. Similarly, to successfully tamper with FDA-approved drugs before distribution, a terrorist would have to defeat the relatively rigorous controls established for routine drug production.

A greater risk, however, is contamination of the vast array of vitamins, health supplements, and "natural" remedies, which do not need FDA approval. The chance prevention, in 1998, of a mailing in which sodium cyanide was deliberately sent packaged as a free sample of a nutritional supplement (Canto, 1998) underscores the vulnerability of these products.

The manufacturers of pharmaceutical products are required by law (21CFR211) to establish and maintain controls over personnel, facilities, and materials (including all raw materials, intermediates, and final products). Such controls are also mandated for producers of active agents subsequently compounded into medications and, to a limited degree, for the producers of excipients.[10] Controls include physical management of material movement and use, especially inventory reconciliation; worker training and qualification for assigned tasks; and strict monitoring of water and air systems within production environments.

The ability of such controls to protect products against deliberate contamination before distribution is clearly dependent on the nature and concentration of the contaminant. Acute poisoning of consumers requires materials and doses different from cumulative or delayed-effect toxins or from radioisotopic substitutions, all of which present more insidious threats. Excipients in particular often

[10]Excipients are the salts, sugars, polymers, and binding agents that are compounded with the active ingredients to produce the final tablet, capsule, or solution.

account for a relatively high fraction of the final dosage form, thus allowing for lethal contamination at low concentrations. Moreover, they are widely used: Several are common to more than a hundred approved drug formulations. While there are multiple suppliers of excipients, contamination of one source could have a widespread impact, including an erosion of public confidence in the safety of medicines generally.

Although assay methods are not likely to be published for proprietary active agents (published materials do exist for testing of generic drugs), they often make up a small weight-fraction of the final dose and are less susceptible to deliberate contamination.

Recommendation 4.13: The FDA, working with the pharmaceutical industry, should lead a review of the security and inventory controls used by manufacturers of drug excipients and health supplements to determine if current methods and standards need to be improved.

Recommendation 4.14: The FDA should facilitate efforts to develop improved technologies for detecting deliberately introduced contaminants in food or drug products. It should direct special attention to technologies capable of simultaneously assessing a range of potentially harmful components.

Protecting Water Supplies

Within the nation's infrastructure the U.S. water supply is probably not the most likely terrorist target for producing mass casualties, because the combination of high dilution and water treatment provides protection against many threats. However, forced entry of a highly toxic agent into the system after water treatment could have serious consequences. Chapter 8 discusses the structure of the nation's water systems and provides recommendations for reducing system vulnerability. Here the focus is mainly on issues related to rendering potential contaminants harmless.

Many agents can cause death or serious illness when introduced into a water system (WHO, 1970; Burrows and Renner, 1999; Clark and Deininger, 2000), the most dangerous being bacteria and toxins.[11] Among the most harmful bacteria are *Bacillus anthracis*, *Shigella dysenteriae*, *Vibrio cholerae*, and *Yersinia pestis* (NRC, 2000). The best line of defense against them is to maintain a chlorine residual in the water distribution system. Of several toxins, the botulinum toxin is the most lethal (NRC, 2000), but doses required for adverse health effects are not very well defined. Data are available only for mice and primate

[11]Chapter 3 provides more details on biological agents, which are mentioned here because of the similarities in surveillance, detection, and prevention of both biological and chemical threats.

models and are usually expressed as an LD_{50} (lethal dose for 50 percent of the exposed subjects). The appropriateness of the LD_{50} is uncertain; some scientists believe that an LD_{10}, or even lower, might be more prudent.

Besides bacteria and toxins, there are a number of other potential contaminants of the water supply. Chemical-warfare agents are normally deployed as aerosols, so contamination of water can be a secondary effect (NRC, 1995). Because many of these agents hydrolyze in water, especially under alkaline conditions, they are eventually rendered harmless. However, some insecticides that are choline esterase inhibitors, similar in action to nerve agents, do persist in water (Larsson, 1958).

Natural outbreaks have provided us with experience in dealing with some biological contaminants. For example, one natural outbreak of the protozoan *Cryptosporidium parvum* contaminated the Milwaukee water supply system in 1993, with serious consequences: Over 50 people died and over 400,000 became ill (Hoxie, 1997). Although this protozoan causes serious health effects in people who are very young or old, or immunocompromised, it does not pose a lethal threat to most healthy people.

Most of the agents that can be introduced into a water supply system will react with a disinfectant residual.[12] (While chlorine is the most commonly used disinfectant in the United States, other chemicals such as ozone—each with its own advantages and disadvantages—can also be used.) Even if reaction and deactivation of a contaminant are incomplete and take time, maintaining a residual of disinfectant in the distribution system is the most important measure for its protection. The residual needs to be monitored at representative locations in real time. The technology is available for this monitoring, but questions remain about the residual itself. Would the level of chlorine necessary to react destructively with most biological agents make the water undrinkable? If so, could the chlorine be removed easily and inexpensively as the water enters homes?

Recommendation 4.15: The EPA should direct additional research to determine the persistence of pathogens, chemical contaminants, and other toxic materials in public water supplies in the presence of residual chlorine.

Recommendation 4.16: NIST and industry associations should examine the possibility of sensor systems that would protect the public water supply. They should also address the question of whether protection is ultimately best carried out at the water-treatment facility or at the tap (using filters or other means of purification).

In addition to the potential threat of contamination, water-supply systems are vulnerable to physical damage that could easily lead to disruption of service.

[12]Some contaminants, such as arsenic, would not be destroyed by disinfectant residual.

While not necessarily catastrophic, this disruption could have serious effects on the economy and on public confidence. The systems need to be highly redundant so that failure of one or more components does not lead to a major disruption. Communities should develop plans for backup, recovery, and repair of intentionally damaged water systems and for provision of emergency water supplies.

Recommendation 4.17: The EPA should convene panels of experts to assess vulnerabilities and recommend corrective actions for the various components of water supply systems. These assessments should be done with the maximum possible cooperation from industry.

RESPONDING TO ATTACKS

Supporting First Responders

The country already has large numbers of personnel who are equipped and trained (to varying extents) to provide the first response to a chemical attack. Examples include HAZMAT (hazardous materials) teams, fire and police departments, civil support teams, and military personnel (see Box 4.2). All these groups would bring critical skills in responding to an incident; the challenge is to maximize their effectiveness and provide them with the support they need to do their jobs safely. Areas in which current capabilities could be improved—protective equipment, training, coordination among various jurisdictions and agencies, predictive models, and access to reliable expertise—are briefly discussed below.

A key requirement is for equipment and procedures that protect critical personnel from being contaminated and becoming casualties themselves. Appropriate systems will undoubtedly require either compromises or multiple sets of equipment, as these systems must be designed to protect first responders not only from a wide variety of chemicals but also from a number of biological and radiological threats.

Another key requirement is to train these groups specifically to deal with chemical terrorism. Effective training includes specialized exercises by individual groups and large-scale exercises that incorporate, for example, the medical system and the National Guard. Also critical will be the development of communications networks and command protocols that establish the chains of command before an attack and allow local, state, and national groups to work together effectively. At present, the lack of strategies for coordination among the various response teams is a major problem, and the response to a chemical attack, if one were carried out today, would be inefficient and, possibly, confused.

Coordination among various jurisdictions and agencies is a serious issue. Differences in mission, style, and command structure result in conflicts among local law enforcement, health care professionals, the FBI, FEMA, and the military whenever these groups operate in the same environment. (See also Chapters

BOX 4.2
Groups That Can Help Respond to a Terrorist Attack Using a Chemical Agent

Many (if not most) cities and many industries have HAZMAT teams trained and equipped to deal with accidental spills and releases of toxic industrial chemicals. They have not been trained or equipped to deal with terrorist incidents, but chemical weapons of the types that would most plausibly be used by terrorists are not fundamentally different from the chemicals that these teams already address.

Among the first responders to chemical terrorism, fire departments can be a major resource. All fire departments have personnel who are trained and equipped to work with respirators and protective gear (as hazardous vapors are always a part of fires), and they are of course trained to deal with emergencies. The police are not routinely equipped to respond to chemical incidents per se (although they play an essential role in maintaining order). Equipping police units with protective gear is, however, a practical way of expanding the number of individuals who can actively participate in the response to a chemical incident.

Weapons of Mass Destruction Civil Support Teams from the Department of Defense are deployed around the country.[1] These groups have a limited but possibly useful capability to coordinate communications among responders and to carry out chemical and biological analyses.

Another substantial capability in place is the military, including active-duty, reserve, and National Guard personnel. The military has trained and equipped for chemical warfare during the past 50 years. It maintains large supplies of relevant equipment—protective suits, prophylactics, and medical countermeasures against nerve and blister agents. These assets are geared, however, to wars on foreign battlefields. An important issue is to understand how to use this capability in time of need inside the continental United States.

[1]As of April 2002, 27 teams had been deployed, with 5 more authorized and in the planning stage.

12 and 13.) In some chemical attacks, still other agencies would be involved (e.g., the USDA for attacks on the food supply and the EPA where decontamination is required). The most efficient mechanism for working through the usual conflicts among these organizations, and for rendering workable the laws and regulations under which they operate, is to carry out field exercises—simulations of real attacks—with all those entities that would be likely to participate. Differences should be settled before an event rather than after it.

Exercises and protocols can only be taken so far, however; it is impossible to envision and plan for all possible scenarios. To minimize the consequences of any attack, it is thus essential that the person (or persons) in charge of the response be able to readily access as much information as possible and to commu-

nicate resulting decisions to the right parties as rapidly as possible. If a tank car filled with chlorine has been blown open in a switching yard, what areas of the city are at risk? If there has been a sarin attack on an office building, how should the nerve agent best be kept localized? There are many factors to consider in determining the answers to these questions; explicit, one-size-fits-all solutions will not always be appropriate. The incident commander must have the ability to adapt in real time.

One important need is for software that will allow the commander to predict the movement of chemical agents—through the city's atmosphere, in buildings, or in tunnel systems. Work on this type of tool, especially in the area of atmospheric modeling, is proceeding, but there are at present several competing models whose results are often in disagreement. Further R&D is clearly needed to resolve these anomalies or develop more dependable alternatives.

Another important source of information for incident commanders is fast access to reliable expertise (sometimes called "reachback"). Chemistry is technically complex, and first responders and their leaders cannot be expected to know the details for all possible chemical attacks. They must be able to consult, in real time, with experts familiar with the characteristics of the weapons. A panel (or panels) of such experts should be formed immediately to improve the likelihood that they will be available when needed and to ensure that appropriate channels for effective communication are established. (Industrial risk and industrial safety groups might be a good source of experts.) The Marine Corps has worked with such a reachback group—the Chemical/Biological Incident Response Force (CBIRF)—and this experience might provide a starting point for the design of groups to serve incident commanders and first responders. Even without a terrorist event, these groups could be of use—there are unfortunately enough chemical spills and accidents nationally for responders to benefit from the group's input (and give it real opportunities to practice).

Recommendation 4.18: FEMA, with technical support from the Defense Threat Reduction Agency (DTRA), should be tasked with developing a communications structure for ensuring that response teams have quick access to reliable expertise when managing chemical incidents. In addition, these agencies should establish and test a prototype panel of experts.

Preparing for Treatment of Victims: Improving the Capabilities of the Medical System and the Treatment Options

The United States has a very competent medical system, but it is not currently prepared to deal with chemical attacks (especially with nerve or blister agents). Two areas in particular are in need of improvement: (1) the inability of the medical system to handle a large number of casualties from a chemical attack and (2) the lack of experience on the part of the nation's health professionals in

dealing with casualties of this type, together with the lack of optimized treatment protocols and the possibility that there are no appropriate drugs.

To enable the medical system to respond to a large number of chemical casualties, several issues must be addressed. First, casualties still contaminated with chemical agents are likely to present at hospitals. To avoid contaminating medical personnel and facilities as well, there must be accepted protocols for decontaminating and handling these casualties. Second, in an attack on a population center, experience suggests that for every legitimate patient presenting at the hospital, between 100 and 1,000 "worried well" will also arrive, looking for reassurance. Hospitals have no capability to manage crowds or to triage large numbers of anxious people. Third, the U.S. hospital system—in the interests of efficiency—has slimmed down to the point that there is essentially no capacity for surges in demand for medical care. Thus there are not enough beds, medical supplies, and respirators to deal with any substantial number of terrorist-event casualties.

Recognizing that the medical system is ill prepared to handle a massive influx of chemical casualties is not the same as knowing how to prepare for such an event. A great deal of work can be done with computer modeling and tabletop exercises, but only through field exercises will the real weaknesses in the system be discovered. Carrying out exercises of this type is expensive, however, and can raise the public's level of anxiety. Deciding on the best course to pursue in preparing for the possibility of mass casualties is an issue of policy, but resolving the technical details requires a balance between paper or computer exercises and checks of reality.

Recommendation 4.19: With the collaboration of hospitals and medical associations, FEMA should lead a careful systems analysis of needs—covering doctors, facilities, supplies, and equipment—for responding to plausible large-scale chemical attacks. This analysis should be used as the basis for planning the acquisition, storage, and distribution of resources in preparation for such attacks.

Recommendation 4.20: The federal government should work with the private sector to develop plans to provide surge capacity and to conduct exercises with the full participation of the medical system.

Recommendation 4.21: The federal government should provide leadership in developing strategies for training medical personnel in appropriate responses to chemical injuries and for stockpiling associated medical supplies.

Treatments for chemical casualties have come primarily from military medicine and are intended to preserve soldier function. Whether these protocols are optimal for civilian casualties has not been resolved or even carefully considered. The issue of long-term damage to the central nervous system is particularly

important. The carcinogenicity of blister agents is a second concern, and each of the other potential agents raises its own set of concerns. Understanding the pathogenesis of these chemical weapons is an important step in developing rational protocols for treatment of the casualties they produce.

Research in this area is complicated by the fact that it is not possible to work with human patients, and the most relevant tests are carried out with higher primates (which are both expensive and widely protected). Developing cellular models, or improved whole-animal models using rodents, will be an important part of this program.

Recommendation 4.22: Under the guidance of the NIH, there should be a program to develop improved treatments for injuries that result from exposures to chemical agents.

This program should have both an applied and a fundamental aspect: It should optimize existing protocols, using the most plausible threats, and it should increase our understanding of the general mechanisms of injury on exposure to toxic chemicals. The program should address treatment for both acute and chronic injury, and it should consider countermeasures and protective measures that embrace the full spectrum of threats. Because of the long time required to develop countermeasures, we should start now on important classes of weapons, even if they are not yet known to be ready for deployment.

The system used for developing drugs in the United States will require modification in order to support the development of treatments for chemical attacks. Several problems will have to be addressed:

- The markets are too small (unless dual-use applications can be developed) to make a serious effort by the pharmaceutical industry worthwhile.
- The system on which FDA clearance is based—the testing of new drugs in humans in carefully controlled trials—cannot be used, as these trials have no benefit for the subjects that would be involved.
- The best surrogates for humans in many studies—higher primates—are very carefully protected.
- Many of the chemical agents involved—especially nerve and blister agents—are difficult (or illegal) to use in universities.

The problems of carrying out this kind of research, and of clearing new drugs for use under appropriate circumstances, may require exceptions from current laws and regulations, along with indemnification of suppliers of materials in case of adverse reactions in humans. The FDA is well aware of these problems with regard to biological attacks, and it is trying to develop a suitable system for drugs that would be used in treating the resulting casualties; similar strategies will be applicable for drugs relevant to chemical attacks.

A STRATEGY TO DEVELOP ECONOMICALLY VIABLE COUNTERTERRORISM TECHNOLOGIES

Technologically speaking, the United States is enormously inventive, but without commercialization, the deployment of technological advances is not very likely. To develop the products and systems needed to protect vital systems and respond to attacks, probably the most successful strategy will be to focus explicitly on technologies that have broader commercial applications as well as value for counterterrorism efforts. (This topic is discussed further in Chapter 13.) For example, some sensor technologies can be developed for more general or larger markets (biomedicine, environmental monitoring, food safety) while also being useful for emergency response and incident management.

A similar trend, driven by the dual goals of environmental quality and economic efficiency, is already moving the chemical industry in new directions. Sustainable (green) chemistry—the design, manufacture, and use of efficient, effective, safe, and environmentally benign chemical processes and products—is now receiving widespread industry attention, though the need for considerable improvement remains. Government, academia, and industry should strive to identify research directions that could lead to safer, intrinsically secure, economically viable chemical processes and procedures that are valuable for our long-term sustainability. Such efforts also have a benefit for our nation's counterterrorism efforts as well: If we make fewer toxic products, use milder manufacturing conditions, and produce less toxic waste, we reduce the opportunities for terrorists.

REFERENCES

Accomazzo, M.A., G. Ganzi, and R. Kaiser. 1988. "Deionized (DI) Water Filtration Technology," *Handbook of Contamination Control in Microelectronics*, D.L. Tolliver, ed. Noyes Publications, N.J., pp. 210-346.

Burrows, W.D., and S.E. Renner. 1999. "Biological Warfare Agents as Threats to Potable Water," *Environmental Health Perspectives,* Vol. 107, No. 12, pp. 975-984.

Canto, M. 1998. "Woman Arrested in Cyanide Scare," *Seattle Times,* August 24.

Clark, R.M., and R.A. Deininger. 2000. "Protecting the Nation's Critical Infrastructure: The Vulnerability of U.S. Water Supply Systems," *Journal of Contingencies and Crisis Management,* Vol. 8, No. 2, pp. 73-80.

Dandrieux, A., G. Dusserre, J. Ollivier, and H. Fourne. 2001. "Effectiveness of Water Curtains to Protect Firemen in Case of an Accidental Release of Ammonia: Comparison of the Effectiveness of Two Different Rates of Ammonia," *Journal of Loss Prevention in the Process Industries,* Vol. 5, pp. 349-355.

Ensor, D.S., and R.P. Donovan. 1988. "Aerosol Filtration Technology," *Handbook of Contamination Control in Microelectronics*, D.L. Tolliver, ed. Noyes Publications, N.J., pp. 1-67.

Food and Drug Administration (FDA). 1998. *Managing Food Safety: A HACCP Principles Guide for Operators of Food Establishments at the Retail Level (Draft).* Available online at <http://www.cfsan.fda.gov/~dms/hret-toc.html>, accessed March 8, 2002.

FDA. 2001. Seafood HACCP. Available online at <http://www.cfsan.fda.gov/~comm/haccpsea.html>, accessed March 8, 2002.

FDA. 2002a. Juice HACCP, available online at <http://www.cfsan.fda.gov/~comm/haccpjui.html>, accessed March 8, 2002.

FDA. 2002b. Dairy Grade A Voluntary HACCP Pilot. Available online at <http://www.cfsan.fda.gov/~comm/haccpdai>, accessed March 8, 2002.

Ho, W.S., and K.K. Sirkar, eds. 1992. *Membrane Handbook,* Van Nostrand Reinhold, New York.

Hoxie N.J., J.P. Davis, J.M. Vergeront, R.D. Nashold, and K.A. Blair. 1997. "Cryptosporidiosis-Associated Mortality Following a Massive Waterborne Outbreak in Milwaukee, Wisconsin," *American Journal of Public Health,* Vol. 87, pp. 2032–2035.

Kawana, N., S. Ishimatsu, and K. Kanda. 2001. *Military Medicine*, Vol. 166, Supp. 2, pp. 23-26.

Larsson, L. 1958. "The Alkaline Hydrolysis of Two Sarin Analogues and of Tabun," *Acta Chim. Scand.*, Vol. 12, p. 783.

Majumdar, G., and K.K. Sirkar. 1988. "A New Liquid Membrane Technique for Gas Separation," *AIChE Journal,* Vol. 34, No. 7, pp. 1135-1145.

National Materials Advisory Board (NMAB), National Research Council. 2002. *Summary. Assessment of Technologies Deployed to Improve Aviation Security: Second Report, Progress Toward Objectives,* National Academy Press, Washington, D.C.

National Research Council (NRC). 1995. *Guidelines for Chemical Warfare Agents in Military Field Drinking Water,* National Academy Press, Washington, D.C.

NRC. 1998. *Containing the Threat from Illegal Bombings,* National Academy Press, Washington, D.C.

NRC. 1999. *Strategies to Protect the Health of Deployed U.S. Forces: Force Protection and Decontamination,* National Academy Press, Washington, D.C.

NRC. 2000. *Strategies to Protect the Health of Deployed U.S. Forces: Detecting, Characterizing, and Documenting Exposures,* National Academy Press, Washington D.C.

Petersen, R.L., and R. Diener. 1990. "Vapour Barrier Assessment Programme for Delaying and Diluting Heavier-Than-Air HF Vapour Clouds in a Wind Tunnel Modeling Evaluation," *Journal of Loss Prevention in the Process Industries,* Vol. 3, pp. 187-196.

Prasad, R., and K.K. Sirkar. 1987. "Microporous Membrane Solvent Extraction," *Separation Science and Technology,* Vol. 22, Nos. 2-3, pp. 619-640.

Scientific American. 2001. "Better Killing Through Chemistry," December, pp. 20-21.

Way, J.D., R.D. Noble, T.M. Flynn, and E.D. Sloan. 1982. "Liquid Membrane Transport: A Survey," *J. Membrane Science,* Vol. 12, No. 3, pp. 239-259.

World Health Organization. 1970. "Health Aspects of Chemical and Biological Weapons," *Annex 5, Sabotage of Water Supplies*, pp. 113-120.

RECOMMENDED READING ON FOOD SAFETY

Hartman, N.F. 1997. "Reducing Food Poisoning Deaths," *Engineering & Technology for a Sustainable World,* Vol. 4, pp. 11-12.

Holcomb, D.L., M.A. Smith, G.O. Ware, Y.-C. Hung, R.E. Brackett, and M.P. Doyle. 1999. "Comparison of Six Dose-Response Models for Use with Food-borne Pathogens," *Risk Analysis,* Vol. 19, pp. 1091-1100.

Institute of Medicine. 2001. *Food Safety Policy, Science, and Risk Assessment: Strengthening the Connection, Workshop Proceedings,* National Academy Press, Washington, D.C.

Liu. S., J.-C. Huang, and G.L. Brown. 1998. "Information and Risk Perception: A Dynamic Adjustment Process," *Risk Analysis,* Vol. 18, pp. 689-699.

Loaharanu, P. 2001. "Rising Calls for Food Safety: Radiation Technology Becomes a Timely Answer," *IAEA Bulletin,* Vol. 43, pp. 37-42.

National Research Council. 1998. *Ensuring Safe Food: From Production to Consumption,* National Academy Press, Washington, D.C.

Otero, R., and J.O. Grimalt. 1994. "Organochlorine Compounds in Foodstuffs Produced near a Chlorinated Organic Solvent Factory," *Toxicological and Environmental Chemistry,* Vol. 46, pp. 61-72.

Strongin, Robin J. 2002. "How Vulnerable Is the Nation's Food Supply? Linking Food Safety and Food Security," *National Health Policy Forum,* NHPF Issue Brief No. 773. George Washington University, Washington, D.C., May 17.

Teixiera, A. 1994. "Connectivity Critically Important in Engineering a Safe Food System," *Resource,* Vol. 1, pp. 12-14.

5

Information Technology

INTRODUCTION

Information technology (IT) is essential to virtually all of the nation's critical infrastructures, which makes any of them vulnerable to a terrorist attack on the computer or telecommunications networks of those infrastructures. IT plays a critical role in managing and operating nuclear-power plants, dams, the electric-power grid, the air-traffic-control system, and financial institutions. Large and small companies rely on computers to manage payroll, track inventory and sales, and perform research and development. Every stage of the distribution of food and energy, from producer to retail consumer, relies on computers and networks. A more recent trend is the embedding of computing capability in all kinds of devices and environments, as well as the networking of embedded systems into larger systems.[1] These realities make the computer and communications systems of the nation a critical infrastructure in and of themselves, as well as major components of other kinds of critical infrastructure, such as energy or transportation systems.

The IT infrastructure can be conceptualized as four major elements: the Internet, the telecommunications infrastructure, embedded/real-time computing (e.g., avionics systems for aircraft control, SCADA systems controlling electrical energy distribution), and dedicated computing devices (e.g., desktop computers). Each of these plays a different role in national life and each has different vulnerabilities.

[1]See CSTB (2001a). Note that most CSTB reports contain many references to relevant literature and additional citations.

IT can also play a major role in the prevention, detection, and mitigation of terrorist attacks.[2] By enabling wider awareness of critical information in the intelligence community,[3] IT may facilitate the identification of important patterns of behavior. Advances in information fusion, which is the aggregation of data from multiple sources for the purpose of discovering some insight, may be able to help in uncovering terrorists or their plans in time to prevent attacks. In addition to prevention and detection, IT may also enable rapid and accurate identification of the nature of an attack and aid in responding more quickly.

THREATS ASSOCIATED WITH IT INFRASTRUCTURE

When the IT infrastructure is attacked, the target can be the IT itself. Alternatively, the true target of the terrorist may be another of our society's infrastructures, and the terrorist can either launch or exacerbate the attack by exploiting the IT infrastructure, or use it to interfere with attempts to achieve a timely and effective response. Thus, IT is both a target and a weapon that can be deployed against other targets.

A terrorist attack that involves the IT infrastructure can operate in one of three different modes. First, the attack can come in "through the wires" alone. Second, it can include the physical destruction of some IT element, such as a critical data center or communications link. Third, the attack can rely on the compromising of a trusted insider who, for instance, provides passwords that permit outsiders to gain entry.[4] All of these modes are possible and, because of the highly public nature of our IT infrastructure and of our society in general, impossible to fully secure. Nor are they mutually exclusive—and in practice they can be combined to produce even more destructive effects.

Most of the nation's civil communications and data network infrastructure offer soft IT targets, but they tend to be localized either geographically or in mode of communication, and if no physical damage is done tend to be recoverable in a relatively short time. One can imagine the use of IT as the weapon in a series of relatively local attacks that are repeated against different targets—banks, hospitals, or local government services—so often that public confidence is shaken and significant economic disruption results. This report is focused on catastrophic terrorism, and the committee's analysis is aimed at identifying those threats in particular and proposing S&T strategies for combating them. Of course, serious efforts are needed to employ security technologies that research might generate to harden all elements of the IT infrastructure to reduce the damage potential for such repeated attacks.

---

[2]CSTB (1996, 1999a).

[3]The intelligence community includes the CIA, FBI, NSA, and a variety of other agencies in the DOD and other departments.

[4]See CSTB (1999b).

IT Attack as an Amplifier of a Physical Attack

Given IT's critical role in many other elements of the national infrastructure and in responding to a crisis, the targeting of IT as part of a multipronged attack scenario could have catastrophic consequences. Compromised IT can have several disastrous effects: expansion of terrorists' opportunities to widen the damage of a physical attack (for example, by providing false information that drives people toward rather than away from the point of attack); diminishment of timely responses to the attack (by interfering with communications systems of first responders); and heightened terror in the population through misinformation (by providing false information about the nature of the threat). The techniques to compromise key IT systems—e.g., launching distributed denial-of-service (DDOS) attacks against Web sites and servers of key government agencies at the federal, state, and local levels, using DDOS to disrupt agencies' telephone services and the emergency-response 911 system, or sending e-mails containing false information with forged return addresses so they appear to be from trusted sources—are fairly straightforward and widely known.

Other Possibilities for Attack Using IT

When an element of the IT infrastructure is directly targeted, the goal is to destroy a sufficient amount of IT-based capability to have a significant impact. For example, one might imagine attacks on the computers and data storage devices associated with important facilities. Irrecoverable loss of critical operating data and essential records on a large scale would likely result in catastrophic and irreversible damage to U.S. society. While no law of physics prevents the simultaneous destruction of all data backups and backup facilities in all locations, such an attack would be highly complex and difficult to execute, and is thus implausible.

The infrastructure of the Internet is another possible target, and given its prominence, may appeal to terrorists as an attractive target. The Internet could be seriously degraded for a relatively short period of time by a denial-of-service attack, but this is unlikely to be long lasting. The Internet itself is a densely connected network of networks,[5] which means that a large number of important nodes would have to be destroyed simultaneously to bring it down for an extended period of time. Destruction of some key Internet nodes would result in slowed traffic across the Internet, but the ease with which Internet communications can be rerouted would minimize the long-term damage.[6] (In this regard, the

[5]See CSTB (2001b). Note, however, that the amount of redundancy is primarily limited by economic factors.

[6]This comment largely applies to U.S. use of the Internet. It is entirely possible that other nations—whose traffic is often physically routed through the United States through one or two locations—would fare much worse in this scenario.

fact that substantial data-networking services survived the September 11 disaster despite the destruction of large amounts of equipment concentrated in the World Trade Center complex reflected redundancies in the infrastructure (and a measure of good fortune as well).)

Higher leverage could be obtained with a "through-the-wires" attack that would require the physical replacement of components in Internet relay points on a large scale, though such attacks would be much harder to plan and execute. Another attack that would provide greater leverage is on the Domain Name System (DNS), which provides translation for the Internet of domain names (e.g., example.com) to specific IP addresses (which denote specific Internet nodes). There are a relatively small number of "root name servers" that provide these translation services, and while the DNS is configured to provide redundancy in case of accidental failure, it has some vulnerability to an intentional physical attack that might target all name servers simultaneously. Though Internet operations would not halt instantly, an increasing number of sites would, over a period of time measured in hours to days, become inaccessible without root name servers to provide authoritative translation information. On the other hand, recovery from such an attack would be unlikely to take more than several days, since the servers themselves are general-purpose computers that are in common use.

A second point to consider is that most companies today do not rely on the Internet to carry out their core business functions. Even if a long-term disruption to the Internet were a major disruption to an e-commerce company such as Amazon.com, most other companies could resort to using phones and faxes again to replace the Internet for many important functions. (For example, the Department of the Interior was largely off the Internet since the beginning of December 2001,[7] and it continues to operate more or less as usual.) Because the Internet is not (yet) central to most of American society, the impact of even severe damage to the Internet is less than what might be possible through other modes of attack.

The telecommunications infrastructure of the public switched network is likely to be less robust. Although the long-haul telecommunications infrastructure is capable of dealing with single-point failures in such centers (and perhaps even double-point failures), the physical redundancy in that infrastructure is not infinite, and taking out a relatively small number of major switching centers for long-distance telecommunications could result in a fracturing of the United States into disconnected regions.[8] An additional vulnerability in this telecommunica-

[7]Jennifer Disabatino. 2001. "Court Order Shuts Down Dept. of Interior Web Sites," *COMPUTERWORLD*, December 17. Available online at <http://www.computerworld.com/storyba/0,4125,NAV47_STO66665,00.html>.

[8]An exacerbating factor is that many organizations rely on leased lines to provide high(er)-assurance connectivity. However, these lines are typically leased from providers of telecommunications infrastructure, and hence suffer from many of the same kinds of vulnerabilities as ordinary lines.

tions infrastructure is the local loop connecting central switching offices to end users—full recovery from the destruction of a central office entails the tedious rewiring of tens or hundreds of thousands of individual connections. Destruction of central offices on a large scale is difficult, simply because even an individual city has many of them, but destruction of a few central offices associated with key facilities or agencies (e.g., those of emergency response agencies, or of the financial district) would certainly have a significant immediate, though localized, impact.

The IT systems and networks supporting the nation's financial system are undeniably critical. However, banking transactions occur through separate networks such as SWIFT and CHIPS; attacks on these networks would require significantly more effort and risk to plan and implement than comparable assaults on the open Internet. For example, successful attacks on SWIFT and CHIPS would likely necessitate significant insider access.[9]

Embedded/real-time computing in specific systems could be attacked. One example is the possibility of corruption over time, much as a Y2K bug was built into many embedded real-time systems. Of particular concern could be avionics in airplanes, collision avoidance systems in automobiles, and other transportation systems. Such attacks would require a significant insider presence in technically responsible positions in key sectors of the economy over long periods of time.

A second type of attack on embedded computing is illustrated by the notion of an attack on the systems controlling elements of the nation's critical infrastructure, e.g., the electric-power grid, the air-traffic-control system, the financial network, and water purification and delivery. An attack on these systems could trigger an event and perhaps stimulate an inappropriate response to the event that drives the system into a catastrophic state. The discussion below, presented as an example, focuses on the electric-power grid[10]—in particular, on the supervisory control and data acquisition (SCADA) systems that underlie IT's control of the electric-power grid—but similar considerations apply to other parts of the nation's infrastructure.

---

[9]The fact that these networks are separate and physically distinct from those of the Internet and the public switched telecommunications network reduces the risk of penetration considerably. In addition, security consciousness is much higher in financial networks than on the Internet. On the other hand, the fact that these networks are much smaller than the Internet suggests that there is less redundancy in them and that the computing platforms are likely to be less diverse than the platforms on the Internet, a factor that tends to reduce their security characteristics as compared to those of the Internet.

[10]Note that the electric power grid is one of the few, if not the only, truly "national" infrastructures in which it is theoretically possible that a failure in a region could cascade to catastrophic proportions before it could be dealt with.

Box 5.1 describes some of the security issues associated with SCADA systems. Attacks on SCADA systems could obviously result in disruption of the network ("soft" damage), but because SCADA is used to control physical elements, such attacks could also result in irreversible physical damage. In those cases where backups for the damaged components were not readily available (and might have to be remanufactured from scratch), such damage could have long-lasting impact.

An electronic attack on a portion of the electric-power grid could result in significant damage, easily comparable to that associated with a local blackout. The real leverage of such an attack would likely be in amplifying the damage and costs associated with a physical attack on some other element of the critical infrastructure.

Another disaster scenario that could rise to the level of catastrophic damage would be an attack on a local or regional power system that cascades to shut down electrical power, possibly with physical damage that could take weeks to repair, over a much wider area. On the other hand, it is unclear whether such an attack could actually be mounted, and a detailed study both of SCADA systems and the electric-power system is probably required in order to assess this possibility. The committee notes, however, that because of the inordinate complexity of the nation's electric-power grid, the effects on the overall grid of a major disruptive event in one part of the system are difficult to predict with any confidence (both for grid operators and terrorists). Thus, any nonlocalized impact on the power grid would be as much a matter of chance as a foreseeable consequence. (See Chapter 6 for a further discussion on electric power vulnerabilities.)

In many of the same ways as embedded computing could be attacked, dedicated computers could also be corrupted in hard-to-detect ways. One possible channel arises from the extensive use of foreign IT talent among software vendors. Once working on the inside, perhaps after a period of years in which they act to gain responsibility and trust, it could happen that these individuals would be able to introduce additional but unauthorized functionality into systems that are widely used. Under such circumstances, their target might not be the general-purpose computer used in the majority of offices around the country, but rather the installation of hidden rogue code in particular sensitive offices. Another channel arises from the connection of computers through the Internet; such connections provide a potential route through which terrorists might attack computer systems that do provide important functionality for many sectors of the economy. (It is likely that Internet-connected computer systems that provide critical functionality to companies and organizations are better protected through firewalls and other security measures than the average system on the Internet, but as press reports in recent years make clear, such measures do not guarantee that outsiders cannot penetrate them.)

BOX 5.1
Security Vulnerabilities and Problems of SCADA Systems

Today's supervisory control and data acquisition (SCADA) systems have been designed with little or no attention to security. For example, data in SCADA systems are often sent "in the clear." Protocols for accepting commands are open, with no authentication required. Control channels are often wireless or leased lines that pass through commercial telecommunications facilities. For example, unencrypted radio-frequency command pathways to SCADA systems are common and, for economic reasons, the Internet itself is increasingly used as a primary command pathway. Thus, there is minimal protection against the forgery of control messages or of data and status messages. Such control paths present obvious vulnerabilities.

In addition, today's SCADA systems are built from commercial off-the-shelf components and are based on operating systems that are known to be insecure. Deregulation has meant placing a premium on the efficient use of existing capacity, and hence interconnections to shift supply from one location to another have increased. Problems of such distributed dynamic control, in combination with the complex, highly interactive nature of the system being controlled, have become major issues in operating the power grid reliably.

A final problem arises because of the real-time nature of SCADA systems, in which timing may be critical to performance and optimal efficiency (timing is important because interrupts and other operations can demand millisecond accuracy): Security add-ons in such an environment can complicate timing estimates and can cause severe degradation to SCADA performance.

Compounding the difficulty of SCADA systems' tasks is the fact that information about their vulnerability is so readily available. Such information was first brought into general view in 1998-1999, when numerous details on potential Y2K problems were put up on the World Wide Web. Additional information of greater detail—dealing with potential attacks that were directly or indirectly connected to the President's Commission on Critical Infrastructure Protection—was subsequently posted on Web pages as well. Product data and educational videotapes from engineering associations can be used to familiarize potential attackers with the basics of the grid and with specific elements. Information obtained through semiautomated reconnaissance to probe and scan the networks of a variety of power suppliers could provide terrorists with detailed information about the internals of the SCADA network, down to the level of specific makes and models of equipment used and version releases of corresponding software. And more inside information could be obtained from sympathetic engineers and operators.

Disproportionate Impacts

Some disaster scenarios result in significant loss or damage that is all out of proportion to the actual functionality or capability destroyed. In particular, localized damage that results in massive loss of confidence in some critical part of the infrastructure could have such a disproportionate impact. For example, if terror-

ists were able to make a credible claim that the control software of a popular fly-by-wire airliner was corrupted and could be induced to cause crashes on demand, perhaps demonstrating it once, public confidence in the airline industry might well be undermined. A more extreme scenario might be that the airlines themselves might ground airplanes until they could be inspected and the software validated.

To the extent that critical industries or sectors rely on any element of the IT infrastructure, such disproportionate-impact disaster scenarios are a possibility.

Possibility, Likelihood, and Impact

The scenarios above are necessarily speculative. But it is possible to make some judgments that relate to their likelihood:

- Attacks that require insider access are harder to mount and thus less likely than attacks that do not. Insiders must be placed or recruited, and insiders are not necessarily entirely trustworthy from the standpoint of the attacker. Individuals with specialized expertise chosen to be placed as infiltrators may not survive the screening process, and because there are a limited number of such individuals, it can be difficult to insert an infiltrator into a target organization. In addition, compared to approaches not relying on insiders, insiders may leave behind more tracks that can call attention to their activities. This judgment depends, of course, on the presumed diligence on the part of employers to ensure that their key IT personnel are trustworthy, but it is worth remembering that the most devastating espionage episodes in recent U.S. history have involved insiders (Aldrich Ames and Robert Hanssen).
- Attacks that require execution over long periods of time are harder to mount and thus less likely than attacks that do not. Planning often takes place over a long period of time, but the actual execution of a plan can be long as well as short. When a plan requires extended activity that if detected would be regarded as abnormal, it is more likely to be discovered and/or thwarted.
- Terrorist attacks can be sustained over time as well as occur in individual instances. If the effects of an attack sustained over time (perhaps over months or years) are cumulative, and if the attack goes undetected, the cumulative effects could reach very dangerous proportions. Because such an attack proceeds a little bit at a time, the resources needed to carry it out may well be less than in more concentrated attacks, thus making it more feasible.
- Plans that call for repeated attacks are less likely than plans that call for single attacks. For example, it is possible that repeated attacks on the Internet could render large parts of it inoperative for extended periods of time. Such an onslaught might be difficult to sustain, however, because it would be readily detected and efforts would be made to counter it. Instead, an adversary with the

wherewithal to conduct such repeated attacks would be more likely to make the initial strike and then use the recovery period not to stage and launch another strike against the Internet but to attack the physical infrastructure; this could leverage the inoperative Internet to cause additional damage and chaos.

- Terrorists, like other parties, have limited resources. Thus, they are likely to concentrate their efforts where the impact is largest for the smallest expenditure of resources. For example, terrorists who want to create immediate public fear and terror are more likely to use a physical attack (perhaps in conjunction with an attack using IT to amplify the resulting damage) than an attack that targets IT exclusively. The reason is that the latter is not likely to be as cinematic as other attacks. What would television broadcast? There would be no dead or injured people, no buildings on fire, no panic in the streets, and no emergency-response crews to the rescue. The image of a system administrator typing furiously is simply much less terrifying than images of buildings collapsing.
- The IT infrastructure (or some element of it) can be a weapon used in an attack on something else as well as the target of an attack. An attack using the IT infrastructure as a weapon has advantages and disadvantages from the point of view of a terrorist planner. It can be conducted at a distance in relative physical safety, in a relatively anonymous fashion, and in potentially undetectable ways. On the other hand, the impact of such an attack (by assumption, some other critical national asset) is indirect, harder to predict, and less certain.
- State sponsorship of terrorism poses threats of a different and higher order of magnitude, for a variety of reasons that include access to large amounts of financial backing and the ability to maintain an actively adversarial stance at a high level for extended periods of time. For example, state-sponsored terrorism might use the state's intelligence services to gain access to bribable or politically sympathetic individuals in key decision-making places, or to systematically corrupt production or distribution of hardware or software.
- Some of the scenarios above are potentially relevant to information warfare attacks against the United States, i.e., attacks launched or abetted by hostile nation-states and/or directed against U.S. military forces or assets. A hostile nation conducting an information attack on the United States is likely to conceal its identity to minimize the likelihood of retaliation, and hence may resort to sponsoring terrorists who can attack without leaving clear national signatures.

While these considerations make certain types of attack more or less likely, none of the scenarios described above can be categorically excluded. This fact argues in favor of a long-term commitment to a strategic R&D program that will contribute to the robustness of the telecommunications and data networks and of the platforms embedded in them. Such a program would involve both fundamental research into the scientific underpinnings of information and network security and the development of deployable technology that would contribute to informa-

tion and network security. Ultimately, the strengthening of the nation's IT infrastructure can improve our ability to prevent, detect, respond to, and recover from terrorist attacks on the nation.[11]

The shape of a strategic research and development agenda is described below. However, it should be noted that this agenda has broad applicability to efforts against terrorism, against information warfare, and against cybercrime. While the scope and complexity of issues with respect to each of these areas may well vary (e.g., an agenda focused on cybercrime may place more emphasis on forensics useful in prosecution), the committee believes that there is enough overlap in the research problems and approaches to make it unwise to articulate a separate R&D agenda for each area.

SHORT-TERM RECOMMENDATIONS

Developing a significantly less vulnerable information infrastructure is an important long-term goal for the country. This long-term goal must focus on the creation of new technologies and paradigms for enhancing security and reducing the impact of security breaches. In the meantime, the IT vulnerabilities of the first-responder network should receive priority attention. Efforts should focus on hardening first responders' communications capability, as well as those portions of their computing systems devoted to coordination and control of an emergency response.

Existing technology can be used to achieve many of the improvements needed in telecommunications and computing. Unfortunately, the expertise to achieve a more secure system often does not reside within the host organizations—this may be the case, for example, in local and state government. These realities lead, then, to three short-term recommendations:

Short-Term Recommendation 5.1: Develop a program to increase the security of emergency-response agencies' communications systems against attack, based on the use of existing technologies (perhaps slightly enhanced).

Some possible options include a separate emergency-response communications network that is deployed in the immediate aftermath of a disaster, and the use of the public network to support virtual private networks, with priority given to traffic from emergency responders. Given the fact that emergency-response agencies are largely state and local, no federal agency has the responsibility and authority to carry out this recommendation. Thus it would likely have to rely on incentives (probably financial) to persuade state and local responders to participate.

[11]See CSTB (1996, 1999a).

Short-Term Recommendation 5.2: Promote the use of best practices in information and network security throughout all relevant public agencies and private organizations.

Nearly all organizations, whether in government or the private sector, could do much better with respect to information and network security than they do today simply by exploiting what is already known about that subject, as discussed at length in *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*.[12] (For example, many technologies for securing IT systems, such as encryption, secure authentication, and the use of private networks for critical communications, are available but not widely deployed.) Those responsible for requiring and implementing such changes range from chief technical (or even executive) officers to system administrators. There is currently no clear locus of responsibility within government to undertake such "promotion" across the private sector—information and network security there is not subject to government regulation—nor even across government itself. The Office of Management and Budget has sought to promote information and network security in the past, but despite its actions the state of information and network security in government agencies remains highly inadequate. In the final analysis, even though the market has largely failed to provide sufficient incentives for the private sector to take adequate action with respect to information and network security, it is likely that market mechanisms will be more successful than regulation in improving the security of the nation's IT infrastructure, though they have yet to do so. The challenge for public policy is to ensure that such market mechanisms develop.

Short-Term Recommendation 5.3: Ensure that a mechanism exists for providing authoritative IT support to federal, state, and local agencies that have immediate responsibilities for responding to a terrorist attack.

One option is to place the mechanism administratively in existing government or private organizations (e.g., the National Institute of Standards and Technology, the Office of Homeland Security, the Department of Defense, or the Computer Emergency Response Team of the Software Engineering Institute at Carnegie Mellon University); and a second option is to create a national body to coordinate the private sector and local, state, and federal authorities.[13] In the short term, a practical option for providing emergency operational support would be to exploit IT expertise in the private sector, much as the armed services draw on the private sector (National Guard and reserve forces) to augment active-duty forces during emergencies. Such a strategy, however, must be a complement to a

[12]CSTB (2002a).

[13]Note that CSTB has a pending full-scale project on information and network security R&D that will address federal funding and structure in much greater detail than is possible in this report.

more persistent mechanism for providing ongoing IT expertise and assistance to emergency-response agencies.

LONG-TERM RECOMMENDATIONS: INVESTING IN IT RESEARCH

The three areas of IT research described below have significant promise in helping to reduce the likelihood or impact of a terrorist attack:

1. *Information and network security.* Research in information and network security is critically relevant to the nation's counterterrorism efforts for several reasons.[14] First, IT attacks can amplify the impact of physical attacks and lessen the effectiveness of emergency responses; reducing such vulnerabilities will require major advances in information and network security. Second, the increasing levels of damage caused by cybercrime and the tendency to rely on the Internet as the primary networking entity both suggest that the likelihood of severe damage through a cyberattack is increasing. Finally, the evolution of the Internet demonstrates increasing homogeneity in hardware and software, which makes it more vulnerable at the same time that it becomes more critical. To address these problems, more researchers and trained professionals focused on information and network security will be needed. Unfortunately, there are currently fewer researchers in these fields than there were a decade ago.[15]

2. *New IT for emergency response.* C3I (command, control, communications, and information) systems are critical to emergency responders for coordinating their efforts and increasing the promptness and effectiveness of response, i.e., saving lives, treating the injured, and protecting property. The issues raised by C3I for emergency response for terrorist disasters differ from those for natural disasters for several reasons. First, the number of responding agencies, including those from the local, regional, state, and federal levels—with possibly conflicting and overlapping areas of responsibility—increases the level of complexity. Second, there is a need to support immediate rescue and medical operations while also securing the site against further attack. Third, the different agencies—such as rescue, law enforcement, intelligence, and security—often have conflicting needs. For example, security issues distinguish terrorist attacks from natural disasters: In the former, security against further attack is essential and must be provided, but security also generally interferes with immediate operations.

3. *New IT for detection, prevention, remediation, and attribution of attacks.* Information fusion promises to play a central role in countering future terrorist

[14]CSTB (1990, 1999b, 2001a).

[15]"Boehlert Gives Cyber Security Address at ITAA Forum," December 12, 2001. Available online at <http://www.house.gov/boehlert/itaaspeech1212.htm>.

efforts. In every case, information from many sources will have to be acquired, integrated, and appropriately interpreted to support decision makers (ranging from emergency-response units to intelligence organizations). Given the range of formats, the permanence and growing volume of information from each source, and the difficulty of accurately analyzing information from single sources, let alone multiple sources, information fusion offers researchers a challenge.

In each of these areas, discussed in turn below, some knowledge is in hand and partial solutions have been developed. Additional research is needed, however, because these solutions are not sufficiently robust or effective, they degrade performance or functionality too severely, or they are too hard to use or too expensive to deploy.

It must also be noted that although technology is central to all these areas, it is not the sole element of concern. None of the related problems can be solved by technology alone; every solution is subject to the reality of being implemented and operated by humans. These are system issues, where individual, social, and organizational behaviors are part of the system and therefore must be part of the research and design. Technology cannot be studied in isolation from how it is deployed, and failure to attend to the human, political, social, and organizational aspects of solutions will doom technology to failure.

To assist decision makers, the committee has included rough assessments of the criticality of the various research areas identified, the difficulty of particular problems, and the likely time scale on which progress could be made (Table 5.1). The criticality of a research area reflects the vulnerabilities that might be reduced if significant advances in that area were accomplished and deployed; areas are ranked high, medium, or low. The difficulty of the research—that is, how hard it will be to make significant progress—are rated very difficult, difficult, or easy. Finally, the time frame for progress is identified as 1 to 4 years, 5 to 9 years, or 10 years or more. Of course, the *deployment* of research results also presents obstacles, which may reduce effectiveness or lengthen the time until a research result can become a reality. Finally, a caveat: These assessments are subjective and subject to some debate.

Information and Network Security

A broad overview of some of the major issues in information and network security is contained in the CSTB report *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*.[16]

Despite diligent efforts to create an effective perimeter defense for computer and telecommunications systems, penetration by a determined adversary is highly

[16]CSTB (2002a).

TABLE 5.1 A Taxonomy of Priorities

Category	Criticality	Difficulty	Time Scale for R&D for Significant Progress and Deployment
Improved Information and Network Security	High	Difficult	5-9 years
Detection and identification	High	Difficult	5-9 years
Architecture and design for containment	High	Difficult	5-9 years
Large-system backup and decontamination	High	Difficult	5-9 years
Less buggy code	High	Very difficult	5-9 years
Automated tools for system configuration	High	Difficult	1-4 years
Auditing functionality	Low	Difficult	10+ years
Trade-offs between usability and security	Medium	Difficult	5-9 years
Security metrics	Medium	Difficult	1-4 years
Intelligence gathering	Medium	Difficult	1-4 years
Field studies of security	High	Easy	1-4 years
C3I for Emergency Response	High	Difficult	1-4 years
Ad hoc interoperability	High	Easy	1-4 years
Emergency deployment of communications capacity	High	Easy	1-4 years
Security of rapidly deployed ad hoc networks	Medium	Difficult	5-9 years
Information management and decision support tools	Medium	Difficult	5-9 years
Communications with the public during emergency	High	Difficult	1-4 years
Emergency sensor deployment	High	Easy	1-4 years
Precise location identification	Medium	Difficult	5-9 years
Mapping the physical infrastructure of IT	High	Easy	1-4 years
Characterizing the functionality of regional networks for emergency responders	High	Difficult	1-4 years
Information Fusion	High	Difficult	1-4 years
Data mining	High	Difficult	1-4 years
Data integration	High	Difficult	1-4 years

TABLE 5.1 Continued

Category	Criticality	Difficulty	Time Scale for R&D for Significant Progress and Deployment
Language technologies	High	Difficult	1-4 years
Image and video processing	High	Difficult	5-9 years
Evidence combination	Medium	Difficult	1-4 years
Privacy and Confidentiality	High	Difficult	1-4 years
Planning for the Future	Medium	Difficult	10+ years

likely. Software flaws, lax procedures for creating and guarding passwords, compromised insiders, and nonsecure entry points all lead to the conclusion that watertight perimeters cannot be assumed. Nevertheless, strengthening defensive perimeters is helpful, and this section deals with methodologies (those of today and tomorrow) that can detect or confine an intruder and, if necessary, aid in recovery from attack by taking corrective action. (Box 5.2 describes some of the fundamental principles of defensive strategy.) The technology discussed here, as in other parts of this IT chapter, is applicable both to cyberterrorism and cybercrime. In addition, many advances in information and network security can improve computer systems' inherent reliability and availability, which are perennial concerns even under ordinary, nonthreat conditions. Such dual-use capability could help generate broader interest in research and development on defensive technology, as well as motivate its incorporation into industry products.

Research to minimize the damage caused by a cyberattack can be grouped in three generic areas: detection and identification, containment, and recovery.

Authentication, Detection, and Identification

Given that an intruder may gain access to a conventional system or, with significantly more effort, a highly secure system, what technology can be deployed to detect and identify the intruder? Similarly, how do we detect a denial-of-service attack and track its originator?[17]

Detection of an intruder or a denial-of-service attack is more difficult than it

[17]CSTB (1999c), pp. 144-152; CSTB (1999b). A denial-of-service attack is one in which a target is flooded with a huge number of requests for service, thus keeping it busy servicing these (bogus) requests and unable to service legitimate ones.

BOX 5.2
Principles of Defensive Strategy

Computer or telecommunications systems that contain sensitive information, or whose functioning is critical, must be protected at high levels of security. Several policies should be mandatory:

- *Use of encryption for communication between system elements and use of cryptographic protocols*. These practices help to ensure data integrity between major processing elements (e.g., host to host, site to site, element to element); prevent intrusion into the network between nodes (e.g., making "man-in-the-middle" attacks much more difficult); and provide strong authentication (e.g., through the use of public-key-based authentication systems that use encryption and random challenge to strengthen the authentication process or to bind other elements of the authentication such as biometrics to the identity of a user).
- *Minimal exposure to the Internet, which is inherently insecure.* Firewalls are a minimal level of protection, but they are often bypassed for convenience. (Balancing ease of use and security is an important research area discussed elsewhere in this chapter.) Truly vital systems may require an "air gap" that separates them from public networks. Likewise, communication links that must remain secure and available should use a private network. (From a security perspective, an alternative to a private network may be the use of a connection on a public network that is appropriately secured through encryption. However, depending on the precise characteristics of the private network in question, it may—or may not—provide higher availability.)
- *Strong authentication technology for authenticating users.* Security tokens based on encryption (such as smart cards) are available for this purpose, and all entrants from a public data network (such as a network-access provider or insecure dial-in) should use them. Furthermore, for highly critical systems, physical security must also be assured.
- *Robust configuration control* to ensure that only approved software can run on the system and that all the security-relevant knobs and switches are correctly set.

Such measures are likely to affect ease of use and convenience, as well as cost. These are prices that must be paid, however, because hardening critical systems will greatly reduce vulnerability to a cyberattack.

might initially appear. Intruders are often indistinguishable from valid users and frequently take great care to hide their entry and make their behavior look innocuous. Detecting a denial-of-service attack is equally challenging. For example, consider an attack that is launched against the major Internet news services to coincide with a physical bomb attack. It would be nearly impossible to distinguish legitimate users, who would simply be looking for information, from attackers inundating the Web site to try to prevent access to that information, possibly increasing panic and *mis*information.

To date, a number of approaches have offered some promise. One of them calls for authentication so that intruders and bogus traffic can more easily be distinguished. Developing such methods that are both fast and scalable (i.e., effective and fast even when they involve authentication of large numbers of parties) remains the major challenge in this area, however. (One technique that may be worth further development, at least in the context of authenticating traffic to and from heavily used Web sites, is easy-to-use subscription models.[18])

A second approach involves self-monitoring both of users and traffic to detect either anomalous users or unusual traffic patterns that might indicate an active attack. Of course, such monitoring requires good characterizations of what "normal" behavior is and knowledge of what various kinds of behavior mean in the context of specific applications. Today, the major deficiency in this approach is the occurrence of too many false positives. That is, the behavior of legitimate users is sufficiently diverse that infrequent but legitimate behaviors are often mischaracterized as anomalous (and hence hostile).

A third approach uses traps (sometimes referred to as "honeypots")—apparently interesting files crafted to attract the attention of an intruder so that he or she might spend extra time examining it. That extra time can then be used to provide warning of hostile intent, and might help in forensic investigation while the hostile party is connected to the system. More effective honeypots, and the development of forensic tools for use in a honeypot environment, may be fruitful areas of research.

Finally, it is especially important for detection methods to function efficiently in large systems, characterized by thousands (or hundreds of thousands) of simultaneous users and a correspondingly large quantity of communicated data. It will be necessary to monitor these extraordinary volumes without seriously degrading network performance.

Recommendation 5.4: Detection and Identification Research

- **Develop fast and scalable methods for high-confidence authentication.**
- **Explore approaches that could self-monitor traffic and users to detect either anomalous users or unusual traffic patterns.**
- **Develop intruder-detection methods that scale to function efficiently in large systems.**

[18]A subscription model calls for a user to register for service in some authenticated way, so that a site can distinguish that user from a random bad user. Because denial-of-service attacks depend on a flood of bogus requests for service, the availability of a database of registered users makes it easy to discard service requests from those that are not registered—and those are likely to account for the vast majority of bogus requests.

Containment

Today's systems and networks often fail catastrophically. That is, a successful attack on one part of a system can result in an entire system or network being compromised. (An example is that the failure of a perimeter defense surrounding otherwise unprotected systems can result in an intruder gaining full and complete access to all of those systems.) More desirable is a system that degrades gracefully—a successful attack on one part of a system results only in that part of the system being compromised, and the remainder of the system continues to function almost normally.[19]

The principle of graceful degradation under attack is well accepted, but system and network design for graceful degradation is not well understood. Nor are tools available to help design systems and networks in such a manner.

In addition, the building blocks of today's systems are generally commercial off-the-shelf components.[20] Despite the security limitations of such components, economics force systems to be built this way. However, it is not known today how to integrate them safely, how to contain faults, and how to disaggregate them when necessary. While this lack of understanding applies to systems ranging from accounting and payroll systems to telephone switching systems, SCADA systems are a particularly important case.

Architectural containment as a system-design principle calls for the ability to maintain critical functionality (such as engine control on a ship) despite failures in other parts of the system.[21] Such an approach could be one of the most effective long-term methods for hardening IT targets that oversee critical operations.

For the most part, current technologies employ a bimodal approach: either no computer control, which is inefficient in modern large-scale systems, or complete computer control, with the inherent vulnerabilities that this implies.[22] Containment essentially navigates between the two extremes; its essential element is the ability to "lock down" a system under attack—perhaps suspend normal operation temporarily, while the system finds and disables potential intruders, and resume normal system operation afterward—with less disruption than shutting down and rebooting might cause.

Research is thus necessary in several areas: understanding how to fuse a simple, highly secure, basic control system used primarily for crisis operations

[19]CSTB (1999c), pp. 144-152.

[20]CSTB (1999b).

[21]Note that an essential aspect of designing for containment is the ability to define and prioritize what functions count as essential. For systems used by multiple constituencies, the existence of this ability cannot be taken for granted.

[22]As an example, consider that a shipwide networking failure on the USS *Yorktown* left the ship without the ability to run its engines.

with a sophisticated, highly effective, computer control system used for normal operations; "decontamination" of a system while it is being used (see below); and resuming operations without the need for going offline. One "grand challenge" might be the development of a system that could be made more secure at the touch of a button; the cost would be in losing some nonessential functionality while the system simultaneously decontaminated itself or shut out attackers. Another serious problem for which few general solutions are known is the distributed denial-of-service attack.

Recommendation 5.5: Containment Research

- **Develop the tools and design methodologies for systems and networks that support graceful degradation in response to an attack.**
- **Develop mechanisms to contain attackers and limit damage rather than completely shutting down the system once an intrusion is detected.**
- **Explore how to fuse a simple, basic control system used during crisis mode with a sophisticated control system used during normal operations.**

Recovery

Once an intruder has been detected, confined, and neutralized, the goal should be to bring the system to full operation as soon as possible. This is the task of the recovery process. Like containment, recovery has major applications for reliability, although the presence of a determined adversary makes the problem considerably harder. Recovery includes preparations not only to help ensure that the system is recoverable but also to enable active reconstitution of a good system state.

Backup is an essential prerequisite for reconstitution. Although the basic concepts of system backup are well understood, there are major challenges to performing and maintaining backups in real time so that as little system state as possible is lost. However, normal backup methods have been developed under the assumption of benign and uncorrelated failure, as opposed to a determined attacker who is trying to destroy information. Further, backups of large systems take a long time, and if the systems are in use during the backup, the system state can change appreciably during that time. Thus, research is needed on ways to preserve information about system state during backup.

Unlike a restore operation used to recreate a clean system after a failure, reconstitution requires an additional step: decontamination, which is the process of distinguishing clean system state (unaffected by the intruder) from the portions of infected system state, and eliminating the causes of those differences. Because system users would prefer that as little good data as possible be discarded, this problem is quite difficult. Decontamination must also remove all active infections, as well as any dormant viruses. Once decontamination is performed,

attention can be turned to forensics in an attempt to identify the attacker[23] and acquire evidence suitable for prosecution or retaliation. In the end, this ability is critical to long-term deterrence.

Given that penetration of computer and telecommunications networks is likely to continue despite our best efforts to build better perimeter security, more resilient and robust systems are necessary, with backup and recovery as essential elements.

New approaches to decontamination are also needed, especially when a system cannot be shut down for decontamination purposes. At present, much of the activity associated with a properly running system interferes with decontamination efforts (particularly with respect to identifying a source of contamination and eliminating it).

Recommendation 5.6: Recovery Research

- **Develop schemes for backing up large systems, in real time and under "hostile" conditions, that can capture the most up-to-date, but correct, snapshot of the system state.**
- **Create new decontamination approaches for discarding as little good data as possible, and for removing active and potential infections, on a system that cannot be shut down for decontamination.**

Cross-Cutting Issues in Information- and Network-Security Research

A number of issues cut across the basic taxonomy of detect and identify, contain, and recover described above.

Reducing Buggy Code. Progress in making systems more reliable will almost certainly make them more resistant to deliberate attack as well. But buggy code underlies many reliability problems, and no attempt to secure systems can succeed if it does not take this basic fact into account.[24]

Buggy software is largely a result of the fact that despite many years of serious and productive research in software engineering, the creation of software is still more craft than science-based engineering. Furthermore, the progress that has been made is only minimally relevant to the legacy software systems that remain in all infrastructure.

Software-system bugs can result from a variety of causes, ranging from low-level syntax errors (e.g., a mathematical expression uses a "plus" sign when it should use a "minus" sign) to fundamental design flaws (e.g., the system functions as it was designed to function, but it does so in an inappropriate place).

[23]CSTB (1999c), pp. 144-152.
[24]CSTB (1990, 1999b).

Buffer overflow—in which memory is overwritten—is a particularly common kind of bug that frequently causes system crashes and can be exploited by an adversary to gain control over a target system.

Dealing with buggy code is arguably the oldest unsolved problem in computer science, and there is no particular reason to think that it can be solved once and for all by any sort of crash project. Nevertheless, two areas of research seem to be particularly important in a security context:

1. *Security-oriented tools for system development*. Tools can be designed to audit source code for certain classes of common flaws.[25] Better programming languages may help as well. (For example, Java and similarly type-safe languages are more resistant to buffer overflows than are other languages.[26]) More tools that support security-oriented development would be useful.

2. *Trustworthy system upgrades and bug fixes*. It often happens that a system bug is identified and a fix to repair it is developed. Obviously, repairing the bug may reduce system vulnerability, so system administrators and users should have some incentive to install the patch. However, with current technology, the installation of a fix or a system upgrade carries many risks—a nontrivial chance of causing other problems, a break in existing functionality, or possibly the creation of other security holes, even when the fix is confined to a module that can be reinstalled.[27] The essential reason for this problem is that while fixes are tested, the number of operational configurations is much larger than the number of test configurations that are possible. Research is thus needed to find ways of testing bug fixes reliably and of developing programming interfaces to modularize programs that cannot be bypassed.

Misconfigured Systems. Because existing permission and policy mechanisms are hard to understand, use, and verify, many problems are caused by their improper administration.[28] There is also a trade-off between granularity of access control and usability. For example, an entire group of people may be given access privileges when only one person in that group should have them. Or a local system administrator may install a modem on the system he or she administers with the intent of obtaining access from home, but this also provides intruders with an unauthorized access point. The ability to generate a crisp, clear description of actual security policies in place and to compare them with desired security

[25]Wagner, D.A. 2000. "Static Analysis and Computer Security: New Techniques for Software Assurance," Ph.D. dissertation, University of California, Berkeley.

[26]Type-safe languages allow memory accesses only to specifically authorized locations. For example, programs written in type-safe languages cannot read or write to memory locations that are associated with other programs.

[27]Brooks, Frederick P. 1975. *The Mythical Man-Month*. Addison-Wesley, Boston, Mass.

[28]CSTB (1990, 1999b).

policies would be helpful. Thus, better system-administration tools for specifying security policies and checking system configurations quickly against prespecified configurations should be developed.

Auditing Functionality. Validation sets are used to ensure that a piece of hardware (e.g., a chip) has the functionality that its design calls for. However, these sets typically test for *existing* functionality—that is, can the hardware properly perform some specified function? They do not test for unauthorized functionality that might have been improperly inserted, perhaps by someone seeking to corrupt a production or distribution chain. Research is needed for developing tools to ensure that all of the called-for functionality is present *and* that no additional functionality is present as well.

Managing Trade-offs Between Functionality and Security. As a general rule, more secure systems are harder to use and have fewer features.[29] Conversely, features—such as executable content and remote administration—can introduce unintended vulnerabilities even as they bring operational benefits. (For example, newer word processors allow the embedding of macros into word processing files, a fact that results in a new class of vulnerabilities for users of those programs as well as added convenience.) More research is required for performing essential trade-offs between a rich feature set and resistance to attack.

Transparent, or at least point-and-click, security would be more acceptable to users and hence would be employed more frequently. For example, there are many authentication mechanisms, both electronic and physical, but the most convenient one to use—passwords—has many serious, well-known disadvantages. Smart cards are more secure, but a user must have them available when needed. New authentication mechanisms that combine higher security with lower inconvenience are needed.

Security Metrics. Many quantitative aspects of security are not well understood. For example, if a given security measure is installed—and installed properly (something that cannot be assumed in general)—there is no way of knowing by how much system security has increased. Threat models are often characterized by actuarial data and probability distributions in which the adverse effects of vulnerabilities are prioritized on the basis of how likely it is that they will occur; but such models are of little use in countering deliberate terrorist attacks that seek to exploit nominally low-probability vulnerabilities. Notions such as calculating the return on a security investment—common in other areas in which security is an issue—are not well understood either, thus making quantitative risk manage-

[29]CSTB (1990), pp. 159-160.

ment a very difficult enterprise indeed.[30] Research is needed for developing meaningful security metrics.

Intelligence Gathering. Given the rate at which information technology changes, it is likely that new types of attack will emerge rapidly. Because insight into the nature of possible attacks is likely to result in additional options for defense, it is highly desirable to keep abreast of new vulnerabilities and to understand the potential consequences if such vulnerabilities were to be exploited.

Field Studies of Security. Traditional criteria, as specified in the Orange Book,[31] have not been successes. They do not capture current needs or models of computation.[32] Worse yet, they have largely failed in the marketplace; very few customers actually bought Orange Book-rated systems, even when they were available. Understanding why previous attempts to build secure systems and networks have failed in the marketplace, or in defending against outside attack, would help to guide future research efforts. (Note that human and organizational factors are key elements of such analysis, as mentioned above.)

Recommendation 5.7: Crosscutting Issues in Information- and Network-Security Research

- **Develop tools that support security-oriented systems development.**
- **Find new ways to test bug fixes reliably.**
- **Develop better system-administration tools for specifying security policies and checking against prespecified system configurations.**
- **Create new tools to detect added and unauthorized functionality.**
- **Develop authentication mechanisms that provide greater security and are easier to use.**
- **Create and employ metrics to determine the improvement to system security resulting from the installation of a security measure.**
- **Monitor and track emerging types of attack and explore potential consequences of such attacks.**
- **Understand why previous attempts to build secure systems have failed and recommend how new efforts should be structured to be more successful.**

---

[30]Information on the economic impact of computer security is given in "The Economic Impact of Role-Based Access Control," National Institute of Standards and Technology, March 2002. Available online at <http://www.nist.gov/director/prog-ofc/report02-1.pdf>.

[31]The "Orange Book" is the nickname for the Trusted Computer System Evaluation Criteria, which were intended to guide commercial system production generally and thereby improve the security of systems in use. Its principal failing was the omission of networking concerns, which arose during the lengthy period between the time it was first drafted and its final approval.

[32]CSTB (1999c), pp. 144-152, and CSTB (1990, 1999b).

IT and C3I for Emergency Response

Technologies for command, control, communications, and information (C3I) have major importance in the response phase of a disaster.

In general, the IT infrastructure must be robust in the face of damage.[33] Although incident management has been well studied,[34] the IT requirements for such management do not appear to have been thoroughly conceived—even though in a disaster it is essential that IT systems provide for the capability to deliver information, interagency communication and coordination, and communication with those affected both within and beyond the immediate disaster area. Equipment must be deployed immediately to provide for appropriate communication to those responding to the situation, among the multiple agencies in the private and public sectors that are affected, and to and between those directly affected by the incident.[35]

There are many options for helping to facilitate interoperable crisis communications among emergency-response agencies. For example, it is likely that some portion of the public networks will survive any disaster; emergency-response agencies could use it to facilitate interoperability if there are mechanisms for giving them first priority for such use. A second option is to allocate dedicated spectral bands for emergency responders and to require by law that they use those frequencies. A third option is to mandate frequency and waveform standards for emergency responders so that they are interoperable. A fourth option is to develop technology to facilitate interoperable communications among emergency responders. Of course, these options are not mutually exclusive.

In addition, numerous computational and database facilities must be established to provide complete and real-time information[36] to diverse constituencies whose information and communication requirements, security needs, and authorizations all differ. These facilities must be established quickly, as minutes and even seconds matter in the urgent, early stages of an incident.[37] Furthermore, tight security is essential, especially if the incident is the result of a terrorist attack, because an active adversary might try to subvert the communications or destroy data integrity.[38] In addition, an atmosphere of crisis and emergency provides opportunities for hostile elements to overcome security measures that are normally operative under nonemergency circumstances; thus, another research area is how to build systems that permit security exceptions to be declared without introducing new vulnerabilities on a large scale.

---

[33]CSTB (1999a), p. 39.
[34]Christen et al. (2001).
[35]CSTB (1996), p. 14.
[36]CSTB (1999a), p. 29.
[37]CSTB (1999a), p. 83, and CSTB (1996), p. 12.
[38]CSTB (1996), p. 24.

Efforts to coordinate communications are complicated by the fact that emergency response to a large-scale incident has many dimensions, including direct on-the-ground action and response, management of the incident response team, operations, logistics, planning, and even administration and finance. Moreover, response teams are likely to include personnel from local, county, state, and federal levels.[39]

Research in a number of areas can advance the state of the art for emergency-response C3I systems, thereby improving their effectiveness for terrorist incidents. In addition, the development of better C3I systems for emergency response will have application to responding to natural disasters as well.

Ad Hoc Interoperability

Different emergency responders must be able to communicate with each other, but poor interoperability among responding agencies is a well-known problem—and one that is as much social and organizational as it is technical. The fundamental technical issue is that different agencies have different systems, different frequencies and waveforms, different protocols, different databases, and different equipment.[40] At the same time, existing interoperability solutions are ad hoc and do not scale well.[41] Moreover, the nature of agencies' missions and the political climates in which they traditionally operate make it difficult for them to change their communication methods. Thus, it is unlikely that agencies will ever be strongly motivated to deploy interoperable IT systems.

Exercises may help identify and solve some social and organizational problems, but rivalries and political infighting about control and autonomy will probably remain. It is for this reason that the notion of uniform standards to which the communications protocols of different agencies will adhere is not likely to be an adequate solution to problems of interoperability. Indeed, such exercises are of particular value precisely because they help to reveal the rivalries and infighting whose resolution is important to real progress in this area.

The communication process somehow has to work within this reality of organizational resistance.[42] In the ideal case, communication among the myriad agencies that respond to a crisis would be done smoothly through at least three different phases. In the first phase, the initial responding agencies immediately deploy their ad hoc communication structures, using their existing communication facilities and equipment. In the second phase, the agency-specific communication structure transitions to one that is systemwide. In the third phase, the

---

[39]CSTB (1999a), p. 7.
[40]CSTB (1999a), p. 26.
[41]CSTB (1999b)), p. 119.
[42]CSTB (1999a), p. 27.

multiple organizations establish full, efficient interoperability.[43] At this point, all participants should be able to communicate with critical teams and get essential information in a timely and efficient manner. Critical central decisions should flow smoothly downward. Similarly, low-level urgent requests for communication, assistance, or information should flow upward to the appropriate agency and then back to the appropriate operatives.[44] Interactions take place among responders and between responders and the public; people who have not worked closely with one another are suddenly brought together under demanding circumstances, yet they are expected to interact well.[45]

In most actual cases, however, these "phases" do not proceed so smoothly. Research is clearly needed on transitioning from the initial, unit-specific, ad hoc structure to an interoperable, systemwide structure and in a graceful manner, with zero or minimal disruption of function during that transfer.[46] This complex problem requires study both by technologists and social scientists: The technologies must be easy enough to use so that they complement the users rather than distract them from their missions, and the technologies of different responders must complement each other as well (or at least not clash).[47]

Thus research is also needed for defining low-level communication protocols and developing generic technology that can facilitate interconnection and interoperation of diverse information resources.[48] One example of research is the development of software-programmable waveforms that can (in principle) allow a single radio to interoperate with a variety of different wireless communications protocols.[49] A second example is an architecture for communications, perhaps for selected mission areas, that translates agency-specific information into formats and semantics compatible with a global system.[50]

Emergency Management of Communications Capacity

In an emergency, extraordinary demands are placed on communications capacity. A disaster is likely to destroy some but not all of the communications infrastructure in a given area, leaving some residual capability. Meanwhile, the disaster provokes greater demands for communication from the general public. The result is often a denial-of-service condition for all, including emergency-

---

[43]CSTB (1996), p. 21.
[44]CSTB (1999a), pp. 25-26.
[45]CSTB (1999a), pp. 30, 32.
[46]CSTB (1999a), p. 26.
[47]CSTB (1999a), pp. 50, 84; and CSTB (1996), p. 33.
[48]CSTB (1999a), p. 85
[49]CSTB (1997).
[50]See CSTB (1999c) for a discussion of mission slices and working the semantic interoperability problem.

communications services. The absence of a telephone dial tone in a disaster area is common because of increased demands.[51] Even under high-traffic but non-emergency situations, cell-phone networks are sometimes unable to handle the volume of users in a given cell because of statistical fluctuations. Nor is the Internet immune to such problems—congestion of shared Internet links, including both last-mile and aggregated feeder links, can cause lockouts to occur on facilities that are still operational in the disaster area.

Research is needed on using residual (and likely saturated) capacity more effectively, deploying additional (surge) capacity,[52] and performing the trade-offs among different alternatives. One problem in this area is the management of traffic congestion and the development of priority overrides for emergency usage (and prevention of the abuse of such authority).[53] A second problem is that optimization algorithms for communications traffic that are appropriate in normal times may have to be altered during emergencies. For example, the destruction of physical facilities such as repeaters and the massive presence of debris could result in an impaired environment for radio-frequency transmissions. The rapid deployment of processors optimized to find weak signals in a suddenly noisier environment could do much to facilitate emergency communications. DSL systems, for example, can reallocate huge bandwidth to a single phone line by coordinating it with all the phone lines nearby (one can sometimes get 10 times the bandwidth if this is done right). Under normal circumstances, the interests of the other users would defeat such a system (with cross talk), but in an emergency those interests could be reprioritized.

Research is also needed for self-adaptive networks that can reconfigure themselves in response to damage and changes in demand, and that can degrade gracefully.[54] For example, in a congested environment, programmed fallback to less data-intensive applications (e.g., voice rather than video, text messaging rather than voice) may provide minimal communications facility. Even today, many cellular networks allow the passing of text messages. Also, public and private elements of communications infrastructure could both be tapped to provide connectivity in a crisis,[55] as happened in New York City on September 11.

---

[51]CSTB (1996), p. 17.

[52]CSTB (1999a), p. 83.

[53]CSTB (1999a), p. 39. In addition, the White House's National Communications System office has moved to implement a wireless priority service that facilitates emergency recovery operations for the government and local emergency-service providers. This service will be implemented in phases, with an immediate solution available in early 2002 in selected metropolitan areas and a nationwide solution (yet to be developed) scheduled for late 2003. Further work after 2003 will concentrate on the development and implementation of third-generation technologies that enable high-speed wireless data services. See Convergence Working Group, *Report on the Impact of Network Convergence on NS/EP Telecommunications: Findings and Recommendations*, February 2002.

[54]CSTB (1999a), p. 39.

[55]CSTB (1999a), p. 39.

Security of Rapidly Deployed Ad Hoc Networks

The management of communications networks poses unique problems in a crowded, emergency disaster zone. Security must be established rapidly from the outset, as the terrorists might try to mix among the first responders.[56] It is also necessary to determine a means for temporarily suspending people's access to facilities, communications, and data without impeding the ability of those with legitimate need to use them. Yet this suspension process has to be done rapidly, given that minutes and seconds matter in severe emergencies.

Research is therefore needed on the special security needs of wireless networks that are deployed rapidly and in an ad hoc manner. (For example, ad hoc networks are not likely to have a single system administrator that can take responsibility for allocating user IDs.)

Information-Management and Decision-Support Tools

In a chaotic disaster area, a large volume of voice and data traffic will be transmitted and received on handheld radios, phones, digital devices, and portable computers. Nevertheless, useful information is likely to be scarce and of limited value. Thus, research is needed on "decision-support" tools that assist the crisis manager in making the most of this incomplete information.[57]

Communications with the Public During an Emergency

In a crisis, channels to provide information to the public will clearly be needed. Radio, television, and often the Web provide such information today, but it is usually generic and not necessarily helpful to people in specific areas or with specific needs. Research is needed to identify appropriate mechanisms—new technologies such as "call by location" and zoned alert broadcasts—for tailoring information to specific locations or individuals.[58] To be effective in interacting with individual users, ubiquitous and low-cost access is required.[59] In addition, such systems should be highly robust against spoofing (entry by an intruder masquerading as a trusted host) so that only authorized parties can use them to send out information.

For example, the current cell-phone system does not directly support these functions, but it might be possible to modify and exploit it to provide "reverse 911" service,[60] i.e., a one-way channel to those affected that provides a continual

[56]CSTB (1996), p. 24.
[57]CSTB (1996), p. 104.
[58]CSTB (1999a), p. 35.
[59]CSTB (1999a), p. 40.
[60]CSTB (1999a), p. 35.

flow of relevant information and guidance. Such mechanisms would probably have to be locally self-sufficient. That is, the disaster might spare the local cell site—or a temporary cell site could be deployed along with wireless alternatives[61] —but access to central services might not be possible.

Finally, providing information to those located outside the immediate emergency area gives important psychological comfort and helps to mitigate the disaster's consequences. (For example, in the immediate aftermath of the September 11 attacks, "I'm alive" bulletin boards sprang up spontaneously.) Research is needed for establishing more effective means of achieving this objective—especially in updating the status of affected people—while compromising the local communications infrastructure to a minimal degree.

Emergency Sensor Deployment

During an emergency, responders need information about physical on-the-ground conditions that is sufficiently fine-grained and accurate to be useful. It is virtually inevitable that no preexisting sensor network will be in place to provide adequate information, so the deployment of sensors in response to a disaster is likely to be necessary. Depending on the nature of the emergency, sensor capacity would be needed to identify and track the spread of nuclear, chemical, or biological contaminants, characterize and track vehicular traffic, locate survivors (e.g., through heat emanations, sounds, or smells), and find pathways through debris and rubble. Developing robust sensors for these capabilities is one major challenge; developing architectural concepts for how to deploy them and integrate the resulting information is another.

Precise Location Identification

In a severe crisis, determining the location both of physical structures and of people is a major problem because of debris, airborne contaminants such as smoke and dust, and perhaps simply a lack of illumination. Therefore, technological solutions, such as embedded location sensors, are probably essential. Distributed sensor networks, either already in place or deployed in response to an incident, can be valuable information sources.[62]

While technologies like the Global Positioning System could also play a major role, airborne contaminants and equipment damage might render them ineffective. The information needs of the responders and those affected will thus

[61]CSTB (1996), p. 18.
[62]CSTB (1996), pp. 24, 25; CSTB (2001a).

require rapid access to accurate databases—of blueprints and building diagrams, for example.[63]

Research is needed to develop digital floor plans and maps of other physical infrastructure.[64] The resulting data could be stored in geographic information systems (GIS), which would allow responders to focus on the high-probability locations of missing people (such as lunchrooms) and avoid dangerous searches of low-probability locations (such as storage areas).[65] Research is needed in wearable computers for search-and-rescue operations[66] so that responders could update the GIS in real time as they discover victims and encounter infrastructural damage. Another research area is in "map ants"[67]—distributed, self-organizing robots deployed in a disaster area to sense movement or body heat, for instance. It may also be possible to develop technology to generate the data for accurate maps of a debris-strewn disaster location.

Finally, keeping track of emergency responders' positions within a disaster area is an essential element of managing emergency response. Technology (similar to E-911 for cell phones) to monitor the progress of these individuals automatically is not yet available on a broad scale.

Mapping the Physical Infrastructure of IT

As noted above, the telecommunications infrastructure is for the most part densely connected; hence physical attack is unlikely to disrupt it extensively for long periods of time. However, the physical infrastructure of telecommunications (and the Internet) does not appear to be well understood (that is, immediate knowledge of where various circuits are located is unavailable), and there may well exist critical nodes whose destruction would have a disproportionate impact. (On the other hand, knowing where these critical nodes are is difficult for both network operators and terrorists.) Thus an important priority is to develop tools to facilitate the physical mapping of network topology, and to begin that mapping now with the tools that are currently available. This is particularly important for converged networks over which both voice and data are carried.

---

[63]Hightower, J., and G. Boriello. 2001. "Location Systems for Ubiquitous Computing," IEEE Computer, Vol. 33, No. 8, August.

[64]As one example, consider that a firm that installs fiber-optic cables in a city's sewers is capable of mapping those sewers as well using a sewer-crawling robot that lays cable and tracks its position.

[65]CSTB (1996), p. 14.

[66]CSTB (1999a), p. 38.

[67]A study in progress by the Computer Science and Telecommunications Board, *Intersections Between Geospatial Information and Information Technology,* discusses these self-organizing robots.

Characterizing the Functionality of Regional Networks for Emergency Responders

To develop mechanisms for coordinating emergency-response activities, it is necessary to understand what the various communications and computer networks of emergency responders in a given region are supposed to do. For example, managers from different agencies often speak different "languages" in describing their needs, capabilities, and operational priorities; a common conceptual framework for these purposes would be enormously helpful for coordination of planning activities, yet one is not yet available.[68] Sharing of information among the various providers of critical infrastructure and emergency-response agencies, even about common tasks and processes, has been a rather uncommon activity in the past.

Recommendation 5.8: IT and C3I Research

- **Understand how to transition gracefully and with minimal disruption from a unit-specific communication system to a systemwide structure.**
- **Define new communication protocols and develop generic technology to facilitate interconnection and interoperation of diverse information sources.**
- **Develop approaches for communication systems to handle surge capacity and function in a saturated state.**
- **Develop methods to provide more capacity for emergency communication and coordination.**
- **Create self-adaptive networks that can reconfigure themselves as a function of damage and changes in demand and that can degrade gracefully.**
- **Understand the special security needs of rapidly deployed wireless networks.**
- **Develop decision-support tools to assist the crisis manager in making decisions based on incomplete information.**
- **Explore mechanisms to provide information tailored to specific individuals or locations through location-based services.**
- **Establish more effective means of communicating the status of affected people to those outside the disaster area.**
- **Develop robust sensors and underlying architectural concepts to track and locate survivors as well as to identify and track the spread of contaminants.**

---

[68]Christen, Hank, et al., "An Overview of Incident Management," *Perspectives on Preparedness,* No. 4, September 2001, available online at <http://ksgnotes1.harvard.edu/BCSIA/Library.nsf/pubs/PO4>.

- **Create digital floor plans and maps of other physical infrastructure, and use wearable computers and "map ants" to generate maps that can be updated.**
- **Develop tools to map network topology, especially of converged networks that handle voice and data traffic.**
- **Begin to characterize the functionality of regional networks for emergency responders.**

Information Fusion

Promising to play a central role in the future prevention, detection, and remediation of terrorist acts, "information fusion" is defined as the use of computer technology to acquire data from many sources, integrate these data into usable and accessible forms, and interpret them. Such processed data can be particularly valuable for decision makers in law enforcement, the intelligence community, emergency-response units, and other organizations combating terrorism. Not surprisingly, an inherent problem of information fusion is data interoper-ability—the difficulty of merging data from multiple databases, multiple sources, and multiple media.

- *Prevention.* Security checkpoints have become more important and more tedious than ever at airports, public buildings, sporting venues, and national borders. But the efficiency and effectiveness of checkpoints could be significantly improved by creating information-fusion tools to support the checkpoint operator in real time. For example, future airport-security stations could integrate data received from multiple airports to provide a more global view of each passenger's luggage and activities on connecting flights. The stations could use data-mining methods to learn which luggage items most warrant hand-inspection, and they could capture data from a variety of biometric sensors to verify the identities of individuals and search for known suspects.
- *Detection.* Intelligence agencies are routinely involved in information fusion as they attempt to track suspected terrorists and their activities, but one of their primary problems is managing the flood of data. There are well-known examples in which planned terrorist activity went undetected despite the fact that relevant evidence was available to spot it—the evidence was just one needle in a huge haystack. Future intelligence and law-enforcement activities could therefore benefit enormously from advances in automatic interpretation of text, image, video, sensor, and other kinds of unstructured data. This would enable the computer to sort efficiently through the massive quantities of data to bring the relevant evidence (likely combined from various sources) to the attention of the analyst.
- *Response.* Early response to biological attacks could be supported by collecting and analyzing real-time data, such as admissions to hospital emer-

gency rooms and veterinary offices or purchases of nonprescription drugs in grocery stores, and integrating it with background information about the affected patient's residence and job address. Prototype systems are already under development, including one that monitors real-time admissions to 17 emergency departments near Pittsburgh, to generate profiles of ER visits, and discern patterns of activity. If anomalous patterns emerge that may signify an outbreak of some new pathogen, system administrators can quickly alert health officials.

Many other opportunities exist for such computer-aided "evidence-based decision making." For example, the monitoring of activity on computer networks might flag potential attempts to break through a firewall; or sensor networks attached to public buildings might flag patterns of activity within the building that suggest suspicious behavior. In these kinds of cases, because the data is voluminous and derives from a variety of sources, an unaided decision maker might have difficulty detecting subtle patterns.

As a general proposition, the development of tools that provide human analysts with assistance in doing their jobs has a higher payoff (at least in the short to medium term) than tools that perform most or all of the analyst's job. This places a greater emphasis on approaches that use technology to quickly sift large volumes of data to flag potentially interesting data items for human attention (as opposed to approaches that rely on computers to make high-level inferences themselves in the absence of human involvement and judgment).

A final dimension of information fusion is nontechnical. That is, disparate institutional missions may well dictate against a sharing of information at all. Underlying successful information fusion efforts is a *desire* to share information—and it is impossible to fuse information belonging to two agencies if those two agencies do not communicate with each other. Establishing the desire to communicate among all levels at which relevant information could be shared may have a larger impact than the fusion that might occur due to advances in technology.

Data Mining

"Data mining" is the automatic machine-learning of general patterns from a large volume of specific cases. For example, given a set of known fraudulent and nonfraudulent credit-card transactions, the computer system may learn general patterns that can be used to flag future cases of possible fraud. Data mining has grown quickly in importance in the commercial world over the past decade, as a result of the increasing volume of machine-readable data, advances in statistical machine-learning algorithms for automatically analyzing these data, and improved networking that makes it feasible to integrate data from disparate sources. Decision-tree learning, neural-network learning, Bayesian-network learning, and logistic-regression-and-support vector machines are among the most widely used

statistical machine-learning algorithms. Dozens of companies now offer commercial implementations, which are integrated into database and data-warehousing facilities.

A typical commercial application of data mining is fraud detection for credit cards, telephone calls, and insurance claims (by learning from historical data on transactions known to be fraudulent). Other applications are in assessing mortality risk for medical patients (by learning from historical patient data) and predicting which individuals are most likely to make certain purchases (by analyzing data on other individuals' past purchasing). The majority of these commercial data-mining applications involve well-structured data.

Limitations of the current commercial technology include the inability to mine data that is a combination of text, image, video, and sensor information (that is, data in "nonstructured" formats) as well as the inability to incorporate the knowledge of human experts into the data-mining process. Despite the significant value of current machine-learning algorithms, there is also a need to develop more accurate learning algorithms for many classes of problems.

New research is needed to develop data-mining algorithms capable of learning from data in both structured and nonstructured formats. And whereas current commercial systems are very data-intensive, research is needed on methods for learning when data are scarce (e.g., there are only a few known examples of some kinds of terrorist activity) by incorporating knowledge of human experts alongside the statistical analysis of the data. Another research area is better mixed-initiative methods that allow the user to visualize the data and direct the data analysis.

Data Integration

New research is needed to normalize and combine data collected from multiple sources, such as the combination of different sets of time-series data (e.g., with different sampling rates, clocks, and time zones) or collected with different data schemas (e.g., one personnel database may use the variable "JobTitle" while another uses "EmployeeType").

Language Technologies

The area of language technologies has developed a wide variety of tools to deal with very large volumes of text and speech. The most obvious commercial examples are the Web search engines and speech-recognition systems that incorporate technology developed with DARPA and NSF funding. Other important technologies include information extraction (e.g., extraction of the names of people, places, or organizations mentioned within a document), cross-lingual retrieval (e.g., does an Arabic e-mail message involve discussion of a chemical weapon?), machine translation, summarization, categorization, filtering (moni-

toring streams of data), and link detection (finding connections). Most of these approaches are based on statistical models of language and machine-learning algorithms.

A great deal of online information, in the form of text such as e-mail, news articles, memos, and pages on Web sites, is of potential importance for intelligence applications. Research is needed on methods for accurately extracting from text certain structured information such as descriptions of events—e.g., the date, type of event, actors, and roles. Research is needed to handle multiple languages, including automatic translation, cross-lingual information retrieval, and rapid acquisition of new languages. Other important areas of future research are link detection (related to the normalization problem mentioned above) and advanced question answering.

Image and Video Processing

The technologies for image and video processing tend to be domain-specific and often combine information from multiple modes. For example, several companies are beginning to offer image-recognition software for face recognition and automatic classification of medical and other types of images. Commercially available video indexing-and-retrieval software improves effectiveness by combining techniques of segmentation, face detection, face recognition, key-frame extraction, speech recognition, text-caption extraction, and closed-caption indexing. This is a good example of information fusion in which multiple representations of content are combined to reduce the effect of errors coming from any given source.

The major limitation of present language and image technologies is that their accuracy and performance, despite significant progress, need to be considerably improved. This is particularly true for counterterrorist systems where the data may be very noisy (that is, surrounded by irrelevant information) and sparse.

Work is needed on improved algorithms for image interpretation and speech recognition. Many of these research issues are specific to problems arising in a particular medium—e.g., recent progress on face recognition has come primarily from understanding how to extract relevant image features before applying machine learning methods, though this approach may not be applicable to machine learning in other contexts. However, new research is also needed on perception based on mixed media—e.g., speech recognition based on sound combined with lip motion.

Evidence Combination

Many of the techniques used to combine information from multiple sources, as in video indexing or metasearch engines, are ad hoc. Current research on principle-based methods for reasoning under uncertainty needs to be extended

and tested extensively in more demanding applications. This is a key technical problem, with widespread implications for many of the applications mentioned above—e.g., how to combine evidence from hospital admissions and from non-prescription drug purchases to detect a probable bioterrorist attack; how to combine evidence from face recognition and voice print to estimate the likely identity of a person; or how to combine evidence from multiple sensors in a building to detect anomalous activity.

Recommendation 5.9: Information Fusion Research

- **Develop more effective machine-learning algorithms for data mining, including learning using different data types (text, image, audio, video).**
- **Develop methods for systems to learn when data are scarce.**
- **Create better mixed-initiative methods that allow the user to visualize the data and direct the data analysis.**
- **Explore new methods to normalize and combine data from multiple sources.**
- **Create methods to extract structured information from text.**
- **Build approaches to handle multiple languages.**
- **Improve algorithms for image interpretation, speech recognition, and interpretation of other sensors (including perception based on mixed media).**
- **Extend, and test extensively in more demanding applications, the principle-based methods for reasoning under uncertainty.**

PRIVACY AND CONFIDENTIALITY

As pressure mounts for the government to collect and process more information, it becomes increasingly important to address the question of how to minimize the negative impacts on privacy and data confidentiality.

Research is needed to provide policy makers with accurate information about the impact on confidentiality of different kinds of data disclosure. Research is also needed on new data-mining algorithms that discover general trends in data without requiring full disclosure of the individual data records. One example is data-mining algorithms that work by posing statistical queries to each of a set of databases, rather than gathering every data record into a centralized repository. Another is zero-knowledge data mining, in which general trends in data can be uncovered without requiring full disclosure of individual data records. (However, note that for many applications such as badges and access tokens, personal information of the sort mentioned is not necessary; the only requirements are that the token be recognizable as valid and that it has been issued to the person presenting it. It doesn't even have to have an individual's name on it.)

A related issue is the fact that a sufficient aggregation of nonpersonally identified information can often be used to identify a person uniquely. For

example, identifying someone as a man of Chinese extraction with a doctorate in physics who enjoys swing dancing, has an adopted 7-year-old daughter, and lives in upper-northwest Washington, D.C., is likely sufficient to specify a unique individual. Thus, the mere fact that information is disconnected from personal identifiers is no assurance that an individual cannot be identified if data are aggregated.

PLANNING FOR THE FUTURE

Planning for the future is also a critical dimension of any research agenda, though the resources devoted to it need not be large. New system architectures and technologies, such as switched optical networks, mobile code, and open-source or multinational code development, will have different vulnerabilities and hence require different defense strategies. Similarly, new device types such as digital appliances, wireless headphones, and network-capable cell phones pose new challenges. Even today, it is hard to interconnect systems with different security models or security semantics; and unless we deal with this problem, it will become increasingly difficult in the future.

Furthermore, the characteristics of deployed technology that protect the nation against catastrophic IT-only attacks today (e.g., redundancy, system heterogeneity, and a reliance on networks other than the Internet for critical business functions) may not obtain in the future. Indeed, some trends, such as deregulation, system monocultures, and the dominance of a smaller number of products, are pushing the nation's critical infrastructure providers to reduce excess capacity, even though this is what provides much of the redundancy so important to reduced vulnerability.

For these reasons, researchers and practitioners must be vigilant to changes in network technology, usage and reliance on IT, and potentially decreasing diversity. In addition, research focused on the future is likely to have a slant that differs from those of the other research efforts described in this chapter. While the latter efforts might be characterized as building on existing bodies of knowledge (and are in that sense incremental), future-oriented research would have a more radical orientation: It would try to develop alternative paradigms for secure and reliable operation that would not necessarily be straightforward evolutions from the Internet and information technology of today.

For example, one such pursuit might be the design of appropriate network infrastructure for deployment in 2020 that would be much more secure than the Internet of today. Another might be an IT infrastructure whose security relied on engineered system diversity—in which deployed systems were sufficiently similar to be interoperable yet sufficiently diverse to essentially be resistant to large-scale attacks.

IMPLEMENTATION

The IT research areas of highest national priority for counterterrorism are information and network security, emergency response, and information fusion. Within each of these areas, a reasonably broad agenda is appropriate, as none of them can be characterized by the presence of a single impediment whose removal would allow everything else to fall into place. Advances in these areas may prevent some attacks on the IT infrastructure from succeeding. In the event an attack does occur, whether against the IT infrastructure alone or against some physical part of the nation, IT may help to rapidly and accurately identify its nature, reduce its effectiveness, aid in responding to it, and enable a quicker and fuller recovery. Indeed, even if the IT infrastructure is not deliberately attacked, significant damage to it may be a consequence of an attack directed elsewhere, and in any event any significant attack will result in extraordinary demands for emergency communications being placed on it. A stronger IT infrastructure would be beneficial in any case.

A point that deserves emphasis is the broad utility of the research agenda described above. Progress in these areas has applications not only for counterterrorism efforts but also for a wide range of other important national endeavors such as responding to natural disasters and decreasing cybercrime.

Most of these research areas are not new. Efforts have long been under way in information and network security and information fusion, though additional research is needed because the resulting technologies are not sufficiently robust or effective, they degrade performance or functionality too severely, or they are too hard to use or too expensive to deploy. Information technologies for emergency response have not received a great deal of attention, though efforts in other contexts (e.g., military operations) are intimately related to progress in this area.[69]

The time scale on which the fruits of efforts in these areas will become available ranges from short to long. That is, each of these areas has technologies that can be beneficially deployed on a relatively short time scale (e.g., in a few years). Each area also has other prospects for research and deployment on a much longer time scale (e.g., a decade or more) that will require the development of entirely new technologies and capabilities.

What drives the designation of these research areas as high priority?

- Information and network security is critical because of the potentially

[69]Military communications and civilian emergency-response communications have similarities and differences. Military forces and civilian agencies share the need to deploy emergency capacity rapidly, to interoperate, and to operate in a chaotic environment. While military communications must typically work in a jamming environment or one in which there is a low probability of intercept, these conditions do not obtain for civilian emergency-response communications. Also, military forces often must communicate in territory without a preexisting friendly infrastructure, while civilian agencies can potentially take advantage of such an infrastructure.

amplifying effect of attacks on IT when combined with attacks on the physical infrastructure, given the nation's increasing dependence (though much of it is avoidable) on information technology.

- IT for emergency response is essential because of the unfortunate reality that the probability of catastrophic terrorism cannot be reduced to zero; the ability to respond quickly and effectively to a catastrophic situation will always be needed.
- Information fusion is important in today's counterterrorism efforts, where the essential problem is how to identify potential threats amidst enormous amounts of possibly relevant information; sophisticated techniques for filtering and processing this information are needed.

Unlike some other sectors of national importance, the IT sector is one over which the federal government has little leverage. IT sales to the government are a small fraction of the IT sector's overall revenue, and IT vendors have little incentive to include security features at the behest of government alone. Moreover, there is essentially no history of government regulation of IT products and services, in contrast, say, to the traditional oversight of the electric-power industry. Indeed, we can expect that attempts at such regulation will be fought vigorously, or may fail, because of the likely inability of a regulatory process to keep pace with rapid changes in technology.

Under these circumstances, it seems most desirable to engage the private sector constructively and to emphasize market solutions. For example, IT vendors probably *will* respond if the private sector demands more security in IT products; if so, security may become a competitive advantage for various IT vendors, much as additional functionality and faster performance are today. At the same time, government may have a role in changing market dynamics in such a way that the private sector does pay more attention to security-related issues.

A second critical dimension of influencing security-related change is the federal government's nonregulatory role, particularly in its undertaking of research and development of the sorts described above.[70] Such R&D might improve security and interoperability, for example, and reduce the costs of implementing such features—thereby making it less painful for vendors to adopt them.

It is not clear which government agency, or agencies, would best be suited to support the above agenda. However, the more important policy issue at present is that the organization of that federal research infrastructure have the attributes itemized below. It would:

---

[70]Another potentially important aspect of the government's nonregulatory role, outside the scope of this report, is the leadership role it could play itself with respect to information and network security. For more discussion, see CSTB (2002a).

- Engage and support multidisciplinary, problem-oriented research that is useful both to civilian and military users.
- Have a research program driven by a deep understanding of vulnerabilities. This will likely require access to classified information, even though most of the research will be unclassified.
- Support a substantial effort in research areas with a long time horizon for payoff. Historically, such investigations have been housed most often in academia, which can conduct research with fewer bottom-line-driven pressures for immediate delivery. This is not to say that private industry has no role. Indeed, because the involvement of industry is critical for deployment, and also is likely to be essential for developing prototypes and mounting field demonstrations, support of both academia and industry (perhaps even jointly) in developmental efforts is highly appropriate.
- Provide support extending for time scales that are long enough to make meaningful progress on hard problems (perhaps 5-year project durations) and in sufficient amounts that reasonably realistic operating environments for the technology could be constructed (perhaps $2 million to $5 million per year per site for system-oriented research programs).
- Invest some small fraction of its budget on thinking "outside the box" in consideration (and possible creation) of alternative futures.
- Be more tolerant of research directions that appear not to promise immediate applicability. Research programs, especially in IT, are often—even generally—more "messy" than research managers would like. The desire to terminate unproductive lines of inquiry is understandable, and sometimes entirely necessary, in a constrained budget environment. On the other hand, it is frequently very hard to distinguish between (A) a line of inquiry that will never be productive and (B) one that may take some time and determined effort to be productive. While an intellectually robust research program must be expected to go down some blind alleys occasionally, the current political environment punishes such blind alleys as being of Type A, with little apparent regard for the possibility that they might be Type B.
- Be overseen by a board or other entity with sufficient stature to attract top talent, provide useful feedback, and be an effective sounding board for that talent.
- Pay attention to the human resources needed to sustain the counterterrorism information technology research agenda. This need is especially apparent in the fields of information and network security and emergency communications. Only a very small fraction of the nation's graduating doctoral students in information technology specialize in either of these fields, only a very few professors conduct research in these areas, and only a very few universities support research programs in these fields.

One additional attribute of this R&D infrastructure would be desirable,

though it is not clear how it might be achieved.[71] The success of the nation's R&D enterprise in information technology (as well as in other fields) rests in no small part on the ability of researchers to learn from each other in a relatively free and open intellectual environment. Constraining the openness of that environment (e.g., by requiring that research be classified or forbidding certain research from being undertaken) would have obvious negative consequences for researchers and the creation of new knowledge. On the other hand, keeping a counterterrorist agenda in mind, the free and open dissemination of information has potential costs as well, because terrorists may obtain information that they can use against us. Historically, these competing interests have been balanced—with more of one in exchange for less of the other. But the committee believes (or at least hopes) that there are other ways of reconciling the undeniable tension, and calls for some thought to be given to a solution to this dilemma that does not demand such a trade-off. If such a solution can be found, it should be a design characteristic of the R&D infrastructure.

Finally, successfully addressing the privacy and confidentiality issues that arise in counterterrorism efforts will be critical for the deployment of many information technologies. These issues are serious enough to merit their own research efforts, though not at the scale and intensity that the other areas might warrant.

REFERENCES

Brooks, Frederick P. 1975. *The Mythical Man-Month*. Addison-Wesley, Boston, Mass.

Christen, Hank, et al. 2001. "An Overview of Incident Management," *Perspectives on Preparedness*, No. 4, September. Available online at <http:ksgnotes1.harvard.edu/BCSIA/Library.nsf/pubs/POP4>.

Computer Science and Telecommunications Board, National Research Council. 1990. *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, Washington, D.C.

Computer Science and Telecommunications Board, National Research Council. 1996. *Computing and Communications in the Extreme: Research for Crisis Management and Other Applications*, National Academy Press, Washington, D.C.

Computer Science and Telecommunications Board, National Research Council. 1997. *The Evolution of Untethered Communications*, National Academy Press, Washington, D.C.

Computer Science and Telecommunications Board, National Research Council. 1999a. *Information Technology Research for Crisis Management*, National Academy Press, Washington, D.C.

Computer Science and Telecommunications Board, National Research Council. 1999b. *Trust in Cyberspace*, National Academy Press, Washington, D.C.

Computer Science and Telecommunications Board, National Research Council. 1999c. *Realizing the Potential of C4I: Fundamental Challenges*, National Academy Press, Washington, D.C.

[71]A Computer Science and Telecommunications Board study in progress on improving cybersecurity research in the United States will address this question.

Computer Science and Telecommunications Board, National Research Council. 2001a. *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers*, National Academy Press, Washington, D.C.

Computer Science and Telecommunications Board, National Research Council. 2001b. *The Internet's Coming of Age*, National Academy Press, Washington, D.C.

Computer Science and Telecommunications Board, National Research Council. 2002a. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later,* National Academy Press, Washington, D.C.

Computer Science and Telecommunications Board, National Research Council. 2002b. *IDs—Not That Easy: Questions About Nationwide Identity Systems,* National Academy Press, Washington, D.C.

Computer Science and Telecommunications Board, National Research Council. 2002. *Intersections Between Geospatial Information and Information Technology*, National Academy Press, Washington, D.C., in preparation.

Convergence Working Group. 2002. *Report on the Impact of Network Convergence on NS/EP Telecommunications: Findings and Recommendations*, February.

Disabatino, Jennifer. 2001. "Court Order Shuts Down Dept. of Interior Web Sites," *Computerworld*, December 17.

Hightower, J., and G. Boriello. 2001. "Location Systems for Ubiquitous Computing," *IEEE Computer,* Vol. 33, No. 8, August.

National Institute of Standards and Technology. 2002. "The Economic Impact of Role-Based Access Controls," March.

U.S. House of Representatives, Committee on Science. 2001. "Boehlert Gives Cyber Security Address at ITAA Forum," press release, December 12.

6

Energy Systems

INTRODUCTION

Our economy and quality of life require a plentiful and continuous supply of energy. Though energy per se accounts for less than 10 percent of our gross national product, much of the balance of the economy will not function without it. Commerce, manufacturing, and employment are all highly dependent on natural gas, refined oil products, and electricity. Health care, schools, and universities are dependent on electricity and, frequently, natural gas. Telecommunications and information technology require a high-quality and reliable electrical power supply. Transportation is most dependent on oil products but also has great need for electricity to manufacture the vehicles and operate airports, traffic management systems, rail transit systems, and terminals. Because our reliance on energy is so great, our vulnerability to an interruption in its supply also is great.

Included among U.S. energy systems are extensive networks of electric generating facilities and transmission lines, natural gas pipelines, oil refineries and pipelines, and coal mines and transport. These systems, and their operators' emergency-response plans, have been tested by natural disasters such as floods and earthquakes; in general, the affected industries have returned disrupted systems to operation relatively quickly. Sabotage of individual components has also posed a nuisance, but the impacts have generally been manageable. However, the industry's response capabilities were not designed to handle extensive, well-organized acts of terrorism aimed at key elements of the energy system.

The oil, natural gas, and electrical systems have several broad characteristics in common. Transport can extend over thousands of miles, often through remote

and unprotected lands. The systems are frequently controlled remotely, relying on supervisory control and data acquisition (SCADA) systems. Each system also has certain unique characteristics. Electricity cannot be stored for use when needed, whereas oil and natural gas products can be stored in limited quantities near points of use (thus lessening the impact of a shortage if the supply is interrupted). Also, oil products can be imported from overseas and transported by a variety of modes. Another important difference is that the refineries for converting crude oil into its large family of products are generally very large and complex facilities, located in just a few areas of the country, while the electric generating facilities come in a great range of sizes and are widely distributed throughout the nation. While some oil and gas operations generate their own power, most are highly dependent on electricity for their operations. In turn, about one-fifth of all electric power is generated from natural gas and oil products.

Analysis of possible targets, weapons, and delivery systems and of direct and indirect consequences reveals several very dangerous scenarios. The scenarios of greatest concern involve the electrical system. When service is lost, there are immediate consequences to every person, home, and business. An extended outage of electricity would have profound consequences.

Natural gas supply is also vulnerable, but the use of gas is not as universal as that of electricity. The oil sector has several vulnerable points, but, as noted above, it has backup alternatives. Coal is the least vulnerable and will not be considered in this analysis.

Several recent trends in the energy industries have increased the vulnerability of their infrastructures and made serious loss of service from terrorist attack more likely. To improve efficiency of operations, there has been a rapid increase in the use of automation and computerization; therefore each industry now relies heavily on information management and telecommunications systems. Low margins and various competitive priorities have encouraged industry consolidation, with fewer and bigger facilities and intensive use of assets in place. With no new refineries having been constructed since 1978, average refinery operation is at 93 percent of capacity (EIA, 2001). Control is more centralized, spare parts inventories have been reduced, and subsystems are highly integrated across the entire business. Few or no personnel at key facilities (i.e., electric substations and pipeline pumping stations), congested transmission corridors, and increased reliance on unsecured telecommunications and SCADA systems are common. (SCADA systems are also discussed in Chapter 5.)

This economic and competitive setting has led to reduced investment in system capacity and technology development. For example, annual additions to electrical transmission capacity declined 60 percent in the 5-year period 1990-1995, as compared with 1985-1990. The result is increased reliance on technology developed by vendors and increased outsourcing of key functions such as maintenance and security.

The electricity sector also is changing fundamentally as it incorporates more

competition and deregulation into what had been a highly regulated system. Independent power producers are gaining market share, but they support essentially no research and development and have little corporate infrastructure for issues such as security. Significant restructuring of the equipment-supply industry has occurred as well, with manufacture of some key components moving abroad. Unlike generation, the transmission portion is not being deregulated. This situation is straining the electric system because the priorities and practices of generating companies, transmission entities, and customers differ.

All these trends have led to systems that are highly efficient, productive, and cost-effective, but also subject to increased stress even without the threat of terrorism. Controls, cost competition, and regulatory uncertainty could each, in one way or another, limit the willingness of companies to invest in security upgrades that might seem desirable from a societal point of view.

It is readily apparent that any prolonged interruption of the supply of basic energy—be it electricity, natural gas, or oil products—would be a devastating blow to the nation and its people. This chapter addresses these systems' vulnerabilities and identifies current means of addressing them, which should be implemented as rapidly as feasible. The chapter then describes key areas for R&D on materials, tools, systems, and methods. These R&D programs should be initiated immediately, and the resulting technologies should also be implemented as rapidly as feasible, although in some cases this could take up to 10 years. Overall, the recommendations in this chapter stress the importance of expediting implementation of technologies to reduce vulnerability due to the urgency of protecting this infrastructure. *The most critical recommendations are numbers 6.9, 6.10, 6.11, 6.15, 6.16, and 6.17 below.*

More fundamental changes, which might reduce vulnerability still further, are of course possible. Electricity generation might become more decentralized, reducing the impact of the loss of key components. The use of renewable energy resources (e.g., wind and photovoltaics) would complement this trend. The use of energy—oil in particular—could become more efficient, reducing the need for imports and, to some extent, vulnerability to upheavals in the Middle East. The use of alternative fuels derived from renewable energy or coal might grow, reducing dependence on the most vulnerable components of the energy systems. However, all these possibilities also have drawbacks, such as poor economics, unreliability, or remoteness. Furthermore, the U.S. energy systems are massive, and major changes can take decades, even after the technologies are developed. While it is worthwhile pursuing these research options and encouraging a diversity of supply, they will make little or no difference in reducing vulnerability to terrorism over the time frame of this study.

Although the threat of terrorism to our homeland places new requirements on energy infrastructures, the industry can draw on experience elsewhere. Because the national security and defense communities of this country have lived with such requirements for decades, a key element of our strategy must be to

accelerate communication and cooperation between members of those communities and the owners of energy infrastructures, including transfer of technology as appropriate.

ELECTRIC POWER

Introduction

The impact of a prolonged interruption in the electric power supply to any region of the country would be much larger than the economic loss to the energy sector alone. With the introduction of digital technology throughout our society, the cost of outages (e.g., from equipment failure or weather-related incidents) has significantly increased—from $30 billion in 1995 to $119 billion in 2001 (Clemmensen, 1993; EPRI, 2001). The nation's electric power systems must clearly be made more resilient to terrorist attack.

The electric power system consists of four major components: generation plants, transmission lines and substations, distribution lines and substations, and system operations (the last mentioned may be located within a utility's service area or may serve a larger set of service territories). Most generation plants consist of fuel supply facilities, generators, turbines, heat exchangers, cooling systems, control systems, and substations that connect to the transmission network. There are about 10,400 generating stations, with a total installed capacity of 786 gigawatts (GW), in the United States (EIA, 2001). Utilities own 82 percent of this generating capacity and independent power producers, the rest. Coal-fired units accounted for about 51 percent of the power generated, with nuclear at 20 percent, oil and gas at 18 percent, and hydropower and other renewable sources at 11 percent. The transmission system includes high-voltage lines, towers, and underground cables, as well as transformers, breakers, relays, and associated control equipment, which is mostly in substations. The distribution system includes the lower-voltage distribution lines and cables, substations, and control equipment. System operations include monitoring, control, and communications equipment.

Utilities have a century of experience to draw upon, and today they make use of ever more sophisticated technology to achieve high reliability and quality of service. However, September 11 has raised additional concerns about the vulnerabilities of these highly integrated systems and the consequences to the people and economy in the event of a terrorist attack.

Representative Vulnerabilities

Two types of terrorist threats are of concern for the electric power system: physical attacks and cyber- and electromagnetic attacks. An isolated assault of either kind on an individual generating station, substation, or control center could

cause a serious but only local disruption. By contrast, a coordinated attack on a selected set of key points in the system could result in a long-term, multistate blackout. While power might be restored in parts of the region within a matter of days or weeks, acute shortages could mandate rolling blackouts for as long as several years. A highly stressed system (e.g., if power imports are high and transmission reserve capacity is low at the time of the attack) would be more vulnerable to cascading failures and the resulting longer-term blackout.[1]

Targets might include equipment used in the production or transmission of electricity and electronic components used to monitor and control the production, transmission, and flow of electricity, which for the purposes of this chapter are labeled "controls."

Much of the equipment under consideration is so large that it must be located outdoors, where it is vulnerable to weapons ranging from rifles to laser-guided missiles. Equipment operating at elevated temperatures could also be targeted with heat-seeking missiles. In addition, many of these facilities are vulnerable to military or even homemade bombs. Transmission towers and cables are located in a variety of settings, few of which are fenced or otherwise protected, and thousands of miles of these lines pass through remote sections of the nation. Thus they could be easily approached for attack, with little likelihood that the activity would be observed. Power lines and substations also are vulnerable to chaff, conducting strands draped over lines or equipment to cause short circuits.

The "controls" are mostly located in control rooms at generating facilities, substations, and system-operation centers. These sites generally are fenced off, but they are not hardened—excepting nuclear plant control rooms and a few system control centers. Most facilities are staffed continuously, but there has been a trend in recent years to reduce personnel at substations in favor of automated equipment under remote supervisory control. At each node in the controlled system, monitoring equipment, sensors, and methods of transmitting the data and control signals are colocated with the equipment being controlled or monitored, increasing vulnerability. Physically, these components can be attacked with weapons similar to those mentioned above, with the possible exception of heat-seeking devices.

---

[1]No widespread, long-term blackouts have occurred in an industrialized country since World War II. The worst recent incident was in Auckland, New Zealand, in 1998, with an estimated cost of U.S.$56 million (McIntyre, 1998). All four main transmission lines to the central business district failed, leaving the center of the city largely without power for about 2 months. Many businesses failed, among other negative outcomes. People were able to compensate to some degree with portable generators that could be refueled from outside the city. Because some of the scenarios envisioned here would not include that option, they could result in considerably more serious consequences.

Control components are also vulnerable to cyber or electromagnetic attack. Cyberattacks would involve intrusion into the control systems via the Internet or the affected utilities' private networks; many of these networks include modem access, which adds significantly to their vulnerability. Electromagnetic pulse (EMP) attack would involve the introduction of radio-frequency or microwave impulses into the circuitry of the control systems, upsetting their electronics and leading to network destabilization and outage. Such outages could be serious, but they are unlikely to require the replacement of much equipment.

The most insidious and economically harmful attack would be one that exploits the vulnerabilities of an integrated electric power grid. "A chain is only as strong as its weakest link" applies here. Simultaneous attacks on a few critical components of the grid could result in a widespread and extended blackout. Conceivably, they could also cause the grid to collapse, with cascading failures in equipment far from the attacks, leading to an even larger, longer-term blackout. In either case, the failure would be caused by the system's inability to recover from a multipoint, or "*n* minus *k*," attack (on *k* points of a network that has a total of *n* nodes). A single "*n* minus 1" failure event (or even an "*n* minus 2" event, under certain circumstances) probably could be handled by current contingency plans, which utilities have used for decades in reacting to natural disasters or major equipment failures. Recognition of an attack in progress, and initiation of a system-level response to minimize the harm being done, must occur within a very short time frame—even just a few seconds. However, distinguishing between a routine failure and the start of a series of planned attacks is a very difficult challenge.

The duration of a terrorist-caused blackout or curtailment would depend on the extent of the failure and the availability of replacement components and skilled personnel to make the repairs. Certain components of the electrical system are of particular concern because few spares are available nationally, and new replacements could take several years to procure. The shortage could be alleviated in part by activating available ties to adjacent systems and utilizing local generating units, but rolling blackouts (as distasteful and economically damaging as these are) could be needed.

Attacks on nuclear power plants could have special consequences for the nation's electric systems. The outage of a single nuclear station would have an impact similar to the outage of any other large generation site. However, the uniqueness of nuclear power, both from a public and regulatory perspective, could result in a much wider impact. Under those circumstances, the U.S. Nuclear Regulatory Commission (USNRC) might require all operating nuclear units to shut down until their safety could be assessed by the USNRC and/or additional security measures could be carried out. In either case, the sudden removal of that capacity—about 20 percent of the nation's generating pool—would put a severe strain on the rest of the system. For some regions of the nation, the generating

capacity loss could approach 40 per cent of the currently available generating capacity.

Implementation of Existing Technology

Redirecting and Prioritizing Security Attention

This country's electric power systems have some attributes that may hinder the implementation of security-based improvements. By their very nature, the systems are geographically distributed, making them difficult to protect. Historically, analysis has focused on threats from natural disasters; security from malevolent attack has generally not been a high priority. With the exception of nuclear power plants, the main purpose of security at most electrical facilities has been to keep people out for their own safety, not to deter terrorists. Reserve capacity (the difference between installed capacity and the amount that's necessary to meet peak demand) has become small for generation, transmission, and distribution; highly stressed systems are less resilient in the face of upsets and take longer to recover. Deregulation has encouraged efficiency, invested-cost utilization, and return on investment rather than redundancy, reliability, and security. For the same reasons, power companies keep fewer spares on hand. Utilities have also reduced their support for research and development;[1] in particular, new protection schemes for countering cyberthreats seriously lag the rapidly advancing cyberweapons available. Another consideration is insider threats. These have been difficult to address because of workplace privacy and individual rights issues, which continue to inhibit the use of screening and profiling tools.

Recommendation 6.1: The federal government should review the current institutional and market settings to determine what, if anything, should be done to facilitate actions for improving the security and resilience of the country's electric power system.

Tools for Identifying System Vulnerabilities to Terrorist Attacks

For a utility or independent power producer, one of the most significant challenges will be to direct its often limited resources to protecting its most important elements. This prioritization must take into account possible threats, probability of threat, consequences of attack, and response capability. At the same time, because the U.S. transmission grids are largely integrated with the

[1]Presentation by Stephen Gell, director of strategic science and technology, Electric Power Research Institute, to the Committee on Science and Technology for Countering Terrorism, Panel on Energy Facilities, Cities, and Fixed Intrastructure, January 10, 2002.

Canadian and Mexican grids, those systems must likewise be analyzed and their hardening plans coordinated with those of the United States. The defense and national security communities in the country have developed tools for vulnerability analysis of physical sites and have used them extensively for over 20 years. Recently, there has been some success in transferring these tools to parts of the energy infrastructure. They should be made available to the rest of the electric power industry. By applying these analytical tools to all critical grid components, the systems approach to electric power security would identify key vulnerabilities in a facility and determine the relative value of possible security-upgrade options. These tools should include methods that help define appropriate use of (1) surveillance of critical sites and equipment, (2) hardening selected sites, (3) barriers to prevent intrusion, and (4) masking of selected equipment.

Recommendation 6.2: The electric power industry (as well as the oil and natural gas industries, discussed later in this chapter) should undertake near-term studies to identify vulnerabilities to physical attack on equipment and controls. These studies should include connected Canadian and Mexican assets. The tools for analysis of vulnerabilities used in the defense community should be transferred to the energy operators for these studies, along with adequate training in their application.

For the nation as a whole, the identification of vulnerabilities requires sophisticated models and simulations of the infrastructure. Because these efforts will require a great deal of information (most of it not easily available to any one individual player) on such issues as threats and interdependencies, some infrastructural segments have started establishing information sharing and analysis centers. This is largely an ad hoc phenomenon, which should be placed on an organized, rational basis. In so doing, sensitive data on equipment, its location, and its vulnerability will have to be examined and protected from those lacking a need to know, necessitating an information classification system. This issue is germane to the oil and natural gas sectors as well.

Recommendation 6.3: Action should be taken to facilitate information sharing between energy sector components. Specifically, the government needs to adjust its policies in order to allow a reasonable balance between the industry's access to information on vulnerabilities and threat scenarios, on the one hand, and the protection of such information to ensure national security, on the other. In addition, industry's concerns about antitrust and liability issues, as well as freedom-of-information (FOIA) risks, need to be addressed. Government support for energy sector information sharing and analysis centers is essential. Also, the security classification system for information must be reviewed, and modified accordingly, in light of the new terrorist threats.

Addressing System Vulnerabilities

After implementing the above, the next step should be for the industry to analyze the system's specific components, probably through the regional reliability planning councils. It would then be possible for the utilities, independent system operators (ISOs), and regional transmission operators (RTOs) to determine which components are most vulnerable from a system perspective.

Once determined, these components should be given the highest priority for hardening and protection, including enhanced surveillance and response, fortified barriers to intrusion (both by land and from the air), installation of bulletproof walls around equipment vulnerable to firearms, and, possibly, installation of redundant, geographically separated systems.

Industry also should examine how to expedite recovery from a widespread attack. This should include a review of current sparing philosophy for critical components. "Business as usual" is not likely to be an adequate approach. Increased redundancy also would be useful, such as with control systems, which could be decentralized and designed with duplicate backups to minimize the loss of control from an attack. Utilities and other operators also should plan for a "black start" following a large-scale blackout. Location of critical equipment to accomplish this might be aided by the use of simulation models, threat scenarios, and system models to deal with the multiplicity of challenges. This action may be augmented in the future by the development of an adaptive grid, as discussed below in Recommendation 6.16.

Recommendation 6.4: Utilities, independent system operators (ISOs), and regional transmission operators (RTOs) should identify the most critical equipment for protection in their respective domains. This protection, where it does not already exist, should then be accomplished with available technology, including (1) increased surveillance of critical sites and equipment, (2) hardening of selected sites, (3) installation of barriers to prevent motor-vehicle or rail intrusion, and (4) masking of thermal signatures of selected equipment. As part of this examination, policies for critical-equipment spare parts should be reviewed, including consideration of cooperative efforts for employing regionally based and coordinated spares centers.

The possibility of cascading damage from an attack on the transmission lines themselves could be reduced by developing and implementing new designs for conductors, towers, and transmission corridors. Although the industry has examined this problem for weather-related and other circumstances, what is now needed is a top-to-bottom review that assumes a deliberate and extensive attack.

Recommendation 6.5: An immediate review of electric transmission lines should be initiated, through the Federal Energy Regulatory Commission (FERC) and the regional reliability councils, to identify opportunities for

retrofit actions that would protect existing facilities from cascading damage after an attack.

Provision for Emergency Federal Policy to Facilitate Recovery from a Catastrophic Shutdown of Electric Power Facilities

Catastrophic terrorist attacks will not only disrupt the system, they will also require follow-up investigations that may necessitate treating parts of electric power facilities as crime scenes. Under these circumstances, business-as-usual regulations could prove a hindrance. Thus there is a need for government and industry to identify statutory authority for certain temporary measures.

Recommendation 6.6: Government, through the Office of Homeland Security, should identify statutory authority that will permit emergency actions to be taken and temporary changes in regulations to be adopted, after an attack, to reestablish service. To the extent feasible, the government and industry should collaborate in preplanning specific actions and changes in regulations, based on reasonably anticipated service disruptions. This capability, which applies to the natural gas and oil sectors as well, should be in place prior to a catastrophic disruption in the supply.

Paying for Security Improvements and Recovering Investments

All of these actions to improve security and the ability to recover from an attack will require investments in facilities and equipment. However, as noted, the environment created by deregulation has compelled utilities to control costs tightly. One consequence has been the reduction in reserve capacities, resulting in the greater utilization of equipment by routinely operating it closer to its capacity limits. The existing mechanisms for cost recovery—ranging from rate relief to competitive market forces—must be reviewed and appropriate incentives developed in order to encourage investments under these changed circumstances.

Recommendation 6.7: Both FERC and the state utility commissions (perhaps through the National Association of Regulatory Utility Commissioners) should allow certain counterterrorism costs—specifically, for actions taken to reduce the vulnerability of critical equipment within an electric utility's operation and to speed recovery following an attack—to be included in the rates that the utility can charge for its services. The federal government also should consider the use of incentives for investments made for security purposes in a competitive market environment.

Allowable actions could include simulation-model development and deployment, increasing surveillance, hardening of sites, retrofitting transmission lines against cascading failure, increasing operating margins, decentralizing control systems, and increasing the availability and numbers of critical equipment spares.

It is also recommended that a dialogue between private sector executives and government policy makers be initiated to define their respective roles in implementing security and response capabilities against terrorist attacks. This dialogue is also needed for defining federal and private sector roles in related R&D. Resolving the issues of who pays for security and system-hardening improvements, and how the accompanying investments are to be recovered, must be an early priority for leaders in all relevant sectors.

Recommendation 6.8: A clear and coordinated strategy should be developed and agreed upon by the federal government, the electric power industry, and the equipment suppliers. This strategy must include (1) the definitions of proper roles for each sector, (2) review of the current R&D programs of the three parties for relevance and added support, (3) coordination on the part of the federal government, through DOE, of relevant research and development being done in various other federal agencies, including the national laboratories, (4) coordination by industries of their R&D efforts through appropriate associations (e.g., the Electric Power Research Institute (EPRI) for the electric utilities), (5) involvement of the regulatory community, through the Federal Energy Regulatory Commission (FERC) and the National Association of Regulatory Utility Commissioners (NARUC), for appropriate rate-base considerations, and (6) government-developed incentives to expedite the early introduction of technology and equipment.

Defending Against Cyberattack

In addition to protecting equipment and facilities from physical attack, the potential for attack on control systems needs urgent attention. The manner in which data are transmitted between control points should be reviewed in order to improve security and reduce the potential for hacking or disruption. Encryption and other in-place defensive mechanisms need to be reviewed and upgraded where indicated. However, as discussed above (and below), the decision to commence security upgrades—whether by a power producer, a transmission provider, or another party—requires resolution of questions regarding who is to pay and how that investment is to be recovered. These issues are as relevant to the gas and oil sectors as they are to the electric power system.

Recommendation 6.9: The manner in which data are transmitted between control points and/or SCADA systems should be reviewed by their owners in order to improve security and reduce the potential for hacking or disruption. In addition, firewalls and procedures for detecting cyberintrusions should be reviewed in order to prevent or reduce the threat of cyberattack on control systems. Additionally, it is recommended that efforts under way for cybersecurity in other areas (such as the national laboratories) be translated into the energy systems environment. Finally, any such systems and devices should be reviewed by appropriate standards-setting groups and

vendors. Coordination should occur through DOE and the Office of Homeland Security.

Research and Development Priorities and Strategies

While much can be done with current technology, additional options are needed in physical protection; equipment redesign for inherent robustness; cybersystem protection and robust information technology (IT) architecture; system modeling for vulnerability analysis; and architecture and supporting technology for flexible, adaptive power systems for impact mitigation. The fraction-of-a-second response times of a power grid allow very little margin for countering the effects of an attack. Therefore, prevention of attacks should have a high priority. Technologies that support automated, split-second action may be difficult to develop but could be crucial in limiting the consequences of an attack. In addition, the costs of current technologies can be reduced through R&D, increasing their level of applicability.

Extra-High-Voltage (EHV) Transformers

The physical design of critical equipment should be modified—for robustness, hardening, blast mitigation, quick repair, and barriers to minimize direct assault (including from the air)—to reduce its physical vulnerability. For example, certain key technologies with identifiable heat signatures should be reviewed for masking those signatures, thereby deceiving terrorists' detection and targeting. The national security and defense communities in this country have developed, over the decades, many design philosophies for achieving reduced vulnerability. These ideas should be studied and aggressively adapted to the power grid.

One area of particular concern is the vulnerability of EHV transformers. These are critical components of the grid. The number of spares available in the nation is very limited, and replacements would require many months to manufacture and ship from foreign suppliers. Building on the general design philosophy of the U.S. Army for small, modular tanks for rapid overseas deployment, a possible solution might be the development of a modular, lightweight, universal EHV transformer for use in the instances envisioned here—namely, the rapid restoration of the ability to deliver power in the event of a widespread attack on a utility grid system.

Research should be undertaken to determine if such a modular universal EHV transformer might be developed. It would be smaller, cheaper, and more transportable than the large, custom-designed EHV transformers currently used in substations. Modular units might be used individually or in multiunit sets to replace EHV units that had suffered damage. Modular units would likely be less efficient and have a lower power rating, but they would be sufficiently affordable to be stockpiled at ISO or RTO sites and used as temporary equipment in the

event of a major loss. They would be analogous to the small spare tire supplied with some cars: vital in an emergency, but to be replaced as soon as possible. They might also be used on a short-term basis where load exceeded capacity; however, such use should be of short duration so as not to preclude their use for the purposes described here. Equipment suppliers must take the lead here, but funding support must come from the federal government (see subsection "New Electric Energy R&D Programs"). EPRI could provide the organizational framework to engage suppliers in precompetitive R&D.

Recommendation 6.10: Research should be undertaken jointly by DOE and the industry (represented by EPRI) to determine if a modular universal EHV transformer might be developed for application throughout the U.S. electric industry.

Advanced Intrusion Detection Systems

Most transmission systems cover many miles and are unattended. The present method of monitoring thousands of miles of rights-of-way—visual inspection, by truck or aircraft—is inadequate to defend the system against terrorism. Operators need new surveillance technologies that hold promise for frequent monitoring and highly reliable detection of unwanted activity. The best sources for these technologies would be the work on drone aircraft, satellite-surveillance technology, intelligent-software-based analysis, change-detection sensors, and intrusion-detection cables that is currently under way in various defense and intelligence agencies. These technologies would have to be adapted to energy systems, which should be done as a public-private partnership with cost sharing. The main obstacle probably would be information classification and "need to know." It would be best to coordinate such research with industry through EPRI. As noted in the discussion of the oil and gas sectors, this issue is relevant to all three energy sectors.

Recommendation 6.11: Surveillance technologies developed for defense and intelligence agencies should be investigated for their usefulness in defending against terrorist attacks on widely distributed oil, gas, and electric transmission assets. These technologies could include drone aircraft, satellite-surveillance technology, intelligent-software-based analysis of surveillance images to scan for unwanted activity, change-detection sensors, and intrusion-detection cables designed to sense unusual vibrations or noises. The Office of Homeland Security should be the coordinator of these efforts.

Structural Materials Enhancement

A key aspect of hardening existing facilities against physical attack is retrofitting structures to increase their resistance to blast shock and fire. Manufacturing, application, and implementation methods must be developed for upgrading

energy-sector facilities at reasonable cost. Materials specifically hardened against explosions and fire are being developed for other uses, and this work could be applied to the energy sector.

Recommendation 6.12: Research and development for hardening energy-system assets against blast shock and fire should be conducted by DOE. Areas of focus might include material coatings and surface-applied structural enhancements.

Cyberthreats

Advanced hardware and software to protect SCADA systems, plant control systems, and overall system controls are needed. Included in this category would be intelligent-agent-based networks to monitor and respond to cyber threats, better encryption methodology, and real-time barriers to intrusion through better architecture and firewalls. This technology development crosscuts many infrastructure areas. R&D currently under way or soon to be initiated, both in federal government and private sector programs, should be applied to the electric power system, supplemented by R&D directed by EPRI (see Recommendation 6.9).

A cyberattack from within, brought about by a disgruntled employee or a terrorist plant, could be particularly damaging. R&D is needed on ways to detect and counter this threat for critical components.

Recommendation 6.13: The technologies discussed in Recommendation 6.9 should be further developed for maximum utility in the electric sector. In addition, to counter internal cyber threats, smart controls should be developed and deployed that limit the manipulation of the system outside normal operating settings—perhaps utilizing artificial intelligence or redundant controls.

Electromagnetic Pulse

EMP has long been a consideration for regional vulnerability under nuclear attack scenarios. Relatively simple devices can produce the same effect on a much smaller and more local scale. To counter such threats, lower-cost electronic shielding needs to be developed and employed to protect critical components.

Defensive Systems

Protecting facilities and systems deemed to be most critical from air attacks is a significant challenge. Facility hardening may not be feasible using conventional approaches, and more sophisticated methods, such as underground siting, could be prohibitively expensive, even for new facilities. The selective use of

active systems—i.e., weapons—needs to be investigated. Such weapons might include surface-to-air missiles in combination with doubly redundant safeguards against unintended launch, as well as nonlethal systems such as directed-energy weapons and energetic-particle shields. Defensive structures, such as structures that would disrupt an incoming aircraft, should also be investigated. These efforts should include model development validated by subscale and full-scale tests. Such innovations in defense may provide cost-effective solutions when combined with traditional security and hardening. These issues also pertain to the oil and gas sectors, as noted later.

Recommendation 6.14: Defensive systems, for use at the most critical assets of the energy infrastructure, should be studied and developed. Such systems would be used in combination with traditional security and hardening methods. In addition, the deployment of weapons, lethal and nonlethal, should be reviewed.

Simulation Models for Analysis and Management

Models can help solve some of the problems of protecting electric power systems from terrorist threats. Regional models of the power grid—such as the Texas grid model for the Houston area, which has been used for analysis of outages—must be expanded and interdependency modeling accelerated (Patton et al., 1999). In that spirit, a federally funded center for interdependency modeling has recently been established (the National Infrastructure Simulation and Analysis Center). Because coordination, perhaps through EPRI, will be essential to obtain data from the power industry, this is a clear opportunity for a federal-private partnership. Also, the sophisticated level of the needed modeling will require state-of-the-art computational tools available at DOE's national laboratories. Protection of the resulting information on the vulnerability of key nodes in the electric power system will demand the highest level of security classification.

Recommendation 6.15: Improved simulation-design tools for modeling the prevention, response, and recovery of energy systems and for analyzing a variety of terrorist-threat scenarios should be developed, under DOE leadership, at the national laboratories. These models would have the following functions: (1) help planners, from the perspective of regional and nationwide system protection, to identify assets for vulnerability assessment; (2) model regional and national power-grid interdependencies to more accurately evaluate each component and node of the infrastructure; (3) determine the most vulnerable sites in the system; (4) test and validate proposed mechanisms to prevent cascading and broad-area effects; and (5) analyze the vulnerabilities of interdependent infrastructures (e.g., the effects of electric power outages on the water supply system).

Intelligent, Adaptive Power Grid

Under normal conditions, the electric power grid is controlled to balance changes in demand with changes in generation. In the event of a broad-based terrorist attack on multiple nodes, controls would be unable to reachieve balance. The result could be outage of an entire grid, with the possible cascading of such effects into other regional grids. Innovation to create a more flexible grid structure is clearly needed.

Recommendation 6.16: Technology should be developed for an intelligent, adaptive power grid that combines a threat-warning system with a distributed-intelligent-agent system. This grid would be able to rapidly respond with graceful system failure and rapid power recovery. It would make use of adaptive islanding—a concept employing fast-acting sensors and controls to "island" parts of the grid as the rest comes down—and technologies such as storage units positioned at key points to minimize damage during shutdown. The system would need to be able to differentiate between a single component failure and the kind of concurrent or closely coupled serial failures at several key nodes that would indicate the onset of a concerted attack.

The trend over time has been to large, remote generating plants, which require large, complex transmission systems. Today there is a growing interest in distributed generation—generators of more modest size in close proximity to load centers. This trend may lead to a more flexible grid in which islanding to maintain key loads is easier to achieve. Improved security from distributed generation should be credited when planning the future of the grid.

Change in the electric power infrastructure will, of necessity, be evolutionary, not revolutionary. As such, implementing new technology for intelligent, adaptive power grids will take time and resources. Recovery of the invested funds through rate mechanisms or in some part through homeland security funding must be examined. Change will also require adjustments in the philosophy of operation of the whole electric-power-grid structure. Thus, industry organizations such as EPRI will need to play a major role (see Recommendation 6.8).

It is clear that we cannot totally prevent a terrorist attack on electric power systems; the question is what can be done to mitigate the effects of such an attack. This intelligent adaptive grid is a new approach and one that could provide resiliency to the grid in a new manner. It entails long-term R&D and will require new technology, some of which is made possible by advances in microelectronics and controls technology.

There is some work under way at EPRI with DOD cosponsorship, on an intelligent, self-healing grid. Since sensors and control systems are integral parts of this concept, the DOE national laboratories must be key participants in the effort. The work spans the range from research through development, so it is appropriate that the funding be shared among government (DOE and DOD), industry (through EPRI), and equipment vendors.

Deployment would be the responsibility of the utilities and ISOs. Vendors will receive the technology transferred from the national labs and EPRI and will in turn commercialize it. The mechanism for development and deployment is well-established, public–private partnerships and transfer of technology from federal investment. Incentives for initial deployment will require support and incentives from FERC and state regulators.

Existing Electric Energy Research and Development Programs

Research and development are mainly supported through three sets of sponsors:

1. The Department of Energy program includes technology development in superconductivity, energy storage, grid reliability, analytical tools, advanced power generation, environmental controls, energy management, and combustion research. If fully developed and implemented, some of these technologies—such as distributed generators based on fuel cells or microturbines—could play a role in making energy systems more resilient in the face of terrorist attacks. Although DOE responded quickly to the recommendations of the Presidential Commission on Critical Infrastructure Protection—it recently established the National Infrastructure Simulation and Analysis Center, as noted above—infrastructure per se has not received a high level of budgetary support. DOE also sponsors technology development in physical-security technology to protect its own facilities, as well as those of DOD and the Department of State.
2. The utilities have long funded a high-quality and valuable R&D program through a cooperative effort led by EPRI, some of which has been concerned with infrastructure. However, it must be noted that investment for this effort has dropped, at least in part because of deregulation.
3. Manufacturers of equipment such as transformers, high-voltage components, and control systems fund technology development internally. However, such efforts are mainly focused on incremental improvements, especially in advanced generation technologies.

These R&D programs should be reviewed for their relevance to improving the security of the electrical supply and transmission systems. Those that meet the standard should then be accelerated, through appropriate funding and assignment of technical resources, and challenged with negotiated deadlines for delivery of results. This may require additional federal funding support.

New Electric Energy R&D Programs

As noted above, the electric utility industry, under historical regulation, had a mechanism at EPRI for carrying out R&D. This mechanism allowed R&D to

be performed in a noncompetitive environment and involved DOE in efforts focused on the longer term; the equipment manufacturers contributed to this collaboration as well. In this way, three entities worked together on bigger efforts than any one of them could do alone.

A similar approach is needed for the counterterrorism R&D agenda. It is clear that for equipment-related research (on inherently hardened equipment and modular transformers, for example), the suppliers must play a fundamental role. But it would be difficult for them to shoulder the entire cost, and in any case significant innovation needs a broader involvement from the nation's science and technology communities. Financial support, principally from government—directly from DOE and via rate adjustments from FERC and the various state commissions—will be needed. Tax breaks and risk financing for the installation of new security-related equipment should also be considered.

Research and development to achieve an intelligent, adaptive power grid will require the participation of experts in fields such as microelectronic systems, sensors, distributed intelligence, and communication. The research already under way in these areas for military applications should be brought to bear on counterterrorism as well. A public–private partnership is recommended, with the industry's involvement coordinated by EPRI and the federal research organized, managed, and leveraged from defense work, where indicated, through DOE (see Recommendation 6.8). R&D on enhancements to structural materials is a cross-cutting issue for many infrastructures. It should draw on appropriate expertise in the universities and research laboratories, with industry-unique R&D managed by EPRI.

Defensive systems research should draw extensively on the work of the defense and national security R&D communities. Weapon systems development should remain a DOD-led activity, with industry interface managed through the regulatory agencies and appropriate industry associations.

A great deal of work on cyberthreats is under way in the private sector as well as at the federal level. These efforts should be adapted to the particular needs of the electric utility industry, both in communications systems and SCADA systems. Interfaces with equipment control systems must of course involve the equipment suppliers, with support from the government and the industry through EPRI.

The areas of simulation tools, vulnerability analysis, and model development will require the best intellectual resources of the industry, the cooperation of regulators, and the involvement of the federal government as a source of funding as well as of technical input, primarily through the national labs. EPRI should serve as coordinator.

Unfortunately, DOE's programs on electric power systems have virtually disappeared in recent years. But in 1999 and 2000, the Department undertook portfolio analyses, and electricity infrastructure was identified as a critical research need, as it is in this chapter. Such programs should therefore be revived,

with particular focus on the hardware and software goals described above and on coordinating the larger studies of national importance—for example, those involving simulation and grid structure. The importance of this work underscores the need for these programs to be managed at the level of the Undersecretary of Energy.

Summary

R&D on the electric power infrastructure, including not only generation but also control systems, communications, and sensors, has not received the attention it deserves in order to meet the sorts of threats listed here. While industry (both manufacturers and utilities) can be called upon to help correct this omission, significant improvements will occur only if the U.S. government takes a leading role.

In the face of a restructured and highly competitive electricity marketplace, government determines the right set of policies and incentives for electric systems to become more resilient and capable of withstanding coordinated attacks. It is not clear, however, just what incentives would attract private investment for building redundancy, toughness, reliability, and the capacity to recover quickly from an attack. While it *is* clear that some of the current R&D and investment in new equipment and systems will have a beneficial effect on counterterrorrism goals, additional measures will be required.

For example, would an approach similar to the Strategic Petroleum Reserve be feasible? That is, could a "strategic electricity reserve" be constructed that would include critical equipment spares placed near important urban centers of the country? How might public–private partnering—bringing to bear the full capabilities of the industry, its suppliers, and the federal government, including efforts under way at the national laboratories—enter into this concept as well as into fulfilling the longer-term R&D needs? How, for instance, might increased reserve generation capacity be provided? Such questions must be throughly addressed if we are to adequately protect the nation's electric power system, its economy, and the well-being of its people.

Recommendation 6.17: A coordinating council should be formed to ensure that the necessary research on electric power systems is carried out, that the resulting technologies have a route to market, that implementation is done expeditiously, and that the costs are recovered through appropriate incentives, fees, rate adjustments, or other funding mechanisms. The council should include, but not be limited to, representation from the North American Electric Reliability Council, DOE, the Office of Homeland Security, NARUC, EPRI and other utility industry groups, manufacturers, and ISOs and RTOs.

OIL AND NATURAL GAS

Introduction

Oil and natural gas are essential energy sources for our economy. Oil products provide 97 percent of the energy used in the transportation sector. Natural gas provides over 25 percent of residential and industrial energy needs (not including the electricity generated from it). Together, these fuels account for almost 62 percent of all energy used in the United States (EIA, 2001). A significant disruption to either of these basic sources—that is, one that lasted for more than a few days—would have serious consequences for the U.S. economy and the health and well-being of the population (NPC, 2001; Badolato, 2002). Because of the importance of oil and gas to the nation and the large number of companies and vendors in the industry, it is important that the industry and government jointly establish a security standard consistent with a post-9/11 world.

The oil products supply system includes 161 oil refineries. The natural gas system includes 726 gas-processing plants. Extensive but separate pipeline networks provide for transport: 1,280,000 miles of gathering, transmission, and distribution lines for natural gas and 220,000 miles of crude oil and oil products lines. Attacks on the natural gas system are more likely to have catastrophic consequences, but oil has its weak points also.

The vulnerability of each of these systems is discussed first. Many of the current implementation issues and longer-term R&D needs are similar for the two systems, so they are treated together. Several of the recommendations in the electric power discussion have equal applicability to oil and gas. These are numbers 6.2, 6.3, 6.6, 6.9, 6.11, 6.12, and 6.15.

Natural Gas Systems

The U.S. natural gas infrastructure, together with the portion of the Canadian system that serves the United States, is very large. The U.S. system alone consists of over 276,000 gas wells, some of them in locations as much as 100 miles offshore, 45,000 miles of gathering pipeline, 410 underground storage fields, 54 complete liquefied natural gas (LNG) facilities, 254,000 miles of transmission pipelines, and 980,000 miles of local-distribution pipelines (NPC, 2001). This vast network, privately owned and operated, was built to meet market demand and was designed for maintainability, with safety as a constant requirement. Vandalism was taken into consideration, but the facilities were not designed and built to withstand terrorist attack.

Several components of the natural gas infrastructure could be considered attractive targets for terrorists (see Figure 6.1):

- Transmission pipelines, including those from offshore collecting sites;

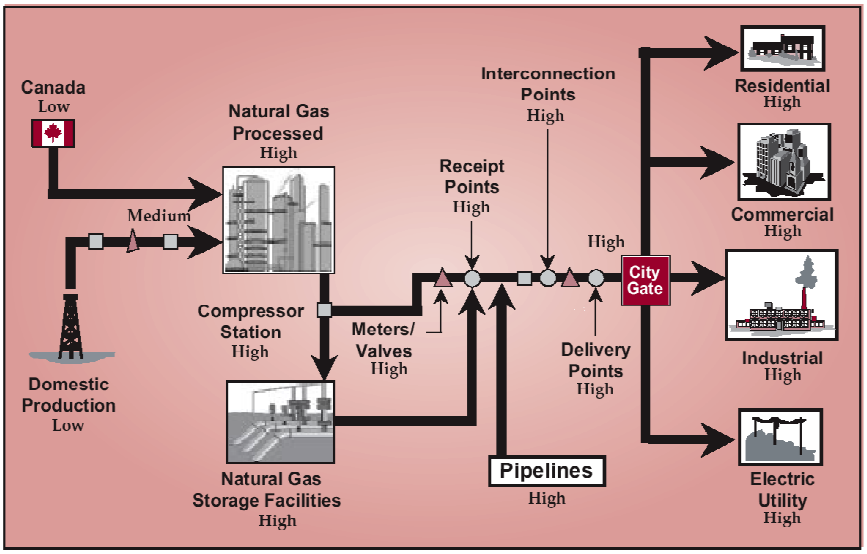

FIGURE 6.1 Physical vulnerabilities of the natural gas infrastructure. SOURCE: National Petroleum Council (2001), p. 34.

- Pipeline interconnections (facilities where one pipeline can be connected through a set of valves and crossovers to other pipelines);
- Compressor stations (where gas compressors, driven by large electric motors or gas-fired engines, pressurize the gas to facilitate its movement through the pipelines);
- City Gates (stations where high-pressure gas from the transmission line is transferred to delivery pipelines at lower pressures for distribution to cities);
- Liquefied natural gas facilities (where the gas is liquefied by compression and cooling and then placed in special containment vessels, such as ships, or where the LNG is taken from the containment vessels and gasified for delivery into the city pipeline distribution system); and
- Control systems, where all of the above functions and processes are controlled and monitored.

Any of these facilities would be vulnerable to a deliberate attack. It could take the form of a direct assault by a small team of terrorists using any weapons and explosives readily available, or it could be in the form of sabotage performed by an insider. A cyberattack on the control system is possible via the Internet, by using radio-frequency devices to scramble microwave signals, or by physical occupation of the control center. Under present conditions, a well-planned and coordinated terrorist attack could take out the nation's gas transmission systems

and keep key pipelines out of service for an extended period of time. The resulting loss of this basic energy supply to large areas of the United States would affect home heating, electric power generation, and business and industry, causing enormous personal and economic damage.

Representative Vulnerabilities

Transmission Pipelines. Natural gas pipelines present appealing targets. Natural gas is produced in concentrated areas, generally along the Gulf Coast, in the Rocky Mountain region, and Alaska, or imported from Mexico and Canada. It must be transported to 1,500 regional and local distribution companies (LDCs) via a comparatively small number of long-distance transmission lines. The Northeast, North Central, and Pacific Coast regions of the United States depend on supplies delivered by these large, long-distance pipeline networks, and there are no viable alternatives to this arrangement. While the pipeline network has a degree of interconnectivity that provides the ability to reroute, several regions are totally dependent on a single major pipeline system. The inter- and intrastate transmission system is characterized by large, buried, high-pressure pipelines, intricate systems of computerized valves, aboveground compressor stations, exposed (and marked) rights of way, and river crossings. Close security over these transmission systems is very difficult because they cover such extensive geographic areas; to deal with interruptions and any malicious damage to these systems, emphasis has historically been on response after detection. The control systems, when in operation, are able to rapidly detect loss of pipeline pressure or abnormal indicators in a pipeline system. Typically, automatic shutdown systems are activated to isolate the problem and provide the opportunity for a repair team to go to the site, assess the situation, and effect repairs. Another option is for the control-system personnel to manually close valves and isolate a problem area. These response scenarios are designed to handle relatively normal interruptions of service. They were not intended for, and are not adequate to deal with, the types of terrorist threats that now must be considered.

Pipeline Interconnections. Pipeline interconnections typically involve large valves, manifold piping, and controllers. Receipt and delivery points with valve interconnections are also found in all pipeline systems; they are located both within individual systems and between pipelines of different transmission companies. The loss of an individual interconnection may not be very serious, but interconnections become critical components with the loss of transmission lines or when they are associated, say, with a major gas storage facility. Interconnections are aboveground and protected by nothing more than chain-link fences unless they are part of a larger facility. Terrorists could easily identify pipeline interconnections that are located in remote areas and breach the chain-link fence. Destruction of an interconnection would eliminate the possibility of rerouting

flows and also could prevent drawing from storage facilities. Attackers could destroy the interconnection facilities with explosives, which would also provide the opportunity for immediate media attention. The spectacular fire and destruction that could be expected from such an attack would meet the terrorists' need for recognition. Because these valves and connections are frequently of unique design, replacement could take months. Premature shutdown of an interconnection valve is another vulnerability. Attackers could shut off valves physically or through takeover of the SCADA system.

Compressor Stations. Natural gas pipelines typically have compressor stations placed about every 60 miles along the route to maintain high pressure (typically 700-800 psi, although pressures can be as high as 1,400 psi). Compressor stations are large facilities that can cost more than $40 million apiece. Their operating components include valves, compressor units, prime movers to drive the compressors, and various piping and controllers. These stations are usually staffed with small maintenance or operating crews, but today some are unattended, being operated instead through remote SCADA systems. Even when staffed, physical security at compressor stations is generally minimal—intrusion alarms, sensors, and surveillance devices are not usually in use. Compressor stations tend to be noisy, so they are often located in remote areas. These stations would be relatively easy targets, particularly during the night when lightly staffed. Compressor stations typically have systems to shut down compressors and activate isolation valves to shut off all gas flow—that way, the risk of explosions and fires is minimized in case of a line break. However, these protective systems would probably be ineffective in a terrorist attack; it would likely occur too rapidly for an operator to have time to activate the isolation valves.

The impact of the loss of a compressor station would vary with season, the number of stations on the pipeline, and the location. During a seasonal peak period, the loss of one compressor station, assuming the pipeline itself was not interrupted, would cause a 25 percent reduction in flow. The duration of the disruption would depend on the components damaged or destroyed. Some components require long lead times for replacement or major repairs because they are not stocked as spare parts, given their high cost and reliability. The loss of two or three compressor stations in a series (or the first compressor station in the series) on any major pipeline could halt its operation for an extended period while repairs were being completed.

City Gates. City Gate stations are where local distribution companies (LDCs) receive gas from the transmission pipeline for their distribution systems. City Gates are essentially interconnections that are critical nodes in the system. The loss of a City Gate station can disrupt service to a large metropolitan area because typically little or no rerouting can be performed, especially during peak periods. City Gate patterns differ among LDCs. Smaller cities and towns may have one

City Gate connection, making that interconnection extremely important to those communities. Major cities such as Chicago may have six or more City Gate stations, which reduces the impact from a disruption at one station; however, during peak periods the disruption of even one City Gate would have the potential to take the whole system down. Today City Gates are often easily identified and poorly protected. Again, the only protection, typically, is a chain-link fence, and repair and restoration of a lost City Gate could take months. Meanwhile, the lack of gas supply—for instance, to a Northeastern city during a cold winter—could cause substantial numbers of illnesses, deaths, and economic hardship.

Similarly, pressure loss could disrupt service to the entire city for extended periods of time. And when service is finally restored, a significant problem would still exist. Every nonelectronic pilot light in the service area would have to be manually relit in order to avoid explosions.

Pipeline Control Systems. Natural gas pipelines typically are controlled remotely, often via microwave communication systems. The destruction of microwave towers could cause significant damage to gas pipelines. These important communication links for the control system are spread throughout the country, easily identifiable, and difficult to protect. Backup telephone control could be employed, but this would increase demand for staff to carry out the manual operations. Companies with sufficient redundancy in their communications/control systems may be less vulnerable to this type of attack.

SCADA equipment consists of sensors, computers, telecommunications links, and other mechanisms that allow station operators to monitor operating conditions and maintain control. Highly developed SCADA systems permit the remote control of valves and compressors. Loss of the SCADA system (or a cyberattack on it) could therefore have serious consequences for operations both on transmission pipelines and, increasingly, within the LDC's territory.

Liquefied Natural Gas. LNG is produced by compressing and cooling natural gas into a liquid for easier transportation—typically by specially designed and built LNG tanker ships. Damage or leakage in an LNG tanker ship or land-based storage tanks could cause an explosion if gas vapors are ignited. The resulting large fire could cause additional fires and human casualties over a large area. Because of this danger, LNG ships and facilities are afforded special security and safety measures commensurate with the threat, and LNG port facilities are carefully designed and constructed to maximize safety. The U.S. Department of Transportation has regulatory oversight, including security authorization, over LNG facilities, so that, like nuclear power plants, they have significant safety and security programs.

LNG security regulations include standards for access control, perimeter protection, barrier strength, patrols, inspections, warning communications, monitoring systems, lighting/power needs, and personnel training and qualification

requirements. The facilities are equipped to handle natural disasters and some terrorist attacks.

Oil and Refined Products

The United States has over 600,000 oil wells, 161 oil refineries, 2,000 oil storage terminals, and about 74,000 miles each of crude and product transmission pipelines. Additional pipelines connect petroleum resources from Mexico and Canada, as well as from platforms and fields up to 100 miles offshore in the Gulf of Mexico, to U.S. storage and refineries. Almost all these assets are privately owned and operated (NPC, 2001). Recent trends in the industry have been toward consolidation, resulting in fewer but larger companies seeking greater efficiency and increased returns on their sizeable investments.

The most vulnerable components of the oil industry infrastructure are its refineries and pipeline pumping stations. Over 40 percent of the refining capacity in the United States is concentrated in Texas and Louisiana, and approximately 60 percent of the Northeast's refined oil products come from these refineries, mostly by pipeline. Even with this concentration, however, a single attack on one component of the infrastructure would not be catastrophic. Offshore oil platforms are also inherently vulnerable to a number of attack scenarios; however the loss of a platform, while likely a spectacular event and a costly one for the crew and the owners, would not rise to the level of being catastrophic for the nation as a whole. Coordinated attacks on multiple key targets could have serious regional impact—including, under some conditions, many fatalities, but the probability of catastrophic impact is much less than in the electric and gas sectors because of the ability to store and import oil products and crude oil.

Representative Vulnerabilities

The physical vulnerabilities of the oil infrastructure are shown in Figure 6.2.

Refineries. Refineries are the centerpieces of the oil products infrastructure. They are complex sets of process units, many of which are custom-built for the task. Major process components, such as the crude distillation or catalytic cracking units, are one of a kind. If such units were lost through a terrorist attack, it could take months or years to rebuild them and bring them back on line. However, most large refineries are made up of several trains of similar process units. Thus in order to bring down an entire refinery for a long time, a highly coordinated attack would be required. Refineries are also vulnerable to attacks on other infrastructures. For example, their sensor and fire-suppression systems are generally reliant on the electricity and water infrastructures.

For institutional, environmental, and financial reasons, no new refineries have been built in the United States in recent years. One result is that the

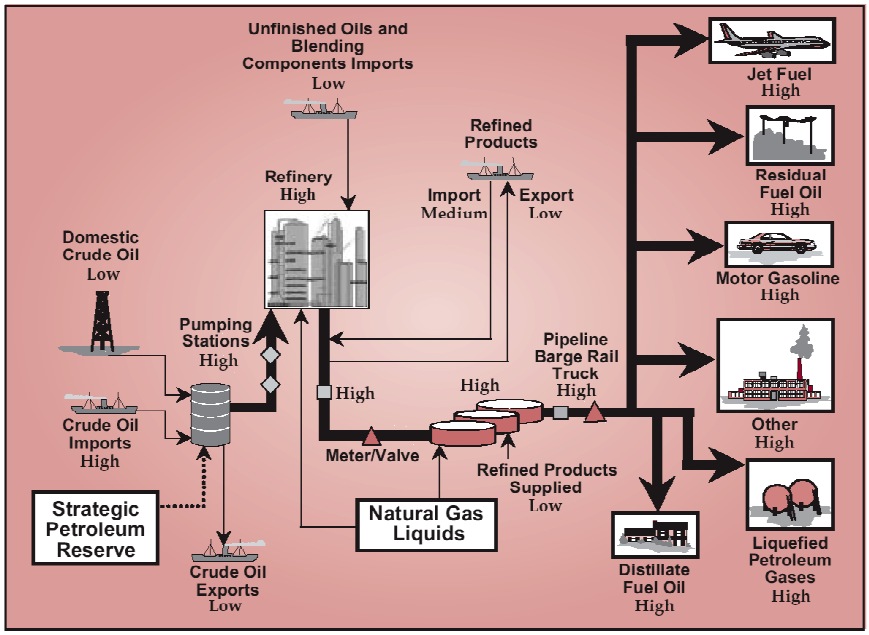

FIGURE 6.2 Oil system vulnerabilities. SOURCE: National Petroleum Council (2001), p. 33.

facilities in place are operating at 93 percent of capacity. Another is increased production at existing facilities. Refineries have, in many cases, installed equipment and tankage close to their fence lines. Meanwhile, some neighboring communities have allowed commercial and residential developments to be built right up to the other side of the fence. Problems within the refineries could directly affect many people. In particular, a few refineries have process units that use toxic chemicals. An attack on one of these units that ruptured one of the associated containment vessels could cause the release of a cloud of toxic gas, which could result in major loss of life. This is the most significant vulnerability of refining with respect to catastrophic terrorism.

Refineries are required to produce over 80 different blends of gasoline to satisfy the diverse environmental regulations throughout the country, making it difficult to replace a gasoline supply in a particular local area when an outage occurs. For example, California could face a fuel shortage following a coordinated attack on its refineries because there is limited ability to supply its uniquely specified fuels from other regions. This impact could be mitigated if the state and federal governments relaxed their location-specific fuel requirements in case of a catastrophic event.

Pumping Stations for Crude Oil and Refined Product. A coordinated attack on several key pumping stations for crude oil or refined products could lead to serious economic disruption. For example, a significant portion of the product used in the Northeast comes from the Gulf Coast by pipeline. Pumping stations are generally, but not always, unstaffed large facilities covering several acres. The pumps may be in the open or housed inside a sheet-metal building. Pumping stations are typically fenced, but they usually have no intrusion detection system. Unfortunately, because the main and backup power transformers for these sites are often colocated with the pumping station, all power supplies could easily be taken out at the same time.

Pumping stations tend to be remotely monitored and controlled through SCADA systems that communicate with a remote control center. The loss of a pump or other single component at a pumping station can usually be handled routinely with existing spares. However, the outage following a terrorist attack that destroys a large amount of equipment could last at least 4 months if replacement pumps and drivers are available, and perhaps 8 months to a year if they are not. In the meantime, supply at the end points of the pipeline would be greatly curtailed, although ships, barges, tank trucks, and trains might be employed to deliver essential products to those in greatest need.

Command, Control, and Communications. SCADA systems are vital to the operation of many facets of the oil business, including pipelines and refineries. SCADAs are particularly vulnerable to cyberattack because they were initially designed without consideration of security. At times, operators allow direct connections between a critical control network and the company's local area networks or the Internet; intranets and the Internet are common vehicles for cyberattack, by insiders or outside hackers (Teumim, 2002). In addition, pipelines use radio-frequency and microwave systems to transmit data and to operate remotely. These wireless transmission systems are vulnerable to intrusion.

SCADA systems also are increasingly integrated into company business systems, making them even more accessible to cyberattack. The industry has not been exposed to the large-scale, sophisticated cyberattacks experienced by the financial sector and by government defense and intelligence agencies, but these may just be a matter of time. Some SCADA design companies and operators are introducing security elements into their SCADA systems to prevent intrusion, but wider application of existing security technology and development of more robust technology are needed.

In addition to cyberattack, physical attack on the pipeline or refinery control centers that house the SCADA systems would cause major disruptions, which could be very difficult to remedy quickly. The industry would also be vulnerable to disruptions caused by the loss of electricity and water supplies needed to run pipelines and refineries.

Implementation of Existing Technology

Implement Vulnerability Analysis to Identify Key Assets for Protection

The facilities of the oil and gas infrastructures are vast and complex, covering large geographic areas and involving numerous components. Tools for vulnerability assessment and prioritization of key assets in these systems must be used to ensure that owners' limited resources are applied effectively. Such tools have been used extensively in the national security and defense communities, and it is recommended that they be aggressively directed to energy infrastructures as well (see Recommendation 6.2).

Create Incentives for the Deployment of Terrorist-Resistant Cybersystems

The oil and gas industries are dependent on cybersystems. Because these industries have not yet suffered the consequences of sophisticated cyberattacks, their expertise on high-security cybersystems is relatively undeveloped; until September 11, they had little incentive to consider the use of these often-expensive security measures. The situation has now changed, and the industries—along with their vendors, standard-setting organizations, and technology suppliers—need to develop and deploy more robust terrorist-resistant cybersystems (see Recommendation 6.9). A partnership with government, perhaps through the national laboratories, might be an appropriate way to pursue this goal.

Improve Dissemination of Information on Threats

Individual companies need timely information on potential attacks in order to take actions that deter them or minimize their impact. A reasonable balance is needed between corporate America's need to know its own risks and the need to secure information for homeland and national security.

Industries, including oil and gas, need a mechanism such as an information sharing and analysis center for receiving and disseminating critical real-time threat information. In fact, the oil and gas industries are in the process of forming such a center. However, one consequence of the industry's highly competitive nature is that industry members are often reluctant to share information with the government if by so doing that information may later be accessed and exposed through a Freedom of Information Act (FOIA) request. FOIA should therefore be modified to exempt information on critical-infrastructure protection (NPC, 2001). Members of the oil and gas industries are also concerned about antitrust and liability issues. All parties must realize that the business-as-usual environment of the past is clearly not suited to the defense of our homeland today, but companies will need to see some changes in government policy to be confident they can move forward without causing new problems for themselves (see Recommendation 6.3).

Provide for Emergency Federal Policy to Facilitate Recovery from a Catastrophic Shutdown of Oil and Gas Facilities

For example, carrying out existing crime-scene restrictions at the site of a gas-pipeline catastrophe could unduly delay emergency repairs. Another example is the large number (80+) of individual gasoline blends required to satisfy various local environmental regulations across the country. Requiring industry to replace all those blends lost in a terrorist attack on refineries or pipelines would seriously hinder recovery. Government and industry should identify and approve temporary measures—and put them in place *prior to* a catastrophic disruption in the supply—to permit emergency actions for a stipulated time that would facilitate energy-supply recovery (see Recommendation 6.6).

Harden Facilities by Deploying Known Technology

The science and engineering of security technologies have been extensively explored and applied by this country's national security and defense communities. The oil and gas industries must now consider applying technologies as well. For example, pipeline systems nodes, junction points, compressor stations, and control centers could be hardened by applying known technology not normally employed by oil and gas operators before September 11. Moreover, as industries continue to assess their own particular vulnerabilities, whatever gaps exist and whatever additional R&D may be needed should become clearer. For example, R&D could reduce the cost of protecting key equipment (see Recommendation 6.4).

Reduce the Potential for Toxic Gas Emissions

Some refineries could release highly toxic chemicals in a gaseous cloud if a reactor were ruptured. Technology has been developed and is commercially available to mitigate this risk. In view of the higher threat level, the oil industry needs to reassess vulnerabilities in refineries where the new technology has not yet been applied.

Recommendation 6.18: In view of the increased threat level, oil refineries using process technology that could release toxic gases should be encouraged to install available technology to mitigate that risk.

Research and Development Priorities and Strategies

There is a variety of areas where new science and technology can help reduce or eliminate the impact of a terrorist attack on oil and gas systems.

Special-Purpose Sensor and Monitoring Systems

Oil or gas systems might be shut down for months or even years if particular critical processing units are damaged. Most refineries have capable perimeter security, while pipelines have only minimal security. In either case, there is a risk that intruders could gain access and detonate an explosive near critical equipment. New high-sensitivity devices for detecting explosive material need to be developed for use in oil and gas environments. Used in combination with communication and control systems, such devices could alert remote operators to a threat and the need to take mitigating steps. This research could be managed by DOE and should draw on current sensor-development work in universities and the national laboratories. Industry-unique issues could be integrated into this R&D, perhaps through such industry groups as the National Petroleum Council.

An alternative to the installation of many fixed-position sensors and support systems would be the use of robotic units with intelligence that could prowl the production units, testing for potential signs of attack. These robotic units could also make good use of video and manipulator systems to allow personnel to examine a suspicious object without risk of exposure. Robotics is further covered in Chapter 11.

Holistic Simulation and Operating Models

Oil and gas operations models need improvements to handle the threat of terrorist attacks. Holistic models should be developed that incorporate the complexity of interdependent systems (water and electricity, for example) and systemwide vulnerabilities to the newly recognized terrorism threat (see Recommendation 6.15). These models could improve the analysis of system vulnerability to attack and indicate (as well as expedite) the appropriate responses should an attack occur. Integrated multisensor warning systems (MWS) should be developed that would recognize unanticipated activities and provide real-time information to the holistic operating models.

Recommendation 6.19: Integrated multisensor warning systems (MWS) should be developed for the oil and gas industries in order to enhance response, control, and postevent analysis. These MWS would recognize unanticipated activities and provide information to new, holistic operating models.

Advanced control systems would take instructions from these holistic operations models to mitigate the consequences of an attack; for example, control equipment might isolate critical components of the network or reduce the volume of the hydrocarbon or chemical released. The modeling of individual facilities would best be conducted by the oil and gas industries themselves. The develop-

ment of models of the interdependencies of infrastructures, however, should leverage the work of the newly established National Infrastructure Simulation and Analysis Center, with industry involvement coordinated through a group such as the National Petroleum Council. Federal funding for this modeling, which might be managed by DOE, is essential.

High-Reliability System Instrumentation

Current instrumentation for monitoring the health of key systems (e.g., pipelines) is sometimes plagued with sensor failure or unacceptably high false-alarm rates. With terrorist attacks a realistic threat, the performance of these technologies must be improved. Tools for high-reliability system design, self-monitoring sensors to detect the onset of failure, and error-checking algorithms should be developed to transform these technologies so that they can provide real-time monitoring for reliable detection of an attack.

Recommendation 6.20: Tools for high-reliability system design, self-monitoring sensors to detect the onset of failure, and error-checking algorithms should be developed to increase the reliability of monitoring in the oil and gas industries.

This R&D would best be accomplished through a public–private partnership between industry and the federal government—specifically, DOE—with industry participation coordinated through a group such as the National Petroleum Council.

Advanced Intrusion Detection Systems

Improved surveillance techniques for the extended rights-of-way of pipeline systems are needed. The present method of monitoring thousands of miles of pipeline right-of-way—through visual inspection in an overflight—is inadequate. Pipeline operators need new surveillance techniques capable of highly reliable detection of unwanted activity. Surveillance technologies developed for defense and intelligence agencies may be useful in defending against terrorist attacks, as well as against simple right-of-way encroachments, on widely distributed oil and gas assets. These technologies could include remotely operated drone aircraft, satellite surveillance systems, intelligent-software-based analysis of surveillance images to scan for unwanted activity, change-detecting sensors, and intrusion-detection cables designed to sense unusual vibrations or noises (see Recommendation 6.11). Intrusion detection technology R&D could be managed through the existing DOD and DOE programs. Its application to the oil and gas industries could be coordinated by industry groups such as the National Petroleum Council.

Cybersecurity

The oil and gas industries must update security for their information technology and telecommunication infrastructures. Technologies are needed that could contain the impacts of an information system intrusion or cyberattack so that the complete system or dependent infrastructures remain relatively unaffected. Another focus should be identifying and managing risk to infrastructures and information, with emphasis on impact, consequences, and effect across multiple components and operators.

For example, in the energy industries, SCADA systems are increasingly being linked with other systems (such as electronic business systems) through the Internet, and they are thus becoming more vulnerable to cyberintrusion. The SCADA security issue is widely felt not only in the energy industries but in virtually all industries—in fact, in operating facilities of all types. Cost-effective solutions to SCADA security problems are therefore widely, and urgently, needed (see Recommendation 6.9). The public- and private-sector R&D aimed at broad application in this area should be leveraged to address unique issues of the oil and gas industries. As in other such endeavors, industry involvement could be coordinated through a body like the National Petroleum Council, with federal management through DOE.

The oil and gas industries are each made up of a few very large companies and many smaller companies. The large companies make some investment in R&D for security improvement, while the smaller companies typically do not. Even for large companies, however, it is difficult to justify investing in security R&D at the level society might desire or, given their highly competitive nature, to share their results. There is a need for government and industry to jointly share the cost and execution of the needed research and development. The government needs to share the security expertise it has with industry as appropriate, and this is an issue that pertains across the energy industry.

Recommendation 6.21: The federal government and the energy industry should together establish appropriate security goals. Building on this alignment, government should cooperate with industry to establish joint security-performance expectations and to define the respective roles and responsibilities of each in ensuring such performance. Industry should design the security measures and procedures needed to achieve the established security goals. Industry also should provide a mechanism to ensure that expectations will be achieved across the spectrum of firms in the industry.

REFERENCES

Ayres, Drummond. 2001. "Energy Chief Issues an Ultimatum on Power Lines," *Civil Engineering*, December.

Badolato, Ed. *Energy and Terrorism*, forthcoming book to be published in 2002.

Bagli, Charles. 2002. "Seeking Safety, Manhattan Firms Are Scattering," *New York Times*, January 29.

Clemmensen, J. 1993. "A Systems Approach to Power Quality," *Proceedings of Power Quality '89*, as cited in "Storing Power for Critical Loads," *IEEE Spectrum*, June.

Electric Power Research Institute. 2001. Report by the Consortium for Electric Infrastructure to Support a Digital Society, "The Cost of Power Disturbances to the Industrial and Digital Economy," *EPRI Journal OnLine*, July 23.

Energy Information Administration, Department of Energy. 2001. *Annual Energy Review 2000*, DOE/EIA-0384, Washington, D.C.

Loomis, William. 2001. "Super-Grid Transformer Defense," presentation to North American Energy Reliability Council, Critical Infrastructure Working Group, Lake Buena Vista, Fla., December 10-11.

McIntyre, K.J. 1998. "By Holding Back, Power Company Pays: Mercury Energy Ltd.," *Business Insurance* 32(29).

National Petroleum Council. 2001. *Securing Oil and Gas Infrastructures in the New Economy,* Washington, D.C., June.

Office of Technology Assessment. 1990. "Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage," OTA-E-453, U.S. Government Printing Office, Washington, D.C., June.

Oman, Paul, Edmund Schweitzer, and Jeff Roberts. 2001. *Protecting the Grid from Cyber Attack Part I: Recognizing Our Vulnerabilities*, November. See <www.pennet.com>.

Patton, A., C. Singh, D. Robinson. 1999. "N-area Reliability Analysis Techniques," *13th International Power Systems Computation Conference,* Trondheim, Norway, June.

Ragan, Patrick T., et al. 2002. "Chemical Plant Safety," *Chemical Engineering Progress*, February, p. 62.

Teumim, David J. 2002. "Are Your Plants and Pipelines Safe from Cyber Attack?" *Chemical Engineering Progress,* February, p. 69.

U.S. Department of Energy. 2001. *Critical Infrastructure Interdependencies: Impact of the September 11 Terrorist Attacks on the World Trade Center*, Washington, D.C., November.

7

Transportation Systems

INTRODUCTION AND OVERVIEW

Transport vehicles and facilities, from airliners to rail terminals, are recurrent targets of terrorist attacks, hijackings, and sabotage.[1] The September 11 hijackers added a new dimension to this linkage by turning four jet airliners into guided missiles targeted on large buildings. Only a few weeks later, the mailer of anthrax capitalized on the anonymity and reach of the postal system to deliver this bioweapon to targeted persons in the national media and federal government (and to random individuals along the way). Given their prominence in past acts of terrorism, there is good reason to believe that the nation's transportation systems will be exploited again in attacks of equal or greater consequence.

The characteristics of transportation systems make them especially vulnerable—and therefore attractive—to terrorists. Passenger vehicles and facilities often contain large numbers of people in enclosed spaces. Vehicles moving fast—whether in the air, on the surface, or below ground—are in precarious and fragile positions; much damage can be done by introducing a relatively small but well-placed force. Certain elements of the transportation infrastructure, such as U.S.-flag carriers and landmark bridges and tunnels, are symbolic to Americans, adding further to their appeal as terrorism targets.

Many transportation facilities and structures are strategically important, serv-

[1]For a description of the range and nature of terrorist attacks in public surface transportation, see Jenkins (1997, 2001). NRC (1999b) also describes the characteristics of previous terrorist attacks on surface transportation.

ing as key nodes in networks and corridors that handle the movement of large volumes of people, goods, and services, including military transports. Moreover, transportation systems are international in scope and intertwined in economic and social activities. For instance, a few seaports handle a major share of the goods moved in international trade, and commuter and rapid rail transit systems are the circulatory systems of urban environments, critical to the functioning of some of the country's largest cities. Hence disruptions to these systems can have potentially far-reaching and long-lasting economic and social effects.

To be sure, transport vehicles and containers can be tempting weapons in and of themselves, as most vehicles are powered by flammable fuels and some carry bulk shipments of extremely hazardous chemicals. By their very nature, they are highly mobile and thus capable of being used to access a range of targets quickly. And they are ubiquitous, moving unnoticed within industrial locations and major population centers and across borders. Their mobility, range, and omnipresence make transportation vehicles a ready means of delivering terrorist weapons, from conventional explosives to unconventional chemical, biological, and radiological agents. And in the case of mail and express package services, the weapons could be carried into nearly every household, business, and government office in the country.

In the following sections, the committee describes the characteristics of transportation systems, security systems that take these characteristics into account, and the kinds of research that will be required to support the development and deployment of such security systems. After the September 11 attacks, President Bush created the Office of Homeland Security. Congress soon afterward passed the Aviation and Transportation Security Act, which established an Under Secretary for Transportation Security and a Transportation Security Administration (TSA) within the Department of Transportation.[2] Civil aviation security had previously been overseen and regulated by the Federal Aviation Administration (FAA), but operational and financial responsibilities rested with the private airlines and the airports owned by state and local governments. Security in other modes of land and maritime transportation had been, and largely remains today, the responsibility of state and local law enforcement authorities, the many public and private entities that own and operate the transport systems, and various federal agencies responsible for port and border security. The committee urges the new TSA to take the lead in identifying coherent security systems for each mode of transportation, to work with the private and public sectors in this country and abroad in deploying these systems, and to further the development of supporting expertise and technologies.

---

[2]The Aviation and Transportation Security Act of 2001 (Public Law 107-71) was signed by President Bush on November 19, 2001.

TRANSPORTATION SYSTEM CHARACTERISTICS

Security strategies must relate to the systems to be secured and defended. Transportation systems' common characteristics include the following:

• *Openness and accessibility.* Designed and organized for the efficient, convenient, and expeditious movement of large volumes of people and goods, transportation systems must have a high degree of user access. In some cases—highways, for example—access is almost entirely open. Many transportation facilities, such as train stations, are public places, open by necessity. In other cases, access is more limited, as in commercial aviation—but still not fully closed. Even in the case of the latter, it is notable that access to most airport lobbies, ticket lines, and baggage check-in areas remains unrestricted. Moreover, much of the transportation infrastructure, from airports to highway and rail bridges, was designed and built long before concerns over security and terrorism. Fully integrating security will take many decades, as assets are gradually modified and replaced.

• *Extent and ubiquity.* Transportation systems require vast amounts of physical infrastructure and assets.[3] The U.S. highway system consists of 4 million interconnected miles of paved roadway, including more than 45,000 miles of interstate freeway and 600,000 bridges. The freight rail networks extend for more than 300,000 miles, and commuter and urban rail systems cover some 10,000 miles. Even the more contained civil aviation system has some 500 commercial-service airports and another 14,000 smaller general aviation airports scattered across the country. These networks also contain many other fixed facilities such as terminals, navigation aids, switchyards, locks, maintenance bases, and operation control centers.

Most of this infrastructure is unguarded and sometimes unattended. Distributed over the networks are millions of vehicles and containers, which are repeatedly moved from one location to another, complicating the task of monitoring, safeguarding, and controlling them.

• *Emphasis on efficiency and competitiveness.* Although much of the transportation infrastructure in the United States is owned by the public sector, the development of this infrastructure is driven largely by the demands of private users. Widespread use of private cars and motor carriers, for instance, spurred greater investment in the highway system relative to public transportation and railroads. Likewise, travel by motor vehicle and airliners displaced demand for intercity passenger rail service in the second half of the 20th century, prompting increased government spending on airports and freeways. The economic deregu-

[3]See Bureau of Transportation Statistics (2000) for more complete statistics on the extent of the U.S. transportation sector. The numbers cited in this subsection are derived mainly from this compendium.

lation that swept through the transportation sector during the last quarter of the 20th century led to even greater emphasis on efficiency as a criterion for transportation investments and, to a certain degree, led to a loss of redundancy and excess capacity in the sector as a whole. The dynamism of the U.S. transportation sector is unmatched in the world, and a major reason for the country's high productivity and mobility. Another consequence of the emphasis on efficiency, however, is that costly security measures that promise unclear benefits or that impede operations are likely to be resisted or eschewed, whereas those that confer economic benefits are apt to be deployed and sustained.

• *Diversity of owners, operators, users, and overseers.* Much of the physical infrastructure of transportation—from highways and airports to urban rail networks—is owned and administered by the public sector. But while the federal government helps fund construction, it owns and operates very little of this infrastructure.[4] Most of it is controlled by thousands of state and local governments. While private companies and individuals own some fixed infrastructure (as with freight railroads), they function mainly as service providers and users, controlling most of the vehicles and containers that ply the networks.

These public and private owners and operators are largely responsible for policing and securing the system, with the help of state and local law enforcement authorities and, for movements outside the country, foreign governments and international organizations. In addition to providing financial support for infrastructure (and now security for commercial aviation), the federal government's main role is in promoting and regulating safety and environmental performance; supporting research and system planning; and monitoring and regulating transportation activity at border crossings and international gateways.[5]

• *Entwinement in society and the global economy.* Trucks of all sizes distribute to retail outlets nearly all the products purchased by consumers and many of the goods and supplies used by industry and government. The rail, pipeline, and waterborne modes, along with large trucks, move products and commodities long distances among utilities, refineries, suppliers, producers, and wholesalers, as well as to and from ports and border crossings. In recent years, these transport modes have increased their efficiency to the point where just-in-time inventorying and manufacturing are commonplace. At the same time, the airlines have become indispensable in connecting cities all over the United States, and passenger airline service is essential to many areas of the country that depend on tourism and business travel.

---

[4]The major exceptions are the FAA air traffic control system; roads on federal lands; and certain support services, such as the provision and maintenance of navigation aids (e.g., GPS).

[5]A number of federal agencies—the individual modal agencies at the Department of Transportation, for example, as well as the USDA, EPA, the Customs Service, the Border Patrol, and the Immigration and Naturalization Service—have specific responsibilities in these areas.

At the more local level, a quarter or more of the workers in some large cities commute by public transportation, which has come to shape some urban centers, most notably on the East Coast. The U.S. Postal Service delivers mail to every household in the United States and most businesses, totaling some 135 million addresses. The highway system pervades the lives of Americans, who use motor vehicles for most daily activities and for much of their longer-distance vacation travel.

Highways are also used by emergency responders, and both the highway and public transportation systems are vital security assets to evacuate people in a crisis and move critical supplies and services. Consequently, disruptions to transportation networks can have far-reaching effects not only on transportation operations but on many other interconnected functions and activities.

IMPLICATIONS FOR SECURITY STRATEGIES

Certainly, undermining the ability of terrorists to attack in the first place is a national imperative. Should these efforts fall short, however, the transportation sector must be prepared to defend itself. The above characteristics reveal the great difficulty, indeed impossibility, of defending each potential target or perceived vulnerability one by one. The transportation sector is simply too spread out, diverse, and open—by necessity—for such a defensive approach to work. This does not mean that little or nothing can be done to counter terrorism. Sound security measures can do a lot; for instance, they can confound and deter terrorist operations, increase the likelihood of the terrorists being detected and intercepted, keep casualties and disruptions to a minimum, and reduce panic and reassure passengers in a crisis.[6]

What the characteristics of the transportation sector do suggest is the need for a coherent and systematic approach to security. In particular, such an approach should be shaped by (1) well-designed, layered security systems, (2) the adaptive, opportunistic, and dual use of security technologies and techniques, and (3) broad-based and unconventional thinking on terrorist threats and responses.

Layered Security Systems

Transportation security can be best achieved through well-designed security systems that are integrated with transportation operations. The concept of a layered security system, in which multiple security features are connected and provide backup for one another, has a particular advantage. Perfect execution by each element in the system is not crucial, because other elements can compensate

[6]This point is made well by Jenkins (2001) in discussing ways to secure very open public transportation systems.

for human, technological, or other shortcomings, and, correspondingly, enhancements to one element can boost the performance of the system as a whole. Such systems, long used to secure communications and information systems, cannot be breached by defeating a single layer. Because the terrorist can find it difficult to calculate the odds of defeating multiple layers, some randomly interleaved, such a system can deter as well as impede terrorist acts.[7]

The dangers of not taking a coherent systems approach to security were manifest in the aviation sector on September 11. Commercial aviation has been the subject of hostile attacks for more than 30 years. Each new attack has prompted the advent of more technologies, procedures, and rules—each superimposed on the last, designed mainly to prevent a recurrence of similar attacks. Aviation security was provided not through truly systematic means, but rather through a collection of mostly unrelated measures that hinged on a very high and sustained level of performance from each, with little or no backup and redundancy. By overcoming a single perimeter defense, such as a metal detector, an attacker could, in effect, overcome the entire security regime.

The design of the security systems themselves must relate closely to the characteristics and functions of the transportation systems they are intended to defend. Technologies and methods developed for one transportation environment that are modified and applied in an incidental manner to another may yield little more than a patchwork regime.

The prevention of future airline attacks, for instance, may be made possible by systematically identifying and defending against all or most vulnerabilities; for instance, access to airfields and aircraft can be closely guarded, passengers and their luggage can be screened with great care, and airline and airport workers can be monitored. By comparison, the much more open and decentralized maritime and land transportation systems are far less amenable to such a defensive, or protective, approach. The intensive inspection and screening methods used for air transportation security, for instance, are likely to be impractical for transportation modes that require more convenient user access and have myriad points of entry. Means of *deterrence* in those systems are therefore critical, as are means to contain and respond to attacks that do occur. Indeed, it is possible that good mitigation, response, and recovery preparations will themselves dissuade terrorists from attacking these targets since ensuing damage and disruption may be limited.

The importance of understanding the characteristics of each type of transportation system in designing layered security systems is illustrated by the security-system concept for shipping containers presented in Box 7.1.

A few large seaport hubs, or megaports, around the world—such as Los

[7]The need for a systems approach to security is emphasized in both NRC 1999a and 1999b.

BOX 7.1
Shipping Container Threat Scenario and Security Strategy

Background

Intermodal shipping containers carry more than 80 percent of the cargo (as measured in value) moved by ocean liners in international trade. A key virtue of these standardized containers is that they allow for mechanized and automated container handling at transfer points and can be moved readily among modes. The sealed containers are also less vulnerable to cargo pilfering and theft. These virtues have vastly improved the efficiency of ship, train, truck, and terminal operations, reducing the time required for international shipping and enabling more businesses to reduce their warehouse and inventory costs through just-in-time logistics.

In the United States, some 50 ports can handle containers, but only a handful have built a significant business around them because of the large investment required for handling equipment, the need for good connections with highway and rail services, and the economies of scale of warehousing and terminal operations. The three megaports of Los Angeles, Long Beach, and Newark-Elizabeth handle about half of all containers entering and exiting the country. Each of these ports can handle as many as 10,000 containers in a single day.

The U.S. Customs Service maintains inspectors at each port. Their main job is to classify and appraise goods and collect applicable customs duties, although their ancillary functions include the interception of contraband and assistance in enforcing other laws and the regulations of some 40 federal agencies. In most cases, entering containers are cleared with a limited review of documents. Most regular, or "known," shippers are precleared, and their shipments and documents are not examined by Customs until up to 30 days later, which may be at the end point of their line-haul inland journey by truck or rail. Only about 2 percent of containers are opened and physically inspected at some point in the process. Such inspections are time consuming—they usually delay shipments for several days—and add to the costs of shippers and receivers, who often depend on just-in-time service.

A Threat Scenario

A terrorist purchases a foreign exporter that has a long-standing relationship with U.S. importers. The exporter routinely loads containers at its own facilities. In one of the containers, the terrorist loads a nuclear, chemical, or explosive device that is timed to activate or that can be activated remotely. The container is transported unopened through a foreign transshipment port and is then placed along with thousands of other containers on a large container ship destined for a major U.S. port that handles thousands of containers each day. Recognizing the known shipper, U.S. Customs preclears the container with minimal review of documents. Along with thousands of other containers, it is transferred to line-haul rail for inland transportation to the port of entry into the U.S. economy. The full documentation for the container shipment is scheduled to arrive at the U.S. Customs office within 30 days of the container's entry into the country.

At any point during this 30-day interval, the deadly device inside can be detonated. Even if intelligence uncovers the plot, there may be no ready way to identify

and locate the container, and there is additional concern about other containers possibly in place around the country already or on the way. The federal government is probably compelled to halt the movement of all containers and isolate thousands of suspect ones. Even if the device is not detonated, commerce is severely affected by the disruption of trade and the public's confidence in the system of deterrence and interception is eroded.

A Layered Security System to Lessen the Threat

Security cannot begin and end at the port but must be integrated into the entire logistics chain. And it must be part of an overall system that can address multiple threats, rather than an unintegrated series of tactics aimed at addressing one vulnerability at a time. Megaports offer a point of leverage for developing such a systems approach. Containers of most shippers will pass through one or more of these large hub seaports in the United States and abroad. The corresponding port authorities and their governments, therefore, are in a position to impose standardized requirements on shipment security, reporting, and information-sharing that will have a near-universal effect on practice throughout the industry. Industry trade associations may be employed to certify compliance with these standards; for instance, a shipper that does not maintain the prerequisites could be denied membership in the association, and nonmember shippers could be denied access to the megaport or have their access severely restricted.

One prerequisite might be that containers be loaded in sanitized facilities that are certified and subject to recertification after a change in ownership. Such facilities, whether at shippers' own locations or those of the freight consolidators, might be secured from unauthorized entry, monitored with surveillance cameras, and equipped with cargo and vehicle scanners. Images from these scanners could be stored with other documentation on the shipment and forwarded to transshipment points or destination ports for comparisons when the shipment arrives or during randomized inspections along the way. A tamper-resistant mechanical or electronic seal might be placed on the container at the certified loading facility. Light or temperature sensors might also be placed in the container and set to transmit a signal or sound an alarm if activated by an unexpected opening.

Drivers of vehicles that deliver the containers to the ports might have their identities confirmed through biometric cards and be subject not only to periodic checks on their background but to scrutiny, using data mining techniques, for discerning unusual patterns of work and behavior. Microcomputers with transponders might be attached to the motor system to track its route and shut down the engines if it veers from the approved course. Meanwhile, manufacturers, importers, and shipping companies could be required to provide authorities with advance notice of the details of their shipments. Such early notification would give inspectors time to assess the validity of the data, using artificial-intelligence and data-mining capabilities, and to check for anomalies that warrant closer examination.

These capabilities might be provided through a central facility with the necessary expertise and resources; its analysts could then advise inspectors and other enforcement officials on the handling of suspect shipments. Those singled out for closer scrutiny, including shipments from uncertified facilities, could be subject to a variety of nondestructive examinations, from simple reweighing to vapor and radi-

continues

BOX 7.1 Continued

ation sampling to radiographic imaging. The container's original scanned image, taken at the original loading facility, could be compared with subsequent scans.

None of these coordinated measures and associated technologies, if fully developed and implemented, would guarantee success in eliminating all of the many vulnerabilities associated with the shipping-container logistics system, nor have the practicality and total costs of such an approach been fully evaluated. However, a layered system—even with several imperfect elements—would greatly increase the chances of deterring and intercepting threats. It would also allow enforcement authorities with intelligence about a threat to take quicker and more effective actions to identify suspect containers. Such a systematic and credible security system, which could be improved continually through the adoption of new technologies and techniques, would help reassure the public in the event of an incident and help contain disruptions in the critical logistics system by precluding the need for a complete shutdown.

SOURCE: Flynn (2000a, 2000b, 2001) and Leeper (1991).

Angeles, Long Beach, Newark-Elizabeth, Rotterdam, Hamburg, and Singapore—offer points of leverage for designing a security system that encourages shippers to load containers in secured facilities and take other related steps to expedite the movement of their cargoes through the megaports and the logistics stream. Because these ports are so critical to the container shipping industry, such requirements may become the de facto standard in short order. Shippers that choose not to comply may be denied access to the megaports or be subjected to greater scrutiny and its resultant delays.

The narrowing of the higher-risk traffic in this manner, supported by such capabilities as data mining and artificial intelligence (as described in more detail in Box 7.1), will allow authorities to make better use of their limited inspection, screening, and enforcement resources. In fashioning such a layered security system that begins early in the logistics stream, the prospects of a containerized weapon being intercepted before reaching the United States, and the chances of the act being deterred in the first place, are likely to be greater than under the current system of infrequent container inspections at destination ports and other border crossings. Moreover, it is quite possible that the side benefits of such a system, such as a decline in the use of shipping containers for the movement of contraband and the efficiency-related benefits of a sound shipment tracking system, would by themselves provide strong incentives for participants to continually maintain and enhance the system. A multilayered means of securing shipping containers, which will require considerable international and private-sector

collaboration, is now being considered by the U.S. Customs Service[8] and other government agencies.

In a different and more varied context, the experience with ensuring aviation safety over the past 30 years demonstrates how such a layered approach can indeed be pursued with much success. In commercial aviation, it is noteworthy that one agency has a dominant role in ensuring safety through multiple, coordinated means. FAA is responsible for everything from establishing pilot training requirements to regulating the design and manufacture of aircraft and their components. Safety is assured through a multipronged process aimed at reducing risks through rigorous standards for flight crew qualification and training; testing and certification of aircraft designs and materials; quality assurance in aircraft production processes; detailed schedules for aircraft maintenance and engine overhauls; a coordinated system for air-traffic management; standardized operating procedures; and minimum requirements for runway maintenance and airport rescue and fire services.

Coincident failures of all these elements are rare, as evidenced by the excellent decades-long safety record of commercial airlines. When failures (or even near failures) do occur, the safety system is evaluated as a whole and adjustments made (possibly to multiple elements) to remedy the problem.[9]

Given the outstanding performance of the aviation safety system, it is notable that aviation security, also regulated by FAA until recently, was not handled in a similarly holistic fashion. By and large, aviation security tactics and techniques emerged piecemeal, in reaction to a series of individual security failures, beginning with the deployment of magnetometers and x-ray screeners for carry-on luggage following a rash of handgun-enabled hijackings during the 1960s and early 1970s. In this case, the screeners were viewed foremost as protective measures, intended to intercept firearms before they could be brought on board an aircraft. Indeed, year after year, thousands of firearms were intercepted and confiscated by airport screeners.[10] Yet, while the screeners did intercept many guns, they also deterred the use of guns by hijackers. Certainly, the September 11 hijackers were reluctant to use handguns. Such deterrence effects, however, were not evaluated explicitly.

---

[8]In April 2002 the U.S. Customs Service launched the Customs-Trade Partnership Against Terrorism (C-TPAT), which "requires importers to take steps to assess, evolve and communicate new practices that ensure tighter security of cargo and enhanced security throughout the entire supply chain. In return, their goods and conveyances will receive expedited processing into the United States" (U.S. Customs Service press release of April 16, 2002). More details about C-TPAT are available on the U.S. Customs Service Web site at <http://www.customs.gov/enforcem/tpat.htm>.

[9]The importance of a systems approach to aviation security was emphasized in the 1997 White House Commission on Aviation Safety and Security, which was chaired by Vice President Gore.

[10]According to FAA statistics, 13,459 handguns and 1,151 other firearms were detected and confiscated by airport screeners from 1994 to 2000 (personal communication, FAA Office of Civil Aviation Security Operations, May 3, 2002).

More systematic evaluations of security approaches surely would have been helpful in understanding the influence of deterrence and opportunities for strengthening it. Indeed, in seeking to regain public confidence in aviation security after September 11, federal policy makers did not have a coherent system in place that could be readily fixed, prompting Congress to take dramatic and hurried measures, from the federalizing of airport screeners to ambitious deadlines for the deployment of costly and potentially unready explosive detectors.

Deterred from one target, the terrorist may well seek another. But if such deflection is indeed what happens, then it is all the more important that deterrence measures are deliberate and well-placed to ensure that the most sensitive potential targets are the ones that are the least appealing to attack.

Security Methods and Techniques That Are Dual-Use, Adaptable, and Opportunistic

Transportation is a diverse and dynamic enterprise. Transportation operations today, from passenger to cargo systems, are fundamentally different from what they were just 20 years ago, when hub-and-spoke systems, express package delivery, just-in-time logistics, and intermodal container operations were in their infancy. Nearly all modes of transportation have experienced sharp increases in traffic volumes and changes in their methods of providing services. It is important, therefore, to ensure that security approaches are capable of adapting to evolving circumstances.

Perhaps the best way to foster such adaptability is to mesh security with other operational tasks and objectives, such as curbing crime, dispatching and tracking vehicles, monitoring the condition of infrastructure, and assuring safe operations.[11] Indeed, providing economic incentives for transportation users and operators to build security into their operations will be critical; simply urging greater security consciousness will not be enough, nor will it have lasting effect in such a competitive and cost-sensitive sector. First, before investing in new technologies and procedures, it is important that consideration be given to how those already at hand may be put to another use. Grounding of aircraft by the FAA's air traffic controllers after the September 11 attacks and the use made by forensic experts of tracking codes imprinted on U.S. mail after the anthrax attacks show that such dual-use opportunities exist and can be integrated into security planning. As a corollary, security-related technologies and procedures themselves can have wider utility; for example, the matching of airline passengers with their bags may also reduce the incidence of lost luggage, and closed circuit television surveillance and undercover patrols by security personnel may reduce

[11]The importance of capitalizing on other transportation-system goals and features to provide security was emphasized in NRC (1999b).

ordinary crimes in public places such as transit stations.[12] Such opportunities must be sought out systematically, recognizing as well that multiuse, multibenefit systems have a greater chance of being maintained and improved over time.

The potential cost and magnitude of the security task in the evolving and expansive transportation sector means that it must be approached not only systematically but resourcefully. Making a long-term commitment to costly security technologies developed and deployed outside a systems context runs the risk of early and prolonged obsolescence as technologies, transportation operations, and security threats change. A more efficient, adaptable, and system-oriented approach might suggest such tactics as the randomization of security screening, the setting of traps, and the masking of detection capabilities—all to allocate security resources most effectively and to create layers of uncertainty that can inhibit terrorist activity through what have been called "curtains of mystery." To minimize costly disruptions to transportation services, it may be desirable to narrow the security task to target the highest-risk actors and activities. To do so will require a better understanding of normal patterns of behavior and activity, allowing for the preidentification and filtering out of legitimate and low-risk travelers and shippers, so as to devote more security resources to the scrutiny of anomalies.

It makes sense, for example, to integrate information gleaned from computerized airline reservations systems with passenger and baggage screening procedures, rather than treating each as a discrete and unconnected process.[13] Information from ticketing that suggests an air traveler poses a risk could be conveyed to personnel at all security checkpoints—guards at the entries to secure concourses, baggage screeners, and airline gate attendants who examine and collect boarding passes.[14] In more open transportation systems, where it can be difficult to identify and track high-risk traffic, information and communications tools may offer a means to create a "virtual" closed system. Large trucks, for instance, may be required to have an identifier tag affixed to the windshield and scanned at critical points along the highway. The tracking information could be used to ensure that higher-risk trucks—that is, those without tag identifiers or with unusual routings—are scrutinized more carefully at border crossings, tunnels, and major bridges down the road. As an added layer of deterrence and protection, trucks may be subjected to random checks of the validity of the tag, as well as the legality of the driver, vehicle, and cargo.

---

[12]As another example of collateral benefits, when London Transport instituted counterterrorism measures on its rail-transit system, crime and vandalism fell throughout the system even as crime rates increased citywide (Jenkins, 2001).

[13]The need for such integration of security capabilities was observed in the 1997 report of the White House Commission on Aviation Safety and Security.

[14]This information could also be used to process individuals through all other exits from the secure area.

Perhaps the most open of all transportation systems are the public transit systems of large urban areas. Indeed, transit systems around the world have become recurrent terrorist targets because of their openness, concentrations of people, and potential for attacks to cause mass disruption and alarm. Many opportunities exist for using information generated by operations (e.g., ticket reservation records, shipment manifests, passenger identification) to devise layered security systems in air and maritime transportation. Similar information is not available for many of the land transportation modes, such as public transit, where users are often anonymous. Nevertheless, security in other surface modes can be layered through other means, while also capitalizing on dual-use applications.[15] When certain opportunities arise, such as during the design of new stations or the remodeling of existing ones, many cost-effective protective features can be added, such as good lighting, blast-resistant structures, air filtration systems, emergency evacuation routes, and open spaces that provide broad fields of vision. And certainly in areas where free access is not required, such as at railcar and bus storage yards, fences, police patrols, and other perimeter protections can be added—not only to provide security against terrorist attacks, but also to help prevent vandalism and other crimes. The well-placed application of certain technologies, such as surveillance cameras and sensors that detect chemical and biological agents, can further strengthen the overall security system by adding an element of deterrence as well as an early diagnosis and response capability. As they mature, facial-recognition technologies may have strategic application in some public transportation settings, thereby strengthening deterrence and detection capabilities.

But to be effective in such a ubiquitous and expansive mode of transportation, security must be approached holistically. Explicit consideration must be given, for instance, to the important security function of civilian staff, such as bus and train operators and station attendants. Their visible presence alone can serve as a deterrent, and they are in the best position to recognize and report situations that are out of the ordinary before they become full-blown incidents. Attention must given to making on-site staff more visible and training them on how to react and respond appropriately—a critical responsibility, since transit operators and attendants are most likely to be the first personnel at the scene of an attack. Similarly, riders themselves can be an important resource. Active public cooperation and vigilance may be encouraged through such means as recurrent messages and public announcements to be alert for and report unattended articles. Indeed, it is in the most crowded locations, where terrorists are most likely to strike, that the chances are greatest that a passerby, if prompted to be attentive, will quickly notice a suspect package and notify authorities.[16] All of these

[15]For a more complete description of ways of layering security in public transportation, see Jenkins (2001).

[16]For specific examples, see pp. 16-17, Jenkins (2001).

elements together—from blast-resistant designs and well-lit spaces to the strategic placement of guards and fences and deliberate means of enhancing situational awareness by personnel and passengers—can provide a multitiered security system that both deters and protects. And, of course, these elements must be backed up by well-devised and well-rehearsed plans for incident response and restoration of service. Public transit systems that are prepared for response and recovery are less desirable targets for attackers banking on mass confusion and disorder to amplify the harm.[17]

Capability to Engage in Unconventional Thinking on Threats and Responses

The size, scope, and ubiquity of the transportation sector, coupled with its myriad owners, operators, and users, means that many opportunities exist for terrorists to exploit components of transport systems in many different, and novel, ways. After all, terrorists may not view individual transportation assets, infrastructure, and services in isolation and in traditional function-oriented ways but rather as tools that can be exploited for other objectives—much as jet airliners and mailed letters were used as weapons delivery systems last fall. Similarly, terrorists may view the components of other systems, such as the electric power grid, as a means to disrupt or impair critical transportation services. Indeed, it is likely that even the perpetrators of an attack might not realize the full array of economic and societal consequences that could arise as the wave of disruptions moves through many complex and interrelated systems.

Given the broad spectrum of possibilities, the institutions traditionally responsible for securing transportation systems are unprepared to counter the unprecedented means by which they can be exploited for terrorist purposes. Yet it is critical that such possibilities and their risks are anticipated and understood in order to devise precautions and countermeasures. Effective security planning and preparation will require a continuous means of engaging in unbiased and nontraditional thinking about vulnerabilities and threats, their consequences, and appropriate planning and policy responses. This needed analytic capability—from scenario-based threat assessments and red teaming to systems modeling—does not exist today.

RESEARCH AND TECHNOLOGY NEEDS

Many technological capabilities, new or enhanced, will be needed to support well-designed, layered security systems in the transportation sector. But success

[17]For a synthesis of efforts by U.S. public transportation authorities to plan for terror attacks, see Boyd and Sullivan (1997).

will not occur without systems research to help establish the big picture within which the individual efforts—some of them novel ideas and innovations, others the adaptations of technologies developed elsewhere with different primary aims—each play their separate but interconnected parts.

Post-September 11, scientists, engineers, and technologists in the public and private sectors alike will be paying a great deal of attention to airline security and transportation security in general; hence, a strategy that helps guide their efforts is crucial. At the moment, numerous expert groups are offering R&D advice to transportation agencies at the federal, state, and local levels. Missing, however, is more enduring advice on how to go about establishing, implementing, and sustaining these priorities. The approach taken in this chapter is to provide strategic counsel on how to go about identifying and establishing these priorities, rather than offering a highly specified research agenda. The specific research ideas offered next, and summarized in Box 7.2, are illustrative and by no means exhaustive.

BOX 7.2
Key Research Needs for Transportation Security

Systems Research

Operations
- Understanding normal patterns of transportation activity and behavior
- Identification of anomalous and suspect activities
- Dual-use opportunities
- Opportunities to leverage security in operations

Human Factors
- Ability of security personnel to recognize context and patterns
- Design of security devices, facilities, and procedures that are efficient and reliable
- Understanding how to obscure the risk of getting caught
- Understanding how technology can complement and supplement humans
- Creation of security institutions that are performance-driven

Legal and Ethical Issues
- Acceptability of surveillance systems
- Use of biometrics for identify verification
- Use of prescreening systems and means to collect and protect personal information

Deterrence

Psychological studies to model terrorist types
Deterrent effects of tactics to create uncertainty (e.g., “curtains of mystery”)
Deterrent effects of layered countermeasures

Systems Research

A fundamental need is a more thorough understanding of the operations, institutions, and other functions and characteristics of the transportation and logistics enterprises. Such an understanding is necessary to identify candidate security systems—for instance, to determine where the megaport-like "linchpins" may lie for new security approaches. Such systems research and analysis will also provide an understanding of normal patterns of transportation activity and behavior, which is essential for developing security programs that filter out trusted passengers and shippers and for designing and deploying networks of sensors in ways that enhance their accuracy and reduce the incidence of missed and false alarms.

Moreover, an understanding of the operations and economics of transportation systems is crucial for finding ways to integrate security with other transportation system objectives. For example, shippers and other commercial users of

Prevention

Data mining and other data-evaluation techniques to filter out lower-risk users
An understanding of the markers of risk associated with travelers
Explosives detection systems able to detect a wider range of materials
Means to network and combine sensors into "sensor fusion"
Standoff and accurate field sensors with low rates of false alarms
Biometrics and other means of verifying travelers and operators

Monitoring and Mitigation

Real-time chemical sensors that are effective in complex environments
Construction methods to harden transportation facilities
Dispersal models for various agents in transportation environments
Ways to use dispatch and control systems for consequence management
Means of protecting traffic-control systems from physical and cyberattacks

Response and Recovery

Neutralizing agents and robots that can test areas and perform decontamination
Communications capacity for emergency responders
Regional emergency-response plans that coordinate highways and public transportation

Investigation and Attribution

Integrating investigative capabilities into transportation operations and control systems

transportation may be willing to accept the outlays for blast-resistant containers, electronic tamperproof seals, and real-time recording of shipment manifests if they facilitate the general movement of cargo and better secure it against theft and loss.[18]

It will also be important to recognize that certain security approaches are practical and acceptable under some circumstances and impractical and unacceptable under others. For example, in the wake of the September 11 attacks, airline passengers have demonstrated a willingness to endure time-consuming and invasive security procedures. For many travelers, airline trips are long anyway and not a daily occurrence, and extra time can thus be spared for additional security measures. To be sure, similar inconveniences would not be so well tolerated by passengers in the more time-sensitive modes used for daily commuting, and air travelers' impatience with burdensome security procedures can be expected to grow over time, especially if the public views security procedures as more symbolic than substantive.

The advent of effective security initiatives therefore depends not only on good research pertaining to transportation operations but also on an understanding of human factors. Such insight is needed for everything from designing airport security checkpoints that are more efficient and less error-prone to developing means of deterring terrorists through the aforementioned "curtains of mystery." Indeed, human factors are integral to all security initiatives, whether they entail technologies, procedures, or organizational structures.

It is especially important that the role of people in operations and security not be determined by default, simply on the basis of what technology promises, but rather as a result of systematic evaluations of human strengths and weaknesses that can be complemented by and supplemented by technology. Human strengths, such as sensitivity to context and pattern recognition, may be difficult or unnecessary to replicate. Indeed, it may turn out that some technologies do not hold promise because they are inferior to, or incompatible with, the performance of human users—for instance, they might interfere with the performance of flight crews, bus drivers, or screeners.[19]

Many other nontechnical issues also loom large in the development and deployment of effective security systems. Privacy and civil rights controversies, for example, dominate the debate over data mining and biometric technologies for passenger prescreening, identification, and surveillance—a debate that goes beyond the transportation sector, extending to other technology-based realms as well.[20] Though technological advances will undoubtedly continue to offer many

[18]See Badolato (2000) and Flynn (2000a, 2000b).

[19]Prior experience with new technologies in aviation has shown the value of this approach, and the FAA is now committed to early integration of human factors in its acquisition programs.

new capabilities, some will raise new legal and ethical issues that must be addressed long before they are used. Sound systems research and analyses—involving operational, institutional, and societal dimensions—will better bring these issues to light.

To be sure, the restructuring of transportation security technologies, techniques, and procedures to form coherent systems will not be easy. It will require an ability and willingness to step back and define security goals and performance expectations, to identify the layered systems best suited to meeting them, and to work with many public, private, and foreign entities to implement them. Security planners must be willing to question many existing security rules, institutional relationships, tactics, and technologies. This will require much strategic planning, supported by well-targeted, systems-level research and analysis.

Deterrence

As noted earlier, the impracticality of eliminating all transportation vulnerabilities means that efforts to deter must be a key part of transportation security strategies. That reality, together with the likelihood that over the past decade deterrence has probably stopped many hostile acts against aircraft in the first place, put it early in the line of defense against transportation terrorism. But in such a large and open transportation sector, deterrence (or deflection of the hostile act to a less damaging or less protected target) may not be achieved simply by traditional means—guards, guns, and gates. Instead, it will require sound intelligence information related to transportation security and the innovative use of resources and capabilities, which together create high degrees of uncertainty among terrorists about the chances of defeating the system (that "curtain of mystery").

The extent to which uncertainty can deter a terrorist from a specific target is a potentially important avenue of inquiry. How does the fear of getting caught influence actions? Even a terrorist intent on suicide does not want to be stopped before achieving his or her goals. Psychological studies have sought to model criminal attitudes by interviewing perpetrators, and similar studies could presumably be directed to terrorist types in order to better understand the factors influencing their decisions to attack or avoid targets. Such knowledge could prove useful in assessing the deterrent effects of specific tactics such as the use of chemical-sniffing dogs, the randomized deployment of surveillance cameras, and

[20]As an example, civil-rights issues associated with automated passenger-profiling systems are discussed in the report of the White House Commission on Aviation Safety and Security (1997), which also offers recommendations for addressing them. Also, see CSTB (2002) for a discussion of the policy and technological issues associated with national identification systems.

the publicizing (but not the identification) of new but unspecified passenger screening procedures.

Prevention

If deterrence is unsuccessful, the next line of defense is prevention, whether by denying access through physical means—guards and fences, for example—or by other methods of interception, such as passenger profiling, baggage inspection, and explosives detection.

A topic likely to generate much research and debate in the years ahead is how best to filter out the lower-risk users of transportation systems in order to focus security resources on anomalies and the higher-risk traffic. Advanced information technologies offer some promising tools for such identification and prescreening. What is needed, however, is a better understanding of the markers of risk, the kinds of data useful for identifying those markers, and how to interpret and use the results for detection and control purposes.

For example, the application of automated passenger prescreening systems may depend less on advances in biometrics, artificial intelligence, statistics, and computer hardware than on the kinds and quality of data that can be employed in these systems. Not only must the multiple, heterogeneous databases involved be accurate and compatible (both criteria present major challenges), but the right information must be extracted and combined. As an example, how can data on a traveler's financial records, immigration status, legal history, demographic characteristics, and matches to traveling companions on the same flight be used to evaluate his or her security risk, and who will act on the results? Will new databases be created by the linking of various private and public data sources? And if so, how will the information be stored and protected, and who will have access to it and for what purposes? Research on numerous such issues is clearly required to help policy makers evaluate preventive measures.[21]

Yet another prevention-related need is for explosives detection systems that are sensitive to a wider range of materials. At the moment, many threats are not detectable; for instance, a pouch sealed in plastic and taped on a person's body may not register with available screening devices. But new and emerging techniques could augment existing detection capabilities. For example, three sensor technologies that appear to hold promise for explosives detection are x-ray diffraction, which detects several types of explosives; microwave/millimeter-wave scanners, which penetrate denser substances; and nuclear quadrupole resonance, which identifies the chemical compositions of selected materials.[22]

---

[21]See CSTB (2002) for a review of important technological and policy issues associated with the development and use of databases for identification systems.

[22]See NRC (1996, 1999b, 2002) for more detailed assessments of deployed and emerging technologies to improve aviation security.

What is clear, however, is that no single sensor technology can be expected to find all threats with acceptable accuracy, so an array of sensor technologies will need to be developed and used together in a reliable, networked ("sensor fusion") manner whereby each sensor can crosscheck the validity of others. Such crosschecking can help reduce false alarms and the need for inconvenient and costly follow-on searches, such as manual baggage inspections.

In general, all detectors—whether they sense explosives, say, or radiological materials—need to be made more accurate for use in transportation modes, where an excessive rate of false alarms can wreak havoc. They must also be made smaller, more affordable, and capable of operating at greater range. These latter requirements are particularly important if detectors are to be deployed strategically in the surface transportation modes.

Monitoring and Mitigation

Knowing when a hostile attack is under way, diagnosing it quickly and accurately, predicting its course, and mitigating its harmful effects are crucial capabilities that research and development can help provide.

Monitoring is essential to all these crisis-management functions. Indeed, the use of FAA's air-traffic management system to ground aircraft on September 11 demonstrated how existing traffic operations and control systems can be used to detect terrorist attacks in progress and help manage the crisis. The fast and decisive actions taken by local traffic control centers to prevent commuter and subway trains from passing under the World Trade Center may have saved hundreds of lives.

Another example of monitoring capabilities that are not yet available but that could prove crucial in transportation settings is the development of real-time sensors to rapidly detect a wide variety of chemical agents. In a busy transportation environment, rapid recognition of a threat is critical to ensure appropriate response. A prerequisite for the development of such sensor systems is baseline information on the background chemicals in facilities such as subway systems and airport terminals, especially to ensure that sensor systems are designed to balance the risks associated with false positive and false negative readings. On the one hand, excessive false alarm rates are a major concern for transportation operators, lest localized service disruptions regularly propagate across an entire network, eventually causing the alerts to be ignored and alarm systems to be turned off. On the other hand, a single missed or neglected alarm runs the risk of exposing thousands of people to deadly agents and postponing effective emergency response. An appropriate balance must be struck between such risks, requiring risk modeling and human factors assessments.

Research on architectural features, materials, and construction methods to harden transportation facilities has the potential to mitigate the effects of blasts. Research on mitigation could also be useful in protecting structures from earth-

quakes and other natural disasters, although such correlations warrant further study. Similarly, the design of blast-resistant containers for aviation may be helpful for other modes of transport. The DOD has conducted much research on blast resistance materials, designs, and structures, some of which may be applicable to transportation.

There is a great deal of interest in the transportation community not only in mitigating the effects of explosions but in containing the release of chemical and biological agents. Specialized research on the dispersal of various agents within transportation environments is needed—for instance, on understanding how trains moving in subway tunnels may push contaminants within the underground system and through external vents into the streets above.[23] In addition to helping devise sensor networks, such knowledge could help in the development of mitigation equipment such as ventilation barriers and filters and in informing emergency response plans.

Response and Recovery

A key to effective postevent response is the capability to communicate and coordinate the actions of firefighters, police, elected officials, and transportation agencies across numerous jurisdictions. Communication paths, equipment, and protocols must be established in advance, as part of emergency response plans, and sizeable capacity must be made available quickly without having to disrupt basic communications links. Research and development on ways to enhance emergency decision making and communications protocols and capabilities is important to the transportation community, as it is to other participants in incident response.

As noted earlier, the ability to quickly recover and reconstitute transportation services is crucial for limiting the cascading effects of terrorist attacks. This may require a range of capabilities, from the specific means to reroute traffic around the disrupted areas to well-rehearsed, regional emergency response plans that coordinate highway and public transportation systems. Restoring transportation services following an attack will also require a range of technological capabilities—for example, neutralizing agents and robots that can survey affected areas and perform decontamination, as well as tools for the rapid repair of key infrastructure elements to render them at least minimally functional.

Investigation and Attribution

To deter and prevent further attacks, technologies and techniques to investigate and attribute past attacks will also be needed. Catching the perpetrators

[23]See Policastro and Gordon (1999).

before they can do harm again is, of course, one reason to investigate and seek attribution. Another is to learn from the attack in order to prevent future ones. Following the September 11 attacks, data were gathered from the air traffic control system and used to reconstruct the timing and pattern of the four airline hijackings. These analyses could prove helpful in improving the monitoring of traffic and recognizing the early signs of an attack. How best to develop such investigative capabilities—much as cockpit voice recorder and flight data boxes are critical for reconstructing airline crashes—is a potentially important avenue of inquiry.

ADVICE TO THE TRANSPORTATION SECURITY ADMINISTRATION ON STRATEGIC RESEARCH AND PLANNING

The Aviation and Transportation Security Act of 2001, which created TSA, set forth a series of responsibilities and deadlines for the agency, from the assumption of airline passenger and baggage screening functions to the deployment of air marshals and explosives detection systems at commercial airports. Whereas most of the act's provisions deal exclusively with civil aviation, it also gives TSA a broader security mandate—affecting all transport modes—that includes the following statutory responsibilities:

- Receive, assess, and distribute intelligence information related to transportation security;
- Assess threats to transportation;
- Develop policies, strategies, and plans for protecting against threats to transportation, mitigating damage from attacks, and responding to and recovering from attacks;
- Make other plans related to transportation security, including coordination of countermeasures with appropriate departments and agencies;
- Serve as the primary liaison for transportation security to the intelligence and law enforcement communities;
- Enforce security-related regulations and requirements;
- Inspect, maintain, and test security facilities, equipment, and systems;
- Ensure the adequacy of security measures for the transportation of cargo; and
- Identify and undertake research and development activities necessary to enhance transportation security.

The many new and challenging operational and implementation requirements laid out in the act are understandably consuming much of TSA's financial and organizational resources, and they are likely to continue to do so for some time. Nevertheless, the overarching mission responsibilities listed above are essential to TSA's success and cannot remain neglected for long. The following

three recommendations are offered to DOT and TSA for assuming this strategic role. The first recommendation stems from a recognition that the transportation sector is so large, dynamic, and fragmented that no single agency can be responsible for day-to-day security tactics and technologies. If TSA is to have a meaningful role in securing all the modes of transportation, it must be prepared to offer advice and assistance at a strategic level. The second and third recommendations recognize that TSA is the only national entity with responsibility for security in the transportation sector as a whole. It is therefore in the best position to ensure research is undertaken that is useful to all transportation modes and that good information on security technologies and methods is provided to the many public- and private-sector users and providers of transportation services.

Creating a Strategic Research and Planning Capacity

Recommendation 7.1: TSA should establish a *strategic* research and planning office—attuned to, but distinct from, the agency's operational and enforcement responsibilities—that can work with DOT, the modal agencies, other federal entities, state and local governments, and other elements of the public and private sectors on security system research, planning, and deployment.

Having a strong analytic capacity, the office could undertake the following:

- Explore and evaluate alternative security system concepts for the different modes of transportation through collaboration with the public- and private-sector owners, operators, and users and through the application of operations research and human factors expertise.
- Ensure that there are no gaps in security planning and preparation because of the narrow purview, perspectives, and knowledge of individual modal agencies and owners, operators, and users of transportation systems.
- Encourage the explicit inclusion of security goals in the transportation planning process and in the design of vehicles, facilities, and operating systems by seeking out dual-use opportunities and by identifying design standards for new transportation systems and facilities that fully integrate security considerations.
- Advise metropolitan governments and transportation agencies on the need to develop integrated regional emergency response plans; and advise local and state transportation agencies, public transportation authorities, and related entities on how to reshape their administrative structures so as to give security prominence in their planning and decision making.
- Explore ways in which security enhancements can be encouraged, and how market and institutional barriers to the deployment of security measures can

be overcome—for example, through balanced roles for regulation, subsidy, education, and standard setting.

- Work with other countries and international standard-setting bodies to exchange information about international shipments, coordinate security measures and overall system strategies, and collaborate in research and development activities.
- Develop a research agenda in support of transportation security systems.

Multimodal in its orientation, such a strategic office will require a systems planning and engineering expertise and the capability to conduct risk assessments. To obtain this expertise, TSA can make effective use of DOT's Volpe National Transportation Systems Center and other resources that TSA and Volpe can bring to bear. It will also need to interact closely with other federal agencies in domains of responsibility integral to transportation (such as the Coast Guard, the Customs Service, FEMA, and the Immigration and Naturalization Service), with international standard-setting bodies (such as the International Civil Aviation Organization, the World Customs Organization, and the International Maritime Organization), and with state and local agencies at the level of implementation.

To be effective and trusted, TSA must be more than a regulatory and enforcement arm of DOT; it must find ways to share needed expertise and information and to work constructively with those parties—from modal agencies to public- and private-sector transportation system operators—entrusted with fielding the security solutions. A strategic research and planning office within TSA, unencumbered by rulemaking, enforcement, and operational responsibilities, could offer these needed services.

Marshaling R&D in Support of Transportation Security

The committee has identified a number of important systems analysis and technology needs for transportation security, and it believes that TSA is uniquely positioned to undertake, encourage, and guide much of the R&D that will meet these needs. To devise coherent security systems and to procure and recommend supporting technologies, TSA must have its own analysis and research capacity. But it also must have the ability to draw on the rich and varied R&D capabilities within the transportation sector as well as those of the federal government and the science and technology community at large.

The modal agencies in DOT, as well as other federal agencies with responsibility for security functions related to transportation (such as Customs and INS), have missions ranging from safety assurance to revenue collection and drug interdiction. Most have small R&D budgets to support these missions; hence, one can expect these agencies to seek a maximum return on their R&D investments by sponsoring research that meets their own mission-oriented needs first,

while offering security advantages as an added benefit. Such duality of use can be beneficial, but approaching security as a side benefit may result in research gaps and a tendency for comprehensive, systems-level research to be neglected because it does not have a lead sponsor.

In viewing the R&D activities of the modal agencies in their totality and from a broader systems perspective, TSA can help fill these research gaps by offering agencies guidance on the allocations of their R&D investments. From this vantage point, TSA can monitor progress on security-related R&D, observe where modest additional investments might yield large benefits, and orchestrate ways to encourage such investments.

To be sure, much of the R&D that will be needed must take place outside the transportation realm, in the nation's universities and research institutions and with support of much larger R&D sponsors such as the DOD, NIH, and NSF. By making the needs and parameters of transportation security systems more widely known, however, TSA can tap this relevant research from outside the transportation field and help to identify and shape those R&D efforts that are most relevant to transportation applications.

Recommendation 7.2: TSA should collaborate with the public and private sectors to build a strong foundation of research on human factors and transportation operations and to make the evaluation of security system concepts a central element of its collaborative research program. TSA must establish an in-house research capacity to undertake such concept evaluations and to support its own large security operations and technology acquisition programs. At the same time, it must adopt a broader, architect-like role in promoting and marshaling R&D to advance these security systems, especially by tapping into the security-related R&D of other government agencies, the broader transportation community, universities, research institutions, and the private sector.

A Technology Guidance and Evaluation Capacity

Academia and the private sector are eager to contribute creative ideas and technologies to the task of enhancing transportation security. At the same time, transportation system owners and operators are eager to hear advice from universities and companies and use the results of good research and technology development. Currently, however, many of the ideas and technologies being proposed for security purposes have only limited potential for application—not only because of inadequate incentives to invest in them but also because technologies and techniques that seem promising in isolation do not fit well in a security system or are incompatible with the transportation operating environment.

TSA could play a catalytic role here by providing scientists and technologists with clearer targets for their research and innovation efforts. In conjunction with commercial developers and transportation system owners and users, TSA

could help develop product evaluation standards and methods, sponsor prototype demonstrations, and conduct field trials. Precedents for such clearinghouse and evaluation services can be found in the transportation sector and elsewhere, and they could be useful as models.[24]

Recommendation 7.3: TSA should create a guidance, evaluation, and clearinghouse capacity that provides technology developers with performance goals for their products and advises transportation system operators on security-related technologies that are available and being developed.

CONCLUDING OBSERVATIONS

The nascent Transportation Security Administration provides a new, and rare, opportunity to approach transportation security in a strategic manner based on sound science and technology application. It is essential that this opportunity not be lost. The Department of Transportation, and particularly TSA, should take steps now to build this strategic capability and ensure its permanence. In the same manner, others have urged the Office of Homeland Security to adopt such a strategic and architect-like role on a broader scale for the federal government as a whole.[25]

TSA's security mission does not extend beyond the transportation sector, but as the events of September 11 revealed, vulnerabilities to terrorist acts may not be limited to components within particular transportation modes and systems. In fact they may exist in the interactions among modes or between transportation modes and other domains such as energy and computer systems. Someone should be thinking about vulnerabilities that exist at these intersections, the threats that may be associated with them, and appropriate strategies for response.

A broader-based understanding of terrorist threats is therefore needed to inform the transportation community and others on the front lines of defense as they formulate security plans and take precautions. To provide this capability, the committee sees a need for an entity unencumbered by operational, oversight, and regulatory responsibilities, whose mission would be to explore and systematically assess the broad spectrum of vulnerabilities to terrorist attacks, probable responses to these attacks, and ensuing consequences. By involving and informing TSA and the transportation community, as well as parties in other domains, the work of this analytic entity could provide valuable guidance to transportation

[24]One such precedent is the Highway Innovation Technology Evaluation Center, created with seed money from the Federal Highway Administration and managed by the Civil Engineering Research Foundation of the American Society of Civil Engineers.

[25]See Carter (2002).

owners, operators, and overseers as they prioritize and make security preparations. (The Homeland Security Institute recommended in Chapter 12 could be such an entity.)

DEDICATION

The panel is indebted to the earlier work of other National Research Council committees, including reports by the National Materials Advisory Board's Panel on Assessment of Technologies Deployed to Improve Aviation Security, led by Thomas Hartwick.[26] In addition, the 1999 NRC report *Improving Surface Transportation Security: A Research and Development Strategy*, by a committee chaired by H. Norman Abramson, is cited repeatedly and helped shape the panel's discussion on R&D strategies and opportunities.[27] A key member of the committee that produced *Improving Surface Transportation Security*, Fred V. Morrone, Director of Public Safety and Superintendent of Police for the Port Authority of New York and New Jersey, died on September 11, 2001, while responding to the World Trade Center attacks. This panel's effort was undertaken in memory of Superintendent Morrone.

REFERENCES

Badolato, E. 2000. "Cargo Security: High-Tech Protection, High-Tech Threats," *TR News*, No. 211, November-December, pp. 14-17.

Boyd, A., and J.P. Sullivan. 1997. *Emergency Preparedness for Transit Terrorism: Synthesis of Transit Practice 27,* Transportation Research Board, National Research Council, Washington, D.C.

Bureau of Transportation Statistics. 2000. *National Transportation Statistics 2000,* U.S. Department of Transportation, Washington, D.C.

Computer Science and Telecommunication Board (CSTB). 2002. *IDs—Not That Easy: Questions About Nationwide Identity Systems,* National Academy Press, Washington, D.C.

Carter, Ashton B. 2002. "The Architecture of Government in the Face of Terrorism," *International Security*, Vol. 26, No. 3, pp. 5-23.

Flynn, S.E. 2000a. "Beyond Border Control," *Foreign Affairs*, Vol. 70, No. 6, November-December.

Flynn, S.E. 2000b. "Transportation Security: Agenda for the 21st Century," *TR News,* No. 211, November-December, pp. 3-7.

Flynn, S.E. 2001. "Bolstering the Maritime Weak Link," testimony before the Committee on Governmental Affairs, U.S. Senate, Washington, D.C., December 6.

Jenkins, Brian M. 1997. *Protecting Surface Transportation Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks*, Report 97-4, Norman Y. Mineta Institute for Surface Transportation Policy Studies, San Jose State University, San Jose, Calif.

[26]See NRC (1999a, 2002).

[27]See NRC (1999b).

Jenkins, Brian. M. 2001. *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview*, Report No. MTI-01-14, Norman Y. Mineta Institute for Surface Transportation Policy Studies, San Jose State University, San Jose, Calif.

Leeper, J.H. 1991. "Border Interdiction: The Key to National Security," presented before the Seventh Annual Joint Government-Industry Symposium and Exhibition on Security Technology, Norfolk, Va., June 12.

National Research Council, National Materials Advisory Board. 1996. *Airline Passenger Security Screening: New Technologies and Implementation Issues,* NMAB-482-1, National Academy Press, Washington, D.C.

National Research Council, National Materials Advisory Board. 1999a. *Assessment of Technologies Deployed to Improve Aviation Security: First Report,* National Academy Press, Washington, D.C.

National Research Council. 1999b. *Improving Surface Transportation Security: A Research and Development Strategy*, National Materials Advisory Board, Transportation Research Board, and Computer Science and Telecommunications Board, National Academy Press, Washington, D.C.

National Materials Advisory Board, National Research Council. 2002. *Assessment of Technologies Deployed to Improve Aviation Security: Second Report. Progress Toward Objectives,* National Academy Press, Washington, D.C.

Policastro, A.J., and S.P. Gordon. 1999. "The Use of Technology in Preparing Subway Systems for Chemical/Biological Terrorism," *Proceedings of the 1999 Commuter Rail/Rapid Transit Conference*, Toronto, American Public Transportation Administration.

Policastro, A.J., F. O'Hare, D. Brown, M. Lazaro, and S. Filer. 2002. *Guidelines for Managing Suspected Chemical and Biological Agent Incidents in Rail Tunnel System,* Federal Transit Administration, U.S. Department of Transportation, Washington, D.C., January.

President's Commission on Critical Infrastructure Protection. 1997. *Critical Foundations: Protecting America's Infrastructures*, October.

U.S. Customs Service. 2002. Customs-Trade Partnership Against Terrorism (C-TPAT). Available online at <http://www.customs.gov/enforcem/tpat.htm>.

White House Commission on Aviation Safety and Security. 1997. Final Report to President Clinton, Executive Office of the President, Washington, D.C., February 12.

8

Cities and Fixed Infrastructure

INTRODUCTION

Today, more than 220 million Americans (some 80 percent of the U.S. population) live in and around our cities, and over 160 million live in *major* metropolitan areas (with populations that exceed a million).[1] American cities are often seen by those in less developed lands as monuments to our freedoms, our lifestyles, and our wealth—and in some ways, our excesses. For these reasons, and because of their abundance of high-value targets, our cities and their inhabitants have also become the object of terrorism schemes (U.S. Conference of Mayors, December 2001; U.S. Census, 2000).

Cities are by definition target-rich environments for terrorism, whether the aim is people or economic damage. The fixed infrastructure elements of the city—which include the utility systems that provide the essential services of water, electric power, and fuels distribution, digital and voice communications, and waste collection and disposal—are highly interdependent. Highways, roads, bridges, and tunnels provide another kind of target (PCCIP, 1997). Tunnels present particular opportunities because they form extensive networks beneath our cities that enable railroads and highways, transit service, sewage collection and transport, and conduits for utilities.

Cities also contain many attractive "surname" targets. Terrorist attacks on notable buildings, along with ballparks and similar public places where large

[1]For this report, the term "cities" is used to refer to both incorporated cities and their surrounding suburban counties.

numbers of people gather, could be both casualty-rich and newsworthy. Unique facilities such as high-profile universities and national research centers are another set of distinctive potential targets.

Emergency operations centers (EOCs) have become a critical part of the operating infrastructure of major cities. They provide the essential responses for cities and their people during floods, hurricanes, and other natural disasters; during major fires and other domestic disturbances; and now, during terrorist attacks. Thus cities face two challenges associated with their EOCs: the need to upgrade them so that they are prepared to handle terrorist attacks and the need to protect EOC facilities and staff, as they could be targets of terrorists seeking to enhance the impact of other attacks.

The loss of any of these potential targets would, by itself, be serious, but multiple losses, the result of simultaneous attacks on different types of targets, could be devastating. For example, the fires in buildings caused by an attack could not be extinguished if, in a coordinated attack, the relevant water-supply pumping stations were put out of service. The close interdependence of such targets greatly increases cities' vulnerabilities (Dean, 2002).

The elements of cities that must be addressed in order to deter and, if need be, respond to terrorist attacks include the following, each of which is addressed in a subsequent section of this chapter:

- Emergency management and emergency operations centers,
- Water supply and wastewater systems,
- Electrical supply interruption,
- Urban information technology and communications,
- Urban transportation and distribution systems,
- Major and monumental buildings,
- Stadiums and other places for large public gatherings, and
- Underground facilities, including tunnels.

EMERGENCY MANAGEMENT AND EMERGENCY OPERATIONS CENTERS

Introduction

Major cities and many large counties have emergency response plans providing for local EOCs and their personnel to respond to crises such as a natural disaster. Responding to terrorist attacks is a relatively new dimension for EOCs. As such, there is a significant and immediate need for appropriate response guidelines, threat-scenario definitions and training procedures, special or improved equipment, and federal funding to support EOCs across the country in achieving an adequate level of preparedness (U.S. Conference of Mayors, December 2001).

An EOC is a complex organization whose success is directly related to the capability of its communications systems and the competence of its staff to handle intra- and intergovernmental operations in a crisis. The EOC must coordinate, by prearranged plan and agreement, the efforts of key leaders beginning with the mayor, city hall staff, and the directors of police, fire, and emergency medical services. Also integral to the EOC mission is interaction with senior officials from public works and public health departments, utilities, and mass care and mortuary facilities. The EOC should also have direct communications links with the control centers intrinsic to the railroads, highway and transit systems, public utilities, communications facilities, and various neighboring and mutual support organizations.

An EOC is the crisis command center for a city. As determined by its assessment of the event, the EOC must properly activate the triage structure for allocating resources and personnel that assure effective control of the immediate crisis and any cascading damages. Because timely information and analysis are essential, the EOC must be in a position to readily communicate not only with principal players in the crisis response but with governments and the public. The EOC is also expected to provide an information system to capture all pertinent event records. Clearly, in an attack crisis, the EOC is a critical asset for the city and its people.

Representative Vulnerabilities

High on the list of vulnerabilities for these densely populated areas is the possible loss or incapacitation of its EOC and its trained and experienced leadership. A variety of methods could be employed to damage the EOC and its staff, including military weapons, explosives, fire, and gasoline or other volatile mixtures. EOCs are particularly vulnerable because in most cities, their facilities are neither hardened nor necessarily easily protected, having been designed to handle responses to *natural* disasters.

Among the most valuable assets of the EOC are the first responders. Typically these are the police, firefighters, and emergency medical service (EMS) personnel who are the first to answer a call. First responders must quickly assess and report the situation they find; protect, rescue, and provide initial care for casualties; and safeguard property. In a terrorist attack, first responders will likely be at greater risk because of their limited ability to determine the cause and extent of the situation they find. Moreover, a terrorist could try to deliberately kill or injure as many first responders as possible in order to leave the remainder of the city more vulnerable to further attack.

For the first responders, knowing what toxins are present in the smoke and dust from an attack becomes the difference between life and death. Those engaged in this work speak of their concern for getting through the first 30 minutes. Of particular need is a quick means to test the air they must work in; air sampling

and testing kits in general use today are too slow. More concerned with victims than with their own welfare, first responders will routinely put on their breathing apparatus to enter a site without first performing tests. If the smoke and dust happen to contain dangerous toxins for which their apparatus is not a safeguard, the lives of the first responders may be lost.

The effectiveness of the EOC operation is directly related to how well, and at what level of confidence, its communications systems operate. In desktop training and simulated event testing, the EOC usually communicates well with police, fire and EMS units, but in real events the situation may change rapidly and planned procedures may not be as effective as intended. Communications equipment must operate reliably in the presence of products of fire and explosion, and when located in suboptimal places. In the World Trade Center (WTC) attack of September 11, where transmission repeaters apparently failed, the situation rapidly broke down; command and control staff could not communicate with their units engaged in the first response (Dwyer, 2002). As a result, first responders, although following the plan, were lost.

Adding to the responsibilities of the EOC, as the significance of an attack becomes known, mutual support and neighboring units—including county, port and other special-purpose district and state and federal personnel—will begin to arrive and the problems with communications interoperability will increase. The radios of one agency do not, by design, readily net with those of others. This communications barrier increases the danger to a city and its inhabitants during a terrorist crisis. Technology exists that could ease this problem, and policy changes and new technology could eliminate it altogether.

Implementation of Existing Technology

Vulnerability of EOC Sites and Facilities

Recommendation 8.1: FEMA, working with OHS and in conjunction with state and local agencies, should develop a recommended requirements list (RRL) of the facility characteristics, expertise, and equipment required to withstand a variety of terrorist attacks and then assess the EOCs of the major cities to determine their greatest near-term needs for improvements in physical makeup, equipment, preparedness, and plans for recovery if damaged. System redundancies and communications assets should receive particular attention. From this assessment, priority attention should be placed on bringing the neediest EOCs up to minimum standards. The city governments should share the costs of such upgrades to ensure that local authorities are committed to the project.

The RRL should be provided by the federal government to assure consistency across all EOCs and across the country. The agency best suited to prepare

such a list, under present relationships, would be FEMA. Yet because of new and wide-ranging terrorist threats, FEMA should jointly develop the requirements list with OHS (the Homeland Security Institute recommended in Chapter 12 would provide useful data and analysis), OSTP, DOJ, and DOD. EOC professionals and county and city governments should also be represented. FEMA's scope is officially expanding to include preparation for responses to terrorist attacks (FEMA, 2002). The background and working skills of the FEMA staff may not currently be exactly suited to undertaking all the necessary tasks, so close collaboration with numerous other agencies will be essential.

Recommendation 8.2: In the near term, the assigned federal roles and responsibilities of FEMA, OHS, and other federal agencies (DOJ, NSA, DOD) must be reviewed and clearly defined with respect to preparedness oversight and support of the nation's emergency operations centers. These definitions should be published in the Federal Register and made generally available through publications issued by FEMA or OHS for the benefit of all parties involved.

Intra- and Intergovernmental Operations

Training is needed to meet intra- and intergovernmental challenges under the stress of emergency conditions (President's Commission on Critical Infrastructure Protection, 1997). Different requirements and needs; different reporting, equipment, tactics, and training; different funding and budgeting practices; unique vocabularies and acronyms; and preexisting attitudes are some of the problems to be faced when mixed-unit operations occur. There is much to be said for deploying simulation models and training modules designed to familiarize staff with threat scenarios and improve the effectiveness of collaboration among agencies and governments.

Recommendation 8.3: In the near term, intergovernmental working groups (federal, state, county, and city), perhaps locally sponsored but following federally issued guidelines, should be established to gather critical information. They should report their findings on the preparedness of each EOC, and of the corresponding state and federal support units, for a terrorist-attack crisis. This information would also provide input for the development of simulation models; weaknesses should be addressed by responsible local leaders.

Vulnerability of First Responders to Toxins

There is a great need for the capability to identify toxins in the smoke and dust within just a few minutes after an attack (CERF, 2001). No immediate solutions are available, however, unless the military has kits for such analysis.

Radio Communications Vulnerability

The failure of radio communications between responders to an attack has both technical and policy dimensions.

Recommendation 8.4: In the near term, changes to equipment, training, and policies must be identified and introduced at the local level to immediately improve the interoperability, reliability, and clarity of radio communications used by EOCs and first responders in crisis situations.

Research and Development Priorities and Strategies

Vulnerability of EOC Sites and Facilities

Recommendation 8.5: Current EOC vulnerabilities, including those of existing locations and their technical systems (communications; data and video processing; heating, ventilation, and air conditioning; site hardening; and other elements to be identified), must be assessed. Thereafter, federal, state, and local government agencies should cooperate in planning the needed improvements. These plans might include the determination that the only way to provide secure command, control, and communications capabilities is by rebuilding some of the facilities. The option of duplicate or mobile EOCs should be a part of this longer-term (3- to 5-year) examination.

FEMA should take the lead in these longer-term assessments as a continuation of its near-term assessments recommended earlier. Coordinating closely with local authorities, it should identify specific EOCs that require significant upgrading or replacement.

Intra- and Intergovernmental Operations

In the longer term, simulation models based on terrorist threat scenarios must be completed, field tested, authenticated, and deployed, along with corresponding training modules. Extensive coordination between city, state, and federal participants will be required to make this effort succeed. The simulation and training tools will bring the EOCs, along with supporting units in government, to higher levels of preparedness.

Recommendation 8.6: Research, development, and production of simulation models and corresponding training modules for EOCs is needed in order to improve terrorist-threat recognition, resource utilization and allocation, intergovernmental and intragovernmental operations, and public information management and media relations.

Recommendation 8.7: These simulation models and training modules should be deployed as soon as possible to identify weaknesses in systems and staff and to test and qualify emergency operations teams.

Recommendation 8.8: The simulation models and training modules should be used for EOC testing and evaluation under federal controls. This should lead to certification, according to federal standards, of EOCs throughout the country and their crisis management teams.

This program must be undertaken on an expedited basis, with FEMA as the expected lead. The threat-based simulation models could be developed by systems analysis experts in the Homeland Security Institute recommended in Chapter 12 as support for OHS. Representatives of the EOC professionals should participate in this development and testing. FEMA would undertake the full implementation of these tools and would conduct the certifications testing in due course.

Vulnerability of First Responders to Toxins

Robotic units with intelligence would represent the best solution for first entry into the site of an attack in order to test the air (autonomous robotic technologies are discussed furthur in Chapter 11). But a simpler solution (if feasible) would be a self-contained, clip-on device that could instantly analyze the air and signal to a first responder whether it contained dangerous toxins. The device would not need to tell what the toxins are or to measure their concentrations, but would simply answer the question, "Is it safe for me to be here now?" If the answer is no, the unsafe site could be sealed off and a specially trained and properly equipped team summoned. Such sensor units, with enhanced support systems, could also be an asset for national intelligence organizations and perhaps for the United Nations Arms Inspections Service.

Recommendation 8.9: Research and development should be directed to creating a special-purpose sensor and supporting system (with its own appropriate set of sampling, calibration, and verification databases) to analyze the air for first responders at the site of a terrorist event. The self-contained, clip-on device would instantly determine if the smoke and dust at the site contain dangerous toxins and signal safe or unsafe.

Recommendation 8.10: Research and development are needed to develop even more sophisticated technological solutions that would enhance the safety of the first responders, such as robotic units that have suitable intelligence and mobility and are affordable for cities and EOCs.

This research and development should occur at the federal level in the many government laboratories with existing programs in sensors and robotics. NIH and emergency-response professionals should participate as well.

Radio Communications Vulnerability

There are at least three challenges in this area: (1) equipment and technology, (2) availability and use of specified frequencies and standards, and (3) funding. Policy changes by the Federal Communications Commission (FCC) and suitable new standards would allow the United States to replicate the solutions now working in Europe, where a common frequency has been established in the best area of the broadcast spectrum for emergency-use radios (Mayer-Schonberger, 2002). Given the proper incentives, it is expected that the radio communications industry would willingly develop the needed technology, including repeaters, base stations, and mobile units. The federal government could expedite this progress by accelerating FCC changes and funding the implementation of the solutions, thus providing confidence that the strategy will be sustained. These critical improvements will occur only if the federal government assures that the new emergency communications units will be supported by policy and standards and will definitely become the required norm. This issue is also addressed in Chapter 5.

Recommendation 8.11: The Federal Communications Commission (FCC) must be urged to make policy changes and promulgate standards that would allow the United States to replicate solutions now working in Europe, where a common frequency has been established in the area of the broadcast spectrum that is best for emergency-use radios.

Recommendation 8.12: Focused development should be directed to prototype communications units that meet the requirements of the EOCs.

While the entire EOC program to improve communications should be under FEMA, the policy issues that have to be dealt with would engage FCC, the Congress, and perhaps DOJ. The OHS and the national laboratories should be involved in the development and testing of the technical solution, and industry should play a central role. The equipment development could effectively be done under a public–private partnership formula, and the resulting technology might be adapted by the radio-communications industry into an attractive commercial product line.

Federal funding should be made available to cities in order to expedite changeover to the prescribed communications systems.

WATER SUPPLY AND WASTEWATER SYSTEMS

Introduction

The water system consists of four parts: (1) supply, (2) treatment, (3) distribution, and (4) sanitary removal. The supply system comprises reservoirs, dams, aquifers and wells, and the aqueducts and transmission pipelines that deliver

water to distant users. The treatment system comprises filtration and other plants that remove impurities and harmful agents and sanitation facilities (e.g., chlorination) that kill biological contaminants. The distribution system comprises pressure-regulating reservoirs and towers, piping grids, pumps, and other components that deliver water from treatment system to final user. The sanitary and waste removal system comprises sewer and related collection systems that deliver waters contaminated with household and industrial wastes to sanitary treatment facilities, the facilities that process these wastewaters, and the outfall facilities that return recycled waters back to the natural environment. Finally, storm sewers collect and convey storm water runoff to treatment and/or discharge to the environment.

Representative Vulnerabilities

Parts of the U.S. water infrastructure date to the 19th century. Their age and deterioration make them vulnerable to disruption. Also, physical security is inadequate; at many locations, the public has unrestricted access to reservoirs and transmission systems. As in the case of other infrastructure networks, should the water supply system fail, we would want it to do so gracefully. Cities such as Boston, New York, Los Angeles, and San Francisco are served by aqueducts, which if lost from service may have cascading effects; more attention should be given to the interconnectedness of water supply systems and water transfers.

There are over 76,000 dams in the United States. Dam failures can result in thousands of deaths and immense costs. As an example, should the Glen Canyon Dam on the Colorado River fail, the resulting flood would overtop Hoover, Davis, and Parker dams downstream, disrupt the power grid of the Southwest, destroy irrigation in southern California, and flood the Imperial Valley. On the other hand, inducing a structural dam failure is difficult. Still, recent vulnerability studies performed for the U.S. Bureau of Reclamation have led to a precautionary measure: restrictions on truck and boat traffic at some of the agency's dams.

Concrete gravity and earth embankment dams are massive structures that hold back river flow by their sheer weight. Large explosive energies are needed for their destruction. At the building of the Aswan High Dam in 1964, the Egyptian government concluded that a terrorist explosive device of a size large enough to breach the dam would more likely be used against a city than the dam and downgraded the threat. Concrete thin arch dams, light structures that serve as diaphragms across a narrow gorge, are more susceptible to explosive attack. Military experience suggests that even thin arch dams are difficult to destroy by bombing from the air; although a truck bomb on the crest of a thin arch dam at full pool could allow water to overtop the structure, few dams can sustain significant overtopping. However, the United States has relatively few of these struc-

tures. An earth dam can of course be breeched with conventional earthmoving equipment, but this would require unrestricted access for many hours.

About half the U.S. water supply comes from groundwater, generally unfiltered. Wellheads are easier targets than dams, because they are dispersed and little protected, but their physical destruction would not be a threat to life; the response time for such disruption could be days to months. The principal threat lies in the potential for introducing contaminants at the wellhead, not in physical destruction.

The waters collected at dams or wellheads are transferred over long distances in pipelines and aqueducts, typically by gravity with occasional pumping stations. For example, the San Francisco water-supply aqueducts from the Sierra Nevada transport water 150 miles. Most aqueducts are covered, but not all. The California Aqueduct carrying water from the Sacramento delta to southern California is an open channel for much of its 400-mile length. Aqueducts are designed to withstand hazards such as earthquakes, and some have systems for monitoring such natural disasters and responding to them, if necessary. These systems could be enhanced to handle attacks.

Sanitary collection systems are also vulnerable and pose the threat of significant disruption to normal societal functioning, if not to loss of life. Metropolitan areas cannot long function without the prompt and efficient removal of sanitary wastes. Loss of sewer services can make cities essentially uninhabitable, possibly requiring large-scale vacating of homes and businesses.

Gasoline or other flammable or explosive liquids allowed to flow into the sewer system pose the potential for explosions. Such an event killed 200 people in Guadalajara in 1992 (Eisner, 1992). Sewer explosions caused by the illegal or inadvertent release of flammable liquids are not uncommon in the United States.

More threatening than physical disruption is the potential chemical, biological, or radiological contamination of the water supply. Deininger (2000) discusses biological agents and industrial chemicals that could be used to taint drinking water. Even if the mortality or morbidity caused by contamination were minimal, the psychological effect of a credible threat to the water supply could be significant. No one willingly drinks water suspected to have even trace contamination.

The potential points of contamination of the water supply are the following: upstream of the intake of a water supply, at the water intake or wellhead, at the treatment plant, or at a point in the distribution system. The threat of upstream or collection point contamination is limited by the large volumes of water and thus the dilution involved at that stage, and by the effect of filtering and sanitation at the treatment plant. Yet, certain biological agents or their toxins may be very hazardous at low concentrations, and water treatment plants are designed to remove only a special set of contaminants, typically those found in nature. A further concern is that the water supply in several U.S. cities is not filtered. Thus,

contaminants that are not neutralized by chlorination can pass through these systems into distribution.

The greatest vulnerability to contamination is at the distribution level. Downstream of the water treatment and sanitation works, any contaminant that enters the system has the potential for traveling unimpeded to end users. A scenario of concern to many water districts is the potential for backflow into the distribution system from any household connection or hydrant. This might affect a few thousand households (Dreazen, 2001). These agents could arrive in concentrations high enough to be harmful and would be subject to only residual levels of chlorine in the water. The contamination could be targeted to specific end users, such as those in a government building.

Water treatment involves hazardous chemicals in large quantities, specifically chlorine. At the time of the Pentagon 9/11 attack, a string of railroad tanker cars filled with liquid chlorine sat across the Potomac at the Blue Plains treatment works. Chlorine, sulfur dioxide, and other dangerous chemicals are routinely used at every water treatment plant.

Implementation Issues for Existing Technology

Deferred Maintenance

It makes little sense to improve the security of our water system against terrorism without addressing the history of deferred maintenance of the water infrastructure. One of the best and most cost-effective ways to make the water infrastructure more robust against malicious threats is to return its physical condition to a satisfactory level of repair. Initiatives by the federal government to develop a nationwide process and a plan for funding of rebuilding water-supply systems are necessary steps.

Water Industry Slow to Change

The water industry has not traditionally been fast-moving. When the U.S. Environmental Protection Agency (EPA) proposes rules, compliance typically spans a decade or more. Outreach and communication is needed to reduce the "time constant" for change in the water sector. Meanwhile, add-ons to existing technology may provide the best opportunity for improvement because they are more easily accepted by the industry than radically new technology.

Facilities Open to the Public

Many parts of the water-supply infrastructure are highly accessible, partly as a result of multiuse provisions written into public funding legislation. However, control of public access to components of the water system is critical for security

and needs to be improved. Modification of certain provisions should be explored so that current legislation continues to adhere to its original spirit while also allowing authorities to introduce selective physical security for sensitive parts of the system.

Lack of Standardization

Because water systems are typically designed, constructed, maintained, and owned by local water companies or authorities, there is little standardization. This impedes the introduction of new processes and technology. Further standardization is needed, however, across local jurisdictions that control water supply, distribution, and treatment; in that way, neighboring providers may assist one another, and the people that they serve, in a crisis. In addition, because some local jurisdictions do not work well together, mutual aid and cooperation pacts need to be created before a crisis arises.

Aqueduct Conveyances

As noted above, several major cities develop their water supplies in remote locations and bring that raw water to the cities through long and often unprotected aqueduct conduits. Stocking sections of replacement conduit and developing scenarios and plans for rapid repair could lessen the threat of extended loss of raw water supply if sections of the aqueduct were destroyed by a terrorist act. Those responsible for systems dependent on aqueducts should take these and other appropriate steps so as to be better prepared for a possible attack.

Reluctance to Test for Exotic Contaminants

The water sector's history of research on exotic contaminants, drought management, and systems analysis could be reevaluated for the lessons it teaches for security. The availability of specialized water testing is limited in most parts of the country, however, and legal liabilities make laboratories reluctant to participate in testing. This constraint could be removed with revisions to applicable laws; the dearth of laboratory capacity poses a serious limitation to our ability to respond to a contamination attack on the water system. Furthermore, terrorists could use a variety of contaminants. We need to evaluate a tiered approach to testing, beginning with broad characteristics that suggest change from a baseline. Examples might be change in total organic halide, change in ultraviolet light absorbance, or change in refractive property.

Recommendation 8.13: Identify and implement revisions to applicable laws or statutes, thereby removing the constraints to testing public water supplies for dangerous contaminants that might be employed by terrorists. Take

other necessary steps to assure that adequate laboratory testing capability and capacity are available for local water utilities.

OHS should work with DOJ and EPA, along with representatives of state and local water supply agencies, in seeking solutions. It is likely that the constraints are based in state law or county or local ordinances and so must be addressed there. These bodies should be ready to cooperate because it is their water supply that is at risk.

Research and Development Priorities and Strategies

The four highest-priority areas for research on water security are physical security, monitoring and identification of biological and chemical agents, decision models and sampling, and interactions across infrastructures. In addition, there is a need to establish a national center of excellence to support communities in conducting risk assessments and to serve as a clearinghouse for communicating research results to the industry. The scope for such a center would become broad, and multiple branches with well-defined missions added when the need is defined.

Physical Security

The water infrastructure enjoys little physical protection. Much of the supply, transportation, and distribution system is unstaffed and readily accessible to the public. New methods for physically securing the system are needed, as are ways of continuously—or at least periodically—monitoring for intrusion across the large areas that water systems cover. As with other physical infrastructure systems, technology is needed to protect against explosives delivered by motor vehicle or rail. The American Water Works Association is currently sponsoring vulnerability and physical-security training for water system operators, and EPA is funding the national laboratories to conduct the actual training.

Monitoring and Identification of Biological and Chemical Agents

A significant issue in contamination of water is the early detection of chemical or biological agents in the system. While water supplies are routinely monitored for a few contaminants, they are infrequently tested for exotic contaminants that might be introduced by terrorists. Much can be done to improve the situation.

New sensors for better, cheaper, and faster sensing of chemical or biological contaminants in water are needed, based on sophisticated analytical techniques that are available in the U.S. chemical industry. These sensor systems should be small, distributed, resistant to interference, and robust against false positives. For

simplicity, such sensor systems might focus on baseline properties like turbidity or ultraviolet absorbency, which may be indicators for the addition of a contaminant.

Conventional wisdom holds that water's dilution effects would necessitate large quantities of contaminants to pose health problems, but this conjecture is poorly supported by research. The point needs more careful analysis to determine precisely what agents, and in what quantities, pose a serious threat if present in a potable water supply. Further, sensors should be deployed that will be effective in continuously testing the water supply to determine with confidence whether it is safe. If installed in distribution systems, these sensors would likely be effective at determining the presence of backflow-introduced contaminants.

Recommendation 8.14: Research and development are needed to create sensors and supporting systems for monitoring the safety of drinking water. These sensor systems would continuously test the water supply for agents in sufficient concentrations to pose serious threats; they would signal a response site, or automatically close valves, as needed.

Decision Models and Sampling

Important research questions include what to monitor and sample in the water system, as well as when and how; what inferences to draw from the data; and what the resulting optimal decisions should be.

Recommendation 8.15: Research should be undertaken on water sampling schemes to determine what types and population of data points are required for a spatiotemporal network and on intelligent decision processing to be able to reliably recognize the pattern of attack indicators vs. natural hazards. Such research would require that priority attention be given to the development of simulation models that would both analyze and simulate events and serve to train operators in systematic recovery, emergency response, and evacuation.

Interactions Across Infrastructures

The water infrastructure depends on electricity to control pumps, valves, and other mechanical components, as well as to power sensor, computer, and telecommunications systems. Disruption to the supply of electricity would thus have a major effect on water supply and treatment. Similarly, an important design requirement of most urban water systems is adequate water pressure for fire protection; an attack that ignited urban fires and disrupted the high-pressure hydrant system at the same time could therefore cause great damage and loss of life. Research is needed to understand the extent of these interdependencies and to create strategies for effectively dealing with them. This is a crosscutting issue that is covered in Chapters 10 and 11.

In addition, the water supply, treatment, and waste removal system is public infrastructure, owned and operated at the local or regional level or by private interests. Much of the support for rehabilitating and securing this infrastructure will have to come from local resources, complemented by federal funding through agencies such as the EPA, the Army Corps of Engineers, the Bureau of Reclamation, and others. The growing privatization of water supply and treatment introduces new uncertainties over improving security. Further research remains to be done on the effect of increasing water supply security requirements on the willingness of the private sector to assume the attendant risks under today's laws and insurance markets. Should the private sector abandon this market, at a minimum, municipalities would have to find the funds to take over the utilities and the expertise to operate them.

ELECTRICAL SUPPLY INTERRUPTION

In the modern city, virtually all basic needs—food, water, shelter, employment—are dependent on the continuing supply of electricity. Interruptions for a few hours or even a day may be tolerable, but weeks or more without electricity could be devastating. Because cities become dangerous and unlivable places without electricity, urban electrical-supply systems must be made tougher and more reliable. This subject is treated in Chapter 6, "Energy Systems."

INFORMATION TECHNOLOGY SYSTEMS AND COMMUNICATIONS

IT systems and communications have also become indispensable to city life, and their disruption could prove costly. They are addressed in Chapter 5, "Information Technology."

TRANSPORTATION AND DISTRIBUTION SYSTEMS

From foot traffic to automobiles to cargo ships to airplanes, cities include virtually every known form of transportation—along with their vulnerabilities. This subject is discussed in Chapter 7, "Transportation Systems."

MAJOR AND MONUMENTAL BUILDINGS

Introduction

Recent experience indicates that buildings at risk include key symbols of American wealth and political power such as the U.S. Capitol building, the White House, and the New York Stock Exchange. They also include high-rise office buildings, such as the Empire State Building, the Sears Tower, and the

Transamerica Building, that occupy special places in the public consciousness. Entertainment complexes might also be targets, and though coordinated attacks on a few day-care centers would not cause serious economic damage, the emotional toll would be enormous (NRC, 1988, 1995, 1999).

Representative Vulnerabilities

Major and monumental buildings, like most others, are vulnerable to structural failure induced by various combinations of impact, explosion, and fire. In addition, the occupants may be threatened by toxins. Scenarios suggested by recent events include the impact of commercial airliners, business jets, and small private planes. The few incidents involving piston-engine impacts with tall buildings, including the 1945 collision of a B-25 with the Empire State Building and the 2002 crash of a Cessna 172 light plane into a building in Tampa, suggest that these aircraft had insufficient energy and fuel to cause great general damage or to precipitate collapse. Intermediate-size jet aircraft of the kind used by large businesses for their executives, on the other hand, might pose a threat. Impact by commercial airliners is unambiguously catastrophic, as recently witnessed.

Prior to September 11, 2001, bombs were considered to be the principal threats to buildings. Information about such bombs may be found in the FBI's Bomb Data Registry and the Bureau of Alcohol, Tobacco and Firearms (ATF) histogram of actual events. The magnitudes of such attacks on U.S. targets have so far been limited by the size and capacity of trucks permitted to park or circulate in the immediate vicinity of the target buildings.

Impacts and explosions, as illustrated in Oklahoma City's Murrah Building and the 1993 and 2001 attacks on New York's World Trade Center (WTC), can destroy key structural elements, allowing gravity to destroy much or all of the building (ASCE, 1996; Corley, 1998). Some structures (such as those designed for minimum weight) could be seriously jeopardized by the loss of just a few columns. Temperatures of 500°C reduce the strength of common structural steels by 50 percent, and 1000°C reduces the strength to near zero. Columns, floor diaphragms, and connections between the columns and floor joists are the vulnerable members (ASTM, 1998).

In reinforced concrete members, the fire resistance is integral because a thickness of concrete covers the embedded steel reinforcement, protecting the steel from the fire temperatures. With steel members, resistance is presumably achieved, by code, with a layer of fireproofing. But this superficial coating may not be applied properly, or sections of it may be removed from the structure over the course of time, thus compromising the level of protection. The forces from a major impact or explosion also may strip fireproofing from structural elements and assemblies, destroy detection and alarm circuits, break pipes and deplete the available water supply for fire protection, and render smoke control and alarm systems ineffective.

Details of how the fire contributed to the collapse of the WTC towers are still being studied. Some estimates suggest that the jet fuel probably burned out within a few minutes of impact, but not before igniting building materials and contents on multiple floors simultaneously. This would mean that the fires were fed primarily by materials that are equivalent to those in most other high-rise office buildings. The 1988 First Interstate Bank fire in Los Angeles and the 1991 One Meridian Plaza fire in Philadelphia burned out multiple floors in very intense fires fed only by the ordinary combustible furnishings and finishes within these office buildings (Nelson, 1989; Routley et al., 1991), but they did not collapse. An important issue, then, is whether a similar fire in the WTC and or similarly constructed megastructures could cause the building to fall even without airliner impacts.

Single, localized ignition is assumed in building design (Ingberg, 1928). However, a low-grade explosive incendiary device or other method of starting multiple small fires could potentially cause enough damage and spread fire over a large enough area to overwhelm the building's sprinkler system and lead to an uncontrolled fire. Redundant water supply for fire protection and/or redundant sprinkler systems might provide additional protection for these situations and for some types of attacks.

In addition to damage to the building itself, the hazards of impact, explosion, or fire also include flying glass shards (there may literally be millions of them) and airborne toxins.

Heating, ventilation, and air conditioning (HVAC) systems could disperse airborne materials. While most HVAC systems in new buildings are partitioned, serving groups of several hundred people or fewer, older HVAC systems may serve much larger areas. In some high-rise buildings, openings for elevators and plenums run the entire height of the building, creating a chimney effect. Outdoor air enters the building at the lowest levels and rises to the top as it is warmed. These paths provide a ready mechanism for distribution of toxins throughout the entire building.

One way to prevent HVAC units from becoming the entry point for toxic agents is to restrict access to the outdoor air intakes and fan rooms. Outdoor air intakes are commonly located in the walls of buildings, accessible to the street level. In existing urban high-rise buildings, relocating them would be quite expensive and therefore unattractive to building owners. Rooftop HVAC systems are less vulnerable. In new buildings, outdoor air intakes can more easily be protected, and fan rooms can be secured. Such changes are achievable through building codes. While most HVAC systems use air filters, they are not capable of removing many types of toxins. Filters that could remove both biotoxins and chemical toxins are available, but they are costly to install and operate. Few building owners would find them worthwhile in today's real estate markets. However, filters to remove just biotoxins (e.g., anthrax) can be installed and operated; these might be a reasonable compromise. Meanwhile, no technology is

currently available to quickly and accurately sense the presence of toxins in HVAC systems and building shafts and automatically initiate responses. Smoke detectors in use today can initiate certain actions, such as shutting down the HVAC. A more sophisticated approach would involve developing new sensors and installing them in HVAC systems that could isolate dangerous toxins in one area of building as soon as the threat is recognized. These sensors could use the same core element that was described earlier to protect first responders.

Implementation of Existing Technology

Historically, the blast engineering of buildings evolved in response to the most recent destructive event. For example, explosions producing extensive amounts of flying glass led to better glazing systems that include robust frames and mullions, films, and composite glazing. The main barrier to wide application of this latter technology, which has two broad categories, is cost. Structures such as courthouses use standard glazing with laminations to resist shattering, and robust frames and mullions; the cost of these systems is typically 25 percent more than glazing with no blast resistance. State Department criteria lead to glazing approximately two times thicker than conventional systems for the lower 10 to 15 stories; the cost is typically 100 percent greater than glazing with no blast resistance. Another component of cost is conservatism arising out of approximations in CONWEP and BLASTX, the most commonly used software for predicting blast pressure. These approximations are often accepted in preference to undertaking costly three-dimensional, computational-fluid-dynamics (3D CFD) models. Recalibration of BLASTX is needed.

Close attention has been given to the blast engineering of column design, especially for steel column splices, which are typically built to resist global structural but not local bending. Blast loading requires splices to resist local bending as well. Implementation of this technology is hampered by construction cost, magnified by uncertainty in the requisite analysis.

Better knowledge of the engineering properties of masonry (such as that employed to build the U.S. Capitol) and of aged reinforced concrete (such as that at the Pentagon) is needed to exploit advanced analytical techniques. Another benefit would be to introduce new materials such as Linex, a spray-on, self-bonding elastomer that has been tested in Israel with U.S. participation. Linex increases the ductility of masonry walls, such as the inside surface of the brick at the Pentagon.

In crowded urban areas, where adequate standoff distance or blast walls are impractical, new structures should consider new materials such as stainless steel curtain walls. Also, louvers and plenums for air-conditioning may occupy up to 20 percent of the lower-floor wall-surface area, creating a soft spot in the building skin. Alternative designs might reduce such vulnerability.

Fire resistance ratings currently in use in the United States should be cor-

rected. They have been rendered obsolete by available technology. Design methods used in other countries, and their technological bases, should be surveyed for possible use in the United States. In lieu of the time-consuming testing and certification process required to change our codes and standards, provisional changes to current practice could be made by utilizing the existing building regulations in such countries as Sweden, Australia, and New Zealand.

Research and Development Priorities and Strategies

Recommendation 8.16: It is essential that research and development be undertaken that leads to the improved blast- and fire-resistance of major buildings. The results of this research must then be disseminated so that new knowledge is incorporated into the design and construction of new buildings and into the remodeling of existing buildings. The specific areas of focus should be the following:

- **Testing and codification of blast-resistant curtain-wall technology;**
- **Testing and codification of blast-resistant glazing and software (e.g., BLASTX and CONWEP) for evaluating glazing systems, including mullions and window frames;**
- **Materials testing and analysis of fire resistance (including full-scale tests of burning aircraft fuel and common building materials) with respect to the following:**
  - **Building structural systems;**
  - **Missing or deficient insulation;**
  - **Fire-induced thermal conditions within an enclosure, including ventilation effects;**
  - **High-temperature properties of building materials and furnishings, including insulation and structural materials; and**
  - **The structural interactions that occur as a result of fires, with particular emphasis on connections between elements such as horizontal and vertical members.**

Recommendation 8.17: Old monumental buildings should be given special consideration in two areas:

- **Inventorying their material properties and structural drawings as a precursor to protective redesign, analysis and recovery, and**
- **Developing fiber-reinforced laminates for increasing the ductility of their masonry.**

Recommendation 8.18: Study the more advanced fire-rating practices in Europe, Australia, and New Zealand to assess their applicability to the United States.

Recommendation 8.19: Research should be done to determine the most expeditious means for integrating performance standards with building codes to cover technologies that resist blasts, impacts, and the consequences of fire. This could take a similar form to what was recently employed by the National Earthquake Hazards Reduction Program (NEHRP) in its guidelines for seismic design.

This program should be led by the federal government, perhaps NIST or selected national laboratories. The insurance industry should be a significant participant in this work. The fire and blast tests should be planned and performed under the oversight of the National Fire Protection Association. Objective evaluation of results by independent reviewers is an important step towards facilitating the efficient application of new knowledge and procedures in codes and standards.

Performance standards for dealing with terrorist attack require a probabilistic risk assessment (PRA) approach similar to what has been adopted for earthquake hazards. In simplified terms, risk is the product of the probability of an occurrence times its consequences.

One of the obstacles to developing a risk-based methodology for predicting losses from terrorism is the (thankfully) sparse database of significant events. But in the mid-1960s, when PRA was first developed for seismic risk, the relevant databases and supporting geological knowledge were also much less complete than they are today. However, the idea became very productive once the data were collected. For the moment, an initial resource for terrorism is the databases, maintained by the FBI and ATF, of domestic incidents involving explosives. For example, the FBI Bomb Data Center General Information Bulletin 97-1 catalogs the 1997 domestic bombing incidents with statistics on actual bombings, attempted bombings, explosive bombings, incendiary bombings, and breakdowns by region, state, and target.

It has been suggested, without supporting evidence, that older, heavier buildings may be inherently better able to withstand some types of terrorist attack than modern ones. PRA is an appropriate framework in which to examine this question. Risk modeling can also address the economic implications of alternative design requirements—for example, if resistance to progressive collapse became obligatory for modern lightweight buildings—and it is an appropriate framework for showing the insurance and reinsurance industries how blast engineering mitigates risk.

Recommendation 8.20: Universities and the national laboratories should conduct research on the applicability of a PRA risk-modeling approach for quantifying the expected performance of blast- and fire-resistant designs.

A better understanding of air movements and mixing in HVAC systems could lead to improved designs for lowering vulnerability to toxins.

Recommendation 8.21: Research is needed to determine how different toxins might be distributed, controlled, or filtered by buildings' air handling and circulation systems. This work will lead to improved techniques for reducing the potential exposures of occupants. In the mean time, HEPA filters could be introduced where space and fan capacity are adequate to replace the simple dust filters currently in use, with the benefit of adding protection from anthrax and other bioterrorism materials.

Under the oversight of the OHS and NIST, this program could be performed by the American Society of Heating, Refrigeration and Air-Conditioning Engineers (ASHRAE), the relevant professional and standard-setting organization.

The exiting of tall buildings under emergency conditions deserves a special note. While the WTC twin towers collapsed with the loss of thousands of lives, the towers actually performed well in that occupants below the floors impacted by the airplanes were provided enough time, after the impacts and before the collapse, to exit the buildings safely. Occupants above the points of impact were not so fortunate because the impact and blast destroyed the stairwells for the multiple floors over which the impact occurred and egress from the upper floors was cut off. It would be appropriate to review emergency egress and related communications systems requirements for tall buildings in light of the WTC experience. Communication systems that provide information to both occupants and first responders about the location and status of egress routes is an essential element for survival.

Recommendation 8.22: The requirements for emergency egress and communications for tall buildings should be reexamined by the National Fire Protection Association in light of the WTC experience and the results of this reexamination should be used to determine appropriate modifications to building codes and standards.

STADIUMS AND OTHER PLACES FOR LARGE PUBLIC GATHERINGS

Introduction

Recent information indicates that popular venues such as ballparks, concert halls, and entertainment complexes (Disney World, for example) are at risk. In a broader context, mass rallies of any kind must also be considered potential targets, together with the gathering places of the nation's intellectual, political, and financial elites and of its most vulnerable citizens—our children in their schools or day-care centers.

Representative Vulnerabilities

Stadiums are vulnerable to structural failure from explosives or aircraft impact; to airborne toxins; and to panic reaction by a crowd. Recent efforts to exclude explosives from sports venues and traditional efforts to exclude hazardous materials from rock concerts both illustrate apparently successful policies. There are no major recorded incidents of bomb attacks on stadiums, and the time-consuming and intrusive screening of attendees appears to be tolerated at present. There are no recorded incidents of attack by aircraft; however, there are many examples of close approaches by aircraft to sports venues (usually as part of the entertainment), so it would clearly be possible to mount such an attack.

The structural hazards would result from destruction of key load-bearing elements, though on the positive side the structural redundancy of these buildings is relatively high. Also, they typically contain few materials, such as carpets and furniture, that feed hot fires in enclosed buildings; on the other hand, their expanses of plastic seating would be a source of fuel. Fabric and hard-roof domes of sports stadiums may be tempting targets for a well-informed attack that destabilizes the self-equilibrating forces in the tendons and ring beams that support the roofs. In most instances, however, these supporting members would not be readily accessible to saboteurs (though they are vulnerable to aircraft impact).

Toxic chemicals and biohazards present similar threats to stadium crowds as to crowds in subways and other confined spaces: A lot of people are concentrated in a small area, making them vulnerable even to a highly localized attack. Terrorists willing to expose themselves to lethal doses could effectively spread chemical and biological toxins in these close quarters by hand. Dispersal patterns by HVAC would vary according to the types of agents involved, making the extent of their impact on the occupants difficult to predict. Biological, chemical, and radiological agents that could be employed are covered in Chapters 2, 3 and 4.

Panic also appears to be a significant hazard for crowds, sometimes even greater than that of the agent itself. Whether the cause is real or imagined, people reacting under panicked conditions could, for example, overwhelm exiting systems designed for normal (and relatively modest) flows, thereby causing many injuries and possible deaths. Panic and other intangible impacts on people are addressed in Chapter 9.

Schools and day-care centers deserve attention not because of the numbers of people typically present there but because harm done to them would so deeply affect the rest of us. Schools have evacuation plans for certain conditions and lockdown plans for others, which teachers and students regularly practice. But given that the typical buildings in which these activities are housed enjoy little or no hardening, not much could be done to defeat a direct attack of any significance—as was seen in the attack on Oklahoma City's Murrah Building, which contained a day-care center. A greater likelihood of threat for schools and day-care centers comes from the secondary effects of an attack on some nearby

location, as was the case in New York on 9/11. Here again, established plans and well-practiced teachers and students minimized the harm that came to the children. The best defense is to be prepared.

Implementation of Existing Technology

The reaction of stadiums to the impact of an aircraft or to explosions from any source needs to be better understood. In addition, in so far as current technology and the designs of current facilities allow, vulnerability to chemical and biological attacks should be minimized. NIST might do this work with universities and the national laboratories.

Recommendation 8.23: Analytical studies, like those performed for earthquake hazard assessments, should be conducted to evaluate the effects of explosions and aircraft impacts on covered stadiums. Each major stadium (and its roof system) in the country should be analyzed.

Recommendation 8.24: Conduct analyses of how different toxins might be distributed, controlled, or filtered by the air-handling and circulation systems of stadiums, as well as of other places where large public gatherings occur, and make the resulting information widely available, particularly for commercial purposes.

Once there is evidence of an attack, adequate provisions for egress must be available. Unfortunately, the egress built into stadiums and similar facilities currently in use do not consider any kind of terrorist attack or the panicked exodus of a large crowd. But crowd management can be improved by physical or structural amenities and by training and preparation. Improved exits, modified barriers that mitigate injuries, signage, and other modifications to the existing requirements for moving people out of crowded and enclosed spaces should be available to local authorities. Such improvements can also have salutary effects on attendees' attitudes—and on their behavior in the event of a crisis. For example, the highly publicized security at the 2002 Super Bowl reassured attendees, so that even if there had been an incident, attendees would probably not have acted irrationally. As noted in Chapter 9, psychology and social science resources can be brought to bear on efforts to develop more effective methods of crowd management.

Research and Development Priorities and Strategies

We must be able to monitor the air circulating in stadiums for dangerous toxins, but reasonable means are not available for detection of the wide variety of potential chemical and biological agents. Therefore sensors to detect toxins,

similar to and perhaps the same as those recommended elsewhere in this chapter for major buildings and for first responders, need to be developed and deployed. They could be used in conjunction with the control of HVAC systems. Testing and evaluation of airborne-material circulation and distribution by the HVAC systems unique to each enclosed stadium (including on-site testing of simulated aerosol releases) would aid in reducing the impacts of released toxic agents. This is a matter for local building departments, acting on technical advice provided at the federal level.

Recommendation 8.25: Research and development should be directed to creating a special-purpose sensor and supporting system (with its own appropriate set of sampling, calibration, and verification databases) to allow air-handling systems to quickly and reliably determine if the air supply in a building (or a subway or other occupied confined space) is safe or not safe and to adjust the HVAC controls accordingly—for example, contain the dangerous toxins in the area of the building where first recognized, or exhaust the tainted air. (The same sensors and systems recommended in the section above on emergency management and emergency operations centers could apply here.)

In the longer term (5 to 10 years), guidelines should be developed that include assessments of vulnerability to terrorist attacks as a component of the plans for any new large facility for public gatherings. One challenge is to integrate operational and structural practices that achieve strong resistance to terrorist threats while minimizing constraints on the public. Operational practices should include effective crowd-screening technology that enjoys public acceptance. And coordination between owner-operators and structural designers may improve the balance between needed crowd surveillance and built-in structural hardness.

For example, alternative HVAC systems for stadiums should be reviewed to determine whether it is possible to use the systems themselves to reduce risk. If a system is capable of being zoned, to cite one possibility, this could moderate or even prevent much of the toxins' transport throughout the space.

In any case, it is essential that the egress of people under crisis conditions be achieved in a safe and orderly fashion.

Recommendation 8.26: Undertake research to identify improved methods of egress for large numbers of people from crowded enclosures under conditions of perceived threat. Examine the most reasonable numbers and capacities of egress points, subject to constraints on the function and structure of the buildings, to accommodate a crowd exiting in a state of fear.

UNDERGROUND FACILITIES, INCLUDING TUNNELS

Introduction

Developed underground spaces include many tunnels, pipelines, basements, and underground parking garages that quietly serve their cities. These unseen and unnoticed assets may also present excellent opportunities for terrorists. Explosive, flammable, or toxic materials could be brought surreptitiously into the city, placed there, and detonated, largely employing the underground environment alone. Awareness should be the first step in limiting this vulnerability because it can point to the need for surveillance, prevention, and detection of potentially harmful activities in these spaces, thereby limiting exposures. However, several particular concerns that require broader responses would still remain.

Representative Vulnerabilities

Many of our major cities have grown up around railroad lines. Over time, however, the need to separate the railroad's activities from the evolving city became apparent. As a result, urban railroad lines can be found today in tunnels or along narrow or depressed rights-of-way. Thus they are largely out of sight. Meanwhile, railroads routinely carry all kinds of freight—including toxic chemicals, petroleum products, agricultural supplies, and other materials—that could serve the purposes of terrorists. The U.S. Conference of Mayors has expressed concern about this situation (USCOM, 2001). The risk is greatest for sites above or adjacent to the railroad—such as a stadium or concert hall—that are regularly occupied by great numbers of people.

Some major cities, which have grown up adjacent to large bodies of water, are especially vulnerable to the rapid flooding of their tunnels. Where those tunnels are used for passenger railroad or transit services, significant loss of life could result.

Every city utilizes sewers buried under its streets to convey wastewater and storm water to remote sites for treatment and safe disposal. These sewers typically do not flow full—rather, the water is conveyed by gravity in open-channel flow. Thus, should a volatile liquid be dumped into such a sewer and allowed to flow through it and mix with the air present, an explosive mixture could result. If ignited, a section of sewer might then erupt violently, lifting the street, damaging buildings and nearby tunnels for other utilities, and killing or injuring people.

Underground parking for large urban buildings is the rule rather than the exception today; for one thing, development approvals typically require the availability of off-street parking. But as we learned in the 1993 bombing at the World Trade Center, these under-building parking areas are also desirable locations for terrorist attack. A well-placed bomb could cause much damage to the building's

supporting structure, to its mechanical, electrical, and communications systems, and result in large numbers of occupant deaths and injuries.

Implementation of Existing Technology

Vulnerability to Railcar and Container Contents

Inspections could be increased, perhaps at their points of origin, provided that more personnel are made available and that shippers accept the additional delays. Overall, however, current technology and systems are not adequate to meet this threat. This topic is covered in more detail in Chapter 7, "Transportation Systems."

Flooding of Urban Tunnels

Urban transit and railroad tunnels that are below the levels of nearby bodies of water are vulnerable to flooding if breached.

Recommendation 8.27: Local authorities should identify and harden sites favorable to the breaching of transit or railroad tunnels that lie below surrounding water levels, and they should increase surveillance of all activities occurring in such areas.

Recommendation 8.28: Once sites are identified, authorities should analyze them to determine their resistance to the effects of explosives detonated either inside or outside the tunnel.

Underground Parking

The vulnerability of underground parking areas could be reduced by limiting the size and carrying capacity of vehicles allowed entry and by making the inspection of suspicious vehicles or containers routine. Although this approach requires that trained personnel be posted at entrances and is thus expensive (to cover training, salaries, and around-the-clock staffing), parking fees could be adjusted to account for the added cost.

Tunnel Ventilation Systems

Both highway and transit systems tunnels serving cities require extensive tunnel ventilation systems for safe operation. The highway tunnel ventilation systems are designed to remove vehicle exhaust fumes from the tunnels and also to respond to a fire or explosion in the tunnel by isolating the affected zone, thus allowing occupants not involved in the event to exit safely. Transit tunnel ventilation systems are primarily designed to perform the isolation function. Terror-

ists could disable or destroy these ventilation systems, rendering the underground spaces unsafe to use. They could also employ the ventilation systems to distribute toxins throughout the underground spaces served. Conversely, as discussed above for building ventilation systems, the systems could also be used by the owners to contain or remove a toxin released in the underground space.

Recommendation 8.29: Terrorist threats to the ventilation systems used in occupied underground space and highway and transit tunnels and ways to mitigate those threats should be researched by the National Fire Protection Association and the Department of Transportation. Guidelines for action should then be provided to the owners and operators of these systems.

Exploding Sewers

The threat of exploding sewers could be reduced if local authorities establish tighter controls on access (including installation of locking manhole covers); monitor the air inside sewers for the detection of flammable volatiles; and install barriers of grating in the larger sewers to prevent movement of vehicles or other large objects.

Research and Development Strategies and Priorities

Vulnerability to Railcar and Container Contents

An approach for reducing the probability of explosives or toxins being delivered into cities by railcar would be to use improved and universally required intelligent information units (IUs)—transducers, perhaps—for every railcar allowed to move on urban tracks. Base units that load and read the IUs could be developed as part of the same undertaking and made available to all need-to-know parties. At the point of origin, each IU would be loaded with information about the specified contents, origin, sender, receiver, destination, route, and schedule and then sealed by the local transportation authority. The IUs would be readable by local base units as the train approaches a city. Anomalies would bring the train to a halt until the uncertainties are corrected or the questionable car is cut out of the train and moved to a safe siding. It is hoped that the railroads will see ancillary economic benefits to such an IU-based system—possibly for freight-movement management, contents control, rate setting, and other business purposes.

Recommendation 8.30: Research and development should be undertaken to produce improved intelligent information units (IUs) for installation on every railcar, along with operating systems and coded base units (which could load and read the IUs) for every city. The IUs would need to be hardened to radio-frequency wave interference.

Recommendation 8.31: Policies should be developed that allow only railcars with the IUs mounted and operating to move on tracks that pass through urban areas.

Implementation of this recommendation would require the participation of DOT, the national laboratories, the railroads, and the cities and the Conference of Mayors, and should be coordinated by OHS.

Flooding of Urban Tunnels

With the capability to quickly isolate vulnerable sections from the rest of the tunnel system, the flooding of urban tunnels could be mitigated. Such technology could also be used to isolate sections of the tunnels so that smoke, gases or other dangerous mixtures released there could not infiltrate other sections.

Recommendation 8.32: Rapidly deployable tunnel barriers should be developed and produced, and they should be installed at appropriate locations in transit and railroad system tunnels, so that they will deploy—automatically or on signal—to block the flow of floodwaters in the tunnels.

This should be a DOT/TRB research area, with strong support to be expected from the cities and the transit properties and railroad systems that have such vulnerabilities.

REFERENCES

American Society of Civil Engineers. 1996. *The Oklahoma City Bombing: Improving Building Performance Through Multi-hazard Mitigation*, prepared for FEMA, August.

American Society for Testing and Materials. 1998. *Standard Test Methods for Fire Tests of Building Construction and Materials*, ASTM E119-98.

Bowles, David, Loren Anderson, and Terry Glover. 1997. "A Role for Risk Assessment in Dam Safety Management," *Proceedings of the 3d Annual Conference on Hydropower 97*, Trondheim, Norway.

Buchanan, A.H. 2001. *Structural Design for Fire Safety*, John Wiley & Sons Ltd., West Sussex, England.

Civil Engineering Research Foundation. 2001. "Protecting Infrastructure," American Society of Civil Engineering brochure summarizing Executive Program Series "Designing and Managing Vulunerability," held in Washington, D.C., October 23-24.

Corley, W.G., P. Mlakar, M. Sozen, and C. Thornton. 1998. "The Oklahoma City Bombing: Summary and Recommendations for Multihazard Mitigation," *Journal of Performance of Constructed Facilities, Proc. ASCE*, Vol. 12, No. 3.

Dean, Joshua. 2002. "Systems Failure," *Government Executive Magazine*, February 2.

Deininger, R.A. 2000. "The Threat of Chemical and Biological Agents to the Public Water Supply Systems," Water Pipeline Database, Science Applications International Corporation, McLean, Va.

Dreazen, Y.J. 2001. "'Backflow' Water-line Attack Feared," *Wall Street Journal*, December 27.

Dwyer, Jim. 2002. "Before the Towers Fell, Fire Department Fought Chaos," *New York Times*, January 30.

Eisner, Peter. 1992. "Mexico Reels from Explosion," *The Tech*, Vol. 112, No. 22, Massachusetts Institute of Technology, Cambridge, Mass.

Federal Emergency Management Agency. 2002. Statement of Bruce Baughman, Office of National Preparedness, FEMA, Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, U.S. House of Representatives, April 11. Available online at <http://www.fema.gov/library/baughman041102.htm>.

Harmathy, T.Z. 1981. "The Fire Resistance Test and Its Relation to Real-World Fires," *Fire and Materials*, Vol. 5, No. 3, pp. 112-122.

Heritage Foundation. 2002. "Defending the American Homeland," The Heritage Foundation, Homeland Security Task Force, Washington, D.C., January.

Ingberg, S.H. 1928. "Tests of the Severity of Building Fires," *Quarterly of the National Fire Protection Association*, Vol. 22, No. 1, July, pp. 43-68.

Luthy, Richard G. 2001. "Safety of Our Nation's Water," testimony before the House Committee on Science, November 14, Water Science and Technology Board, National Research Council, Washington, D.C.

Mayer-Schonberger, Viktor (to be released). *Emergency Communications—The Quest for Interoperability in the United States and Europe*, Harvard University, Cambridge, Mass.

McGraw, J.R., Jr., and F.W. Mowrer. 1999. "Flammability and Dehydration of Painted Gypsum Wallboard Subjected to Fire Heat Fluxes," *6th International Symposium on Fire Safety Science*, Poitiers, France.

National Research Council. 1988. *The Protection of Federal Office Buildings Against Terrorism,* National Academy Press, Washington, D.C.

National Research Council. 1995. *Protecting Buildings from Bomb Damage; Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications,* National Academy Press, Washington, D.C.

National Research Council. 1999. "Blast Mitigation for Structures," *1999 Status Report on the DTRA/TSWG Program*, National Academy Press, Washington, D.C.

Nelson, H.E. 1989. "Engineering View of the Fire of May 4, 1988 in the First Interstate Bank Building, Los Angeles, California," *NISTIR 89-4061*, National Institute of Standards and Technology, Gaithersburg, Md., March.

President's Commission on Critical Infrastructure Protection. 1997. "Critical Foundations," Washington, D.C., October.

Ramabhushanam, E., and M. Lynch. 1994. "Structural Assessment of Bomb Damage for World Trade Center," *Journal of Performance of Constructed Facilities, Proc. ASCE*, Vol. 8.

Routley, J.G., C. Jennings, and M. Chubb. 1991. "High-Rise Office Building Fire, One Meridian Plaza, Philadelphia, Pennsylvania (February 23, 1991)," USFA Fire Investigation Technical Report Series Report 049, Federal Emergency Management Agency, Washington, D.C.

Science Applications International Corporation. 1994. "Methods for Evaluation of Cable Wrap Fire Barrier Performance," EPRI Report, Project 3385-05, Draft Report, October.

Topographic Engineering Center. 2001. *National Inventory of Dams*, U.S. Army Corps of Engineers, Alexandria, Va.

U.S. Census Bureau, Department of Commerce. 2000. *Population Change and Distribution*, Washington, D.C.

U.S. Conference of Mayors. 2001. *A National Action Plan for Safety and Security in America's Cities,* December.

9

The Response of People to Terrorism

The purpose of terrorism, of course, is to terrorize. And terror is, above all, a response on the part of people. This definitional truth, however, is only partial. The effects of terrorist activities, like the individual and collective motives for such activities, can be multiple—political, economic, military, and symbolic.

This report emphasizes throughout that it is exceedingly difficult to foresee and plan to cope with any specific terrorist act. The nation must make efforts to deter such acts and, when that is not possible, to counter and minimize terrorists' actions. For example, since good intelligence is extremely difficult to acquire, it may be useful for the academic community to study terrorist recruitment techniques, organizational modes, and methods of operations (such as choice of targets and weapons). This is only one of the areas to which social science research can make a useful contribution. Given that terrorists may arise from many cultures and be motivated by a range of attitudes, studying the phenomenon of terrorism from a social and behavioral perspective could help to interpret fragments of intelligence information, to broaden understanding of terrorists' modes of actions,[1] and perhaps ultimately tell us how to curtail such actions. In this report, however, the committee constrains itself to discussing people as the primary target of terrorists. This chapter shows how the behavioral and social sciences can provide knowledge of and insights into the responses of individuals and organizations to the threat of terrorism and to terrorist events.

[1]Chapter 10 discusses the importance of modeling terrorist decision making as an input for understanding vulnerabilities of critical infrastructures and systems and the effectiveness of proposed ways to mitigate those vulnerabilities.

HUMAN POPULATIONS AS TARGETS OF TERRORISM

Vulnerability of People

Some possible terrorist agendas involve more-or-less direct assaults on human life as a primary objective. These include the following:

- Bombing of human assemblies at sporting events and other mass gatherings;
- Attacks on large cities using nuclear weapons;
- Assaults on toxic/explosive storage and production sites;
- Assaults on water systems;
- Bombing of mass-transit systems, particularly at rush hour;
- Bombing of hospitals and day-care centers; and
- Biological, chemical, and radiological contamination.

Attacks such as these blend into attacks that involve the possibility of human deaths but whose primary objective is to disrupt institutional functions and social processes. Examples of the latter type of attack include the following:

- Destruction of reservoirs;
- Disruption of transportation and distribution systems; and
- Disruption of energy systems.

Still other types of assault do not involve expectations of physical casualties but may inflict incidental harm on humans:

- Disruption of financial and market institutions;
- Disruption of communication, data, and identification systems; and
- Assaults on symbolic targets such as the Statue of Liberty or the Washington Monument.

Institutional, Group, and Political Vulnerability

Understandably, our initial impulse in thinking about the human consequences of terrorist attacks is to envision casualties—the numbers of people killed or wounded, as well as the emotional wounds to their families and loved ones. But there are several other dimensions of societal vulnerability as well, springing from the fact that not only is society made up of people but that people are organized in relation to one another in complex ways.

Institutional Interdependence

Throughout this report the committee recognizes that the targets of potential attack—transportation, communication, and energy systems, for example—are systemically related, and that an attack on one spreads to and perhaps cripples others. This principle of "systemness" applies to the organization of human life as well. It has been recognized for more than two centuries—notably in the work of Adam Smith (1937 (1776)), Herbert Spencer (1897), and Émile Durkheim (1949 (1891))—that as commercial, technological, and industrial development proceeds, social activities become progressively more differentiated and at the same time more mutually dependent. This is readily recognizable in the case of economic specialization, wherein the sites of production (firms, service agencies) come to be organized separately from the sites of consumption (households and organizations). This principle applies to other institutional spheres as well. In premodern times the family assumed responsibility for educational, medical, and welfare functions that have since become structurally separated and now reside in schools, hospitals, and government agencies.

Differentiation and mutual dependency constitute sources of vulnerability. The crippling of an industry responsible for vital products (such as food) or of the financial, medical, or legal system can injure (through deprivation) all those who are dependent on it and cannot readily perform its activities themselves. The effects can be even more serious if the damage is widespread, when repairing, rebuilding, or replacing lost functions may become long-term matters.

The Group Dimension

The growth of a complex industrial and service-based society not only leads to differentiation of social roles and of the institutions that directly affect individuals, but it also makes for a more complex *group* life. A panoply of groups based on economic interest—such as business groups, professional associations, and labor unions—sometimes cooperate with other groups and sometimes come into conflict with them. Modernized societies also evolve a system of social classes that crosscut associational life. Historically, the class dimension has not been a prominent feature of American society (as it was in many European societies), but during periods of labor disturbance such as the Great Depression, class interests have become more salient. Finally, the United States is characterized by many groups based on religious, ethnic, and racial identity, deriving historically from the heritage of slavery and waves of immigration that continue up to the present. These groups constitute bases for community association as well as social and political identity. Historically, relations among them have been variable as well, encompassing friendliness, accommodation, competition, latent tension, and, occasionally, open conflict and violence.

The point to be made here in connection with major terrorist attacks is that the group divisions in the country constitute fault lines that can become more unstable in periods of attack and recovery. Later the committee will comment on the opposite tendency—to pull together and show solidarity in the event of external attack—but if attacks are widespread or catastrophic they may generate scarcity, feelings of unjust treatment, and social disorder. If this is the case, existing group cleavages, as well as new ones that may arise as a result of attacks, can worsen internal conflict in the society. This is all the more likely if the agencies responsible for maintaining law and order are damaged and disrupted.

Political Apparatus

The last observation in this section points to one of the most vulnerable institutions—the political apparatus. The committee is aware that top national leaders are being protected: In times of crisis it is imperative for the government, as the centralized body responsible for maintaining the society and coordinating domestic operations and military activities, to be kept intact. The idea of disrupting our system of government is attractive, as the mailings of anthrax to various political leaders illustrated. While these incidents did not actually harm any political leaders, or even disrupt the government process for any significant period of time, they did illuminate the nature and possible consequences of future incidents. The disablement of multiple government operations by whatever means could trigger military, economic, and law enforcement failures.

While the protection of our top leaders and the continuity of our present federal structure is a priority, we must not overlook the importance of regional, state, and local government entities and their preservation. Local responses to attack must be coordinated by multiple levels of government and private sector organizations, and the efforts must all be integrated.

THE UNIVERSALITY OF HUMAN RESPONSES

Despite variations in directness of attack—whether on humans or on human institutions—and despite overlap among types of attack, *all* attacks generate behavioral, attitudinal, and emotional responses in the populations affected. The committee therefore concludes there is a human dimension to every type of terrorist attack, with each type evoking its own associated responses.

The human response to crisis situations can be influenced by factors such as adequacy of preparedness, effectiveness of warnings, and confidence in agencies designated to deal with crises. However, because it involves attitudes and feelings, it cannot be fully controlled by the state, planning authorities, or other agencies. Nor should it be. In a democratic society, we would not *want* such total control, for the reason that attempting to apply it would involve unacceptable intrusions on citizens' freedoms.

Human responses need to be examined at four distinct stages of the attack process: (1) anticipatory attitudes, emotions, and behavior; (2) responses to warnings; (3) immediate responses to the attack itself; and (4) recovery. The remainder of this chapter addresses each of these stages in turn.

ANTICIPATION AND PREPAREDNESS

The possibility of terrorist attacks on the United States has been appreciated for decades, and before September 11 there had in fact been an accumulation of incidents abroad (e.g., bombings of embassies, the attack on the USS *Cole*) and at home (the Unabomber, the Oklahoma City bombing, the bombing of the World Trade Center in 1993). However, September 11 brought the nation dramatically into an "age of terrorism," and it conditioned reactions to all that might follow. Public apprehension is now much greater than before, and reactions to future terrorist events will be strongly affected by the memory of September 11 and its aftermath.

Preparedness for attacks involves two sets of actors—the responsible authorities and the population in general. Government preparation should attempt to be exhaustive and conditional—trying to anticipate every conceivable kind of attack, understanding probable ripple effects, thinking in terms of multiple attacks, preparing proper responses for agents who would give out information in crisis situations, detailing the roles of first-line response agencies such as police and rescue agencies, and developing a range of backup responses to contain damage and minimize future damage. These measures also call for new levels of cooperation among government entities, the media, schools, businesses, hospitals, churches, and other entities large and small, including households. Applied research on all these aspects of preparedness, conducted in advance, would be a wise investment.

In general, each relevant social unit in the country (communities, cities, states) should make an informed effort to establish priorities for preparedness efforts based on its most likely vulnerabilities. And while each unit should prepare well for a range of possible assaults, it should not try to prepare for all conceivable kinds of assaults. To invoke an analogy, it makes sense for California cities to prepare for earthquakes and fires in the dry season, but not for tornadoes and hurricanes; it makes sense for some Southern states to prepare for the latter two but not the former two. Similarly, cities should prepare for a different range of terrorist activities than agricultural regions. Each unit should establish its priorities by devising scenarios for the attacks most likely to affect it. In devising these scenarios, the units should consult widely not only within their ranks but also with units at other levels, both above and below.

It is likely that the following general principles will hold with respect to how the populace anticipates an attack:

- The longer the time between an attack and subsequent attacks, the greater will be the human memory-lapse and denial. It is not psychically economical for people to worry about rare events all the time; the reluctance of populations in earthquake-vulnerable areas of the world to organize their daily lives around the possibility of a serious earthquake traces in large part to the infrequency of such events. (It also might pay to recall the high-profile, sometimes-hysterical movement in the 1950s and 1960s to protect against fallout in the wake of a nuclear attack. Despite encouragement both by government and media, only one in every 100,000 people actually built some sort of fallout shelter (*New York Times*, Week in Review, December 23, 2001, p. 12)). This slippage of public apprehension works its way into public opinion, and the resulting complacency may become an obstacle to maintaining readiness. The desired but difficult-to-achieve equilibrium is to keep public consciousness high without whipping up public anxiety.
- Making information available about the possibilities of an attack will raise the level of public anxiety.
- Making information available about measures taken to prevent or defend against an attack will tend to lower the level of public anxiety.
- The more information that is made available about how to behave in the event of different kinds of attacks (including readiness training and drills, for example), the more likely it is that people will have a sense of control over uncertain situations and that they will be less anxious. As much unambiguous information as possible should be disseminated about different kinds of attacks—information that is clear, placed in context, repeated, and authoritative (Mileti, Fitzpatrick, and Farhar, 1990).
- The more people are overtrained (with repeated instruction about appropriate behavior in response to many different kinds of attacks or with constant drills), the more likely they will become indifferent, irritable, and critical of the authorities if no such attacks occur.

As discussed in other chapters of this report, technology has the potential to provide a wide variety of measures to defend against or prevent any given type of attack. Some of these measures, such as sensor networks to improve detection of chemical, biological, or nuclear agents or improvements in the electric power grid, will be complicated institutional or national efforts, but other relatively simple measures can be taken by individuals, such as making sure they have backup water supplies and flashlights. For people to be most reassured about the safety and preparedness of the nation, they should be given information about both types of defenses (what the government and others are doing to protect the nation *and* what they can do to protect themselves).

WARNINGS

Warning systems, too, demand a delicate balance. Authorities should strive to make warnings free of ambiguity, directed to all who are at risk (wherever they may be), and available through multiple channels—public warning devices such as sirens, radio, television, and the Internet (Working Group on Natural Disaster Information Systems, 2000). False alarms and misdirection of warnings to people not at risk, however, generate the same negative consequences as overtraining.

Warnings may take the form of public statements that, based on intelligence information, an attack is possible or even likely on a given date or within a given span of time. Alternatively, the warning may state unequivocally that an attack is about to happen immediately or is under way. In either case, the following principles may be expected to hold:

- The better prepared and "programmed" people are about how to respond to an attack, the less likely will be extreme behavioral reactions such as terror, random flight, and panic (Liu et al., 1996).
- Warnings about impending attacks that do not occur could cause a cry-wolf syndrome, especially if the warnings occur repeatedly. Similarly, people who are warned but are not at risk will ignore or become blasé about warnings; some may even try to disable warning devices (Working Group on Natural Disaster Information Systems, 2000, p. 18).
- Under some conditions of warning (e.g., to evacuate a city), people will not follow instructions immediately but will move first to make contact with or join family and loved ones (Killian, 1951).

Recommendation 9.1: Warning systems should be carefully designed with respect to who issues the warning, optimal lead time of warning, unambiguous language, and moderated emotional tone.

When feasible, warnings should also include specific instruction about what kind of behavior is appropriate under the circumstances (stay at home, go to designated locations, evacuate the city using designated routes, or use only bottled water, for example).

Recommendation 9.2 (Research): Comparative empirical studies of past disaster and terrorism situations should be undertaken to gather information that increases understanding of what past actions resulted in (1) effective warnings; (2) failures to warn; (3) false alarms; and (4) overwarning.

Data gathered from past events could also be used to develop models that might help predict the effects of different types of interventions in the future.

THE OCCURRENCE OF ATTACK

Immediate behavioral and emotional responses to attack are difficult to predict, in part because there are so many *types* of attack. It is possible, however, to specify some dimensions of attacks, each of which conditions the nature of the response:

- The suddenness of the attack: from immediate and unanticipated (e.g., bombings) to slowly unfolding (the spread of infectious viruses).
- The scope of the attack: highly localized (e.g., the bombing of one building) to broadly destructive (such as the successful disruption of much of the nation's electric power system or the explosion of a nuclear device over or in a metropolitan center).
- Whether the attack is a one-time event or there are multiple attacks.
- If attacks are multiple, whether spacings are regular, irregular, or random.
- Whether the attack is local (e.g., the isolated attack on a fuel pipeline) or general (release of an infectious virus or toxification of mail or currency).
- The level of knowledge about the agent of attack: known, suspected, unknown, unknowable.
- The degree to which a target is symbolically neutral (e.g., the blowing up of a railroad track) or symbolically charged (bombing of the White House or the U.S. Congress).
- The degree to which an attack appears to be grossly inhumane (e.g., attacks on innocent urban populations, attacks on children).

Because of this variability, the principles involved have to be advanced with a sense of contingency, not certainty, and in an other-things-being-equal spirit. That caution ventured, the following principles, based on best-available behavioral and social science knowledge, can be enunciated:

- Outright "behavioral" panic will be rare. It is most likely to occur under special conditions when escape routes are clogged or believed to be closing, and if people learn (or it is rumored or imagined) that there is only limited time to escape (Quarantelli, 1977). Some scenarios for panic would be attempting to escape entrapment in a building, trying to evacuate a metropolitan area under crisis conditions, and fleeing from an assault on a mass gathering in a stadium or arena.
- Psychological panic (fear, hysteria, terror) is more likely, and its intensity will vary according to the level of uncertainty about the scope of the attack, its duration, the degree to which it is to believed to be general, and the agent of attack.
- The more multiple or random the attacks, the greater the level of public terror.

- The more certain the knowledge about the agent of attack, the more likely it is that outrage and a call for retaliation will stand out from other behavioral and emotional reactions.
- The more the attack is seen as inhumane, the more likely it is that the public will feel sadness, depression, and rage.
- The greater the clarity of information communicated about the nature of the attack—along all of the dimensions above—the weaker will be any fear and terror reactions.
- The better the fit between that information and the previously established preparedness procedures and routines, the less likely there will be extreme emotional responses and disorganized behavior and the more orderly the withdrawal, help-seeking, rescue, and other coping behaviors.
- The greater the degree to which the target is symbolically laden (e.g., sacred), the greater the shock and anger in relation to other emotional responses.

Information and the Media

All these principles apply to the social-psychological perceptions of an attack that result from the adequacy or inadequacy of knowledge about the situation. These perceptions derive from interpersonal communication of information, the spread of rumors, and above all the immediate reporting and interpretations of the event by the mass media.

The media play an important role in defining the nature, scope, and level of threat in critical situations, in disseminating both reliable and unreliable information, and in calming the population or generating extreme reactions such as anxiety and terror. This truth has become even more evident as technology now permits instant worldwide dissemination of news and opinion. A special responsibility for reporting and dissemination seems to attach to events that are immediate, threatening, and easily generalizable.

The role of the media is double-edged. On the one hand they can displace informal and uncontrolled flows of information with accurate, timely, and authoritative reporting. On the other hand they can be conduits—and multipliers—of misinformation if they report soft "facts" and unconfirmed rumors, often in the rush of trying to scoop competitors. Indeed, the media can inadvertently change the basic dimensions of an attack. The widespread reporting of the anthrax contamination in the weeks after September 11 served to expand those events from several localized incidents into a potential generalized threat. All this underscores the crucial roles of both the mass media and authoritative sources such as the police and political leaders in giving definition (psychological reality) to an attack. It also underscores the great need for responsibility and prudence on the part of these entities in moments of crisis.

Recommendation 9.3: Representatives of the major media should consider developing—voluntarily—a code of norms that they would observe in reporting events related to terrorism.

Such efforts are not without precedent. For example, most newspapers and other media exercise great care in protecting the privacy of child crime victims. The media usually refrain from identifying the victim or giving away personal particulars. A similar code could be developed for terrorism-related incidents that while only slightly restricting the amount of information being reported, would not compromise the investigation of the incident or oversensationalize it. For the media to address these issues voluntarily would keep them from government control and recognize the special responsibilities that they bear.

While the media have an obligation to the public and to the government to try to disseminate information as efficiently and accurately as possible, the government has the responsibility to provide such information to the media and the public as efficiently and accurately as possible. In the same ways that federal agencies are preparing technological responses to possible attacks (e.g., stockpiling vaccines), the government must also be preparing the informational response. Who will be able to speak with authority when a terrorist attack occurs, i.e., who will be a trusted spokesperson for the public? The answer of course depends on what sort of attack takes place and the type of information to be communicated. For example, in a radiological event (a dirty bomb), the Surgeon General might be the right person to speak on how to minimize radiation exposure,[2] while in a biological attack, someone from the Centers for Disease Control or perhaps the Surgeon General might be the right person to describe steps people can take for self-protection (e.g., the use of simple breathing masks to filter the air, whether to stay inside).[3] In many types of attack, someone from FEMA might be the right person to announce evacuation plans and routes if necessary. In all cases, identification and training of these potential spokespeople should occur before an attack takes place, so the government can respond not only by providing emergency services but also by providing important, accurate, and trustworthy information clearly, quickly, and authoritatively.

First-Line Responders to Attacks

The differentiation and mutual dependence, or "systemness," in contemporary society, mentioned earlier in this chapter, apply as well to the numerous agencies responsible for maintaining law and order, protecting the society from

[2]The need for a trusted spokesperson is especially important for events relating to nuclear and radioactive materials; see discussion in Chapter 2.

[3]One factor that must be considered is the perception of political motivation: Will the spokesperson be distrusted because he is perceived as having political authority rather than technical expertise?

attack, responding to attack, and recovering from attack. The actions of these multiple agencies must be integrated and coordinated if they are not to be fragmented and ineffective. Nowhere is this truer than in the initial responses to attack, when quick decisions and direct actions are required. The accumulated body of research on natural disasters reveals all too many instances of scarce information, deficient communication, poor coordination, and jurisdictional conflict among nominally coordinating organizations (Kreps and Bosworth, 1993; Tierney, Lindell, and Perry, 2001).

Coordination is complicated because it involves agencies at different levels, from federal to local, and different types of government and private agencies. It is also complicated because once a disaster occurs, informal new groups come into being—often under conditions of extreme confusion—and must be taken into account by those officially designated as responders (Drabek, 1986). In his first press conference after assuming federal responsibility for homeland security, Governor Tom Ridge properly called attention to the seriousness of the issues of overlap and coordination among government agencies. The committee knows of no more important and pressing concern with respect to effectiveness of response.

For all stages of the attack circumstance—preparedness, warning, attack, and recovery—agencies responsible for aspects of any of them should coordinate their assignments as closely as possible. This means knowing how to act when different kinds of attacks occur, how to cooperate, and how to communicate. It also means continuously reviewing each agency's jurisdiction relative to that of others and refining responses in the light of as many hypothesized scenarios as can be developed. It also means planning for rigorously monitoring and correcting the coordination process in midcourse, as required by the specifics of the crisis. The need for such coordination and backup is especially critical in attacks when some response agencies are themselves disabled.

Recommendation 9.4: Agencies designated as responsible for the preparedness, warning, attack, and recovery phases of the government's counterterrorism activities should coordinate their responsibilities as closely as possible.

Recommendation 9.5 (Research): There should be a deepening of research—basic, comparative, and applied—on the structure of agencies responsible for dealing with attacks and other disasters, on the optimal patterns of information dissemination and communication among them, and on the most effective strategies of coordination—and self-correcting of coordination—under extreme conditions. Research should also focus on the origins and consequences of organizational failure, miscommunication, lack of coordination, and jurisdictional conflict and on the impact on public confidence when organizations fail to act.

Many factors, including overlapping and unclearly defined missions for existing agencies and complex regulations prescribing the scope of agency activities, affect agencies' ability to carry out key functions such as hiring personnel with appropriate expertise and training them and coordinating with other agencies or other levels of government. A number of fields—including political science, sociology, and organizational management—have important contributions to make to research in this area.

Reactions to Extraordinarily Catastrophic Attacks

The focus of this report is catastrophic terrorism, as defined in Chapter 1, and the principles outlined above describe people's reactions to such terrorist events or the threat of them. However, in the case of extraordinarily catastrophic attacks—such as serial nuclear bombings of cities, destruction of an entire region, poisoning of a large segment of the population, prolonged paralysis of the nation's energy system, or any event in which there are hundreds of thousands (or millions) of casualties—these principles become shakier. The nation has never experienced catastrophes of such severe proportions, so knowledge of the human effects is correspondingly weak. Three general points, however, can be noted:

1. Certainly we can expect magnified reactions of shock, despair, helplessness, and paralysis. The greater the destruction, the greater the likelihood of socially disorganized behavior and the less the likelihood of effective mobilization of people and social agencies.
2. The greater the magnitude of the attack, the more likely that governmental agencies and law-and-order agencies (military, police, fire control) are themselves rendered ineffective or altogether destroyed. Some terrorist attacks—for example, assassinations and the bombing of strategic government buildings—would attempt specifically to confuse and disrupt governmental processes. Others would specifically target response agencies. Extraordinarily catastrophic attacks could wipe out whole systems for response to disaster and disrupt government functioning. Needless to say, without these capacities and without effective backup systems, the seriousness of the attack is multiplied.
3. Research on natural disasters reveals that many of them result in an ensuing period of social solidarity (to be described in several of its aspects below) characterized by mutual help, certain kinds of self-denial, and some reduction in looting and other antisocial behavior (Barton, 1969; Lindell and Perry, 1992). The generalizability of such findings is uncertain, however, and under extreme conditions they may not hold; serious breakdowns of law and order must at least be anticipated. The main reasons for this would be the potentially high degree of resulting social disorganization, together with the disruption of law-and-order agencies. Some research has shown that when local police authorities vacillate or are absent from the scene, urban riots and related behavior such as looting are

likely to spread. Other historical research indicates that one ingredient of successful revolutionary overthrow is the inactivity, complicity, or defection—i.e., the essential absence—of the police and military (Smelser, 1962). Widespread breakdowns of social order also heighten the probability that mutually hostile class, ethnic, and racial groups (the fault lines mentioned earlier) will come into open conflict, especially if different groups perceive that they have been treated unfairly in relation to others. To say all this is not to predict that extreme terrorist attacks will inevitably bring social and political chaos or that recovery will not happen, but given the enormous magnitudes of human reactions and immediate coping efforts in the attacks' aftermath, such possibilities must be considered.

RECOVERY

Recovery-related processes can be discussed under the headings of shorter-term and longer-term recovery to terrorist attack, without attempting to say how many weeks or months either would last.

Short-Term Recovery Processes

Short-term recovery processes can be expected to resemble known developments in other kinds of disaster situations:

- There will be a period of mourning, longer and more difficult if casualties are great, the attack inhumane, or the target a sacred one. This mourning process will become less intense if attacks are repeated and become a way of life.
- A period of collective solidarity—a pulling together of the community affected and, to a lesser degree, of other communities and the nation—will occur. As with mourning, these responses will be weaker if attacks are multiple and repeated.
- There will be a more or less immediate mobilization to clean up the rubble, restore impaired functions as quickly as possible, and generate the requisite economic resources. These activities will become less effective as the number and scope of attacks increase and as greater pressure is put on the resources available.
- People will keep away from areas of vulnerability made evident by an attack. The avoidance of airline travel in the wake of September 11 is an obvious example. If a nuclear power installation is attacked, there will no doubt be heavy public pressure to close others down, even at the cost of reducing the nation's energy supplies.
- If a given function or activity is impaired or avoided, people will turn to alternatives—note, for example, the increase of business after September 11 in all forms of ground transportation. A widespread curtailment of electric power will occasion a run on lanterns, flashlights, batteries, and generators. An impairment

of electronic communications will create a crisis of overload for the telephone system.

- Every attack—whether successful or thwarted—can be expected to enhance efforts to prevent further attacks of the same kind. A simple but telling example is the instituting of random shoe inspections of airline passengers after the aborted shoe-bomber incident in December 2001.
- If the attack is believed to have been avoidable, and the agents responsible for its avoidability are identified or suspected, a season of scapegoating, public investigations of culpability, and calls for punishment will ensue.
- If agencies of public order (police, National Guard, military) and rescue agencies (firefighters, Red Cross, volunteer workers) are perceived to have been ineffective or improperly coordinated, scapegoating will be directed toward these agencies as well.
- Contrariwise, there will be an identification and adoration of heroes in crises. This effect will also decrease if attacks become repetitive.

Most disasters are both sudden and ephemeral, and immediate responses quickly give way to a wide variety of long-term recovery and rebuilding activities. Therefore research on immediate disaster responses generally relies on hastily assembled journalistic reports and after-the-fact accounts based on participants' recollections. Both types of sources are subject to selectivity and distortion. Teams of behavioral and social science researchers collecting data on the spot and analyzing it in the context of established knowledge about disaster situations would supplement and likely improve on existing ways of generating information about disaster response. Some universities have a tradition of such fire-brigade research, but efforts should be made to expand and systematize it.

Recommendation 9.6 (Research): Relevant research agencies (universities, think tanks, or government) should establish the capacity to move quickly to the scene of a disaster and study immediate responses *while they are occurring*.

Analysis of preparedness, warning, and response tends to rest on the assumption of an undifferentiated community or public. Research on disasters, however, has revealed that individuals and groups differ both in readiness and response according to previous disaster experience, ethnic and minority status, knowledge of the local language, level of education, level of economic resources, and gender (Tierney, Lindell, and Perry, 2001). Research on these and other differences should be extended and deepened, and it should be taken into account when designing systems of preparedness, warning, and response to terrorist attacks and other disaster situations.

Recommendation 9.7 (Research): Research on how different individuals and groups prepare for and respond to crises should be extended and deepened.

Long-Term Recovery Processes

Longer-term recovery periods will more explicitly involve political, economic, and cultural considerations.

Political Aspects of Recovery

A postattack period of political solidarity parallels the burst of social solidarity noted above. Citizens express increased trust and support of political leaders, and this condition may endure for a long time if a sense of crisis continues and it is perceived that leaders are dealing with it well. The most dramatic evidence of this effect came from the polling of African-American citizens in late December 2001: Results revealed 75 percent support for President George W. Bush in a segment of the population that had cast only 10 percent of its votes for him one year earlier. Such support does not last indefinitely, however, as demonstrated by the fate of his father, President George H.W. Bush, after the Gulf War.

Political leadership also pulls together in such times of crisis, particularly if the crisis involves an attack on the nation as a whole. This effect is not necessarily seen in other types of crises, such as a severe downturn in the domestic economy or major political scandals, which typically set off both class and party conflicts.

Partisan politics are quick to return, however, even in areas that have some connection with the crisis. It was less than 2 months after September 11, 2001, when Democrats and Republicans split along recognizable lines over the issue of whether airline security personnel should be federal employees or remain as private sector employees. By December, the *New York Times*, in summarizing the national situation, quipped that "the Democrats and Republicans are fighting about everything but terrorism" (Week in Review, December 23, 2001, p. 1). Apparently this effect is a general one. In 1689, after the semiforced departure of the Catholic King James II and the succession of William of Orange, a Whig political leader observed that "fear of Popery has united [Whigs and Tories]; when that is over, we shall divide again" (O'Gorman, 1997, p. 43).

Four other political possibilities must be mentioned:

1. *Tension between the exigencies of national security and the preservation of civil liberties.* This tension is real and perhaps inevitable in times of political crisis. The two sets of considerations pull in opposite directions. Three foci of tension after September 11 were (1) the detention of immigrants; (2) the use of military tribunals for trying apprehended terrorists; and (3) the practice of ethnic profiling in checking and searching for suspects. This tension between vigilance and liberty is of special significance in the context of American democracy, given its long-standing commitment to individual rights.

2. *Discrimination against and scapegoating of related minority groups in*

the domestic population, sometimes encouraged or even executed by the government. The actions taken against German-Americans during World War I and the more drastic measures taken against Japanese-Americans during World War II are the obvious cases in point. Since September 11, neither the government nor the populace has turned visibly against Muslim-Americans, except for some local incidents. The crisis has created uneasiness and ambivalence in that sector of the population, however, despite exhortations in government and media circles for tolerance. Though a sense of comfort and pride can be gained from that posture of moderation on the part of government, press, and the public, it should not be assumed that the issue is permanently closed. Successful terrorist attacks in the future, especially major ones, or evidence or suspicion of terrorist activities on the part of Muslim-Americans, could quickly excite a season of pointed, even explosive, group antagonisms.

3. *Confusion of political opposition with lack of patriotism.* During national crises of the sort now being experienced, opposition parties and groups manifest unusual solidarity with top national leaders. The engine that drives this trust and cooperation is patriotism—love of nation. Two factors tend to maintain this diminution of partisanship, at least for a while: (1) a temptation on the part of the leaders and the party in power to play their political trump card by claiming or insinuating that the political opposition is not loyal and (2) the tendency for the opposition to drift toward self-imposed muteness out of apprehension that voters in their own districts may also confuse opposition with lack of loyalty.

4. *Extremist political movements.* An extension of these three tendencies can produce nationally disruptive political movements that excite accusations of disloyalty during periods of real or exaggerated threats. There is nothing inevitable about the development of such movements, but it is worth recalling two disturbing episodes of stereotyping and group punishment in the 20th century: (1) the Red Scare of the early 1920s, in which government intimidation and actual raids were carried out in the context of a national fear of Bolshevism and (2) McCarthyism in the late 1940s and early 1950s, which arose from a high state of national anxiety over the development of nuclear explosives and weaponry by the Soviet Union and the fall of China to communism. Both movements, while limited in duration, seriously compromised the civil liberties and livelihoods of some citizens and left ugly scars on the body politic.

Raising these four possibilities is in no way meant to predict that any will materialize as the nation struggles with its current situation. But it would also be unwise to put them out of mind altogether.

Economic Aspects of Recovery

Some potential terrorist targets are economic in nature. The disruption of the stock market, the paralysis of credit systems, and the contamination of currency

with toxic or infectious agents come to mind. While potentially very damaging in the short run, these types of attacks—except perhaps the last—could reasonably be envisioned to show rapid recovery.

Other direct economic consequences include the costs of rebuilding what has been damaged or destroyed. Depending on the scope and success of attacks, these costs can be very significant. The full cost of replacing the World Trade Center (including compensation for survivors) and the damaged portion of the Pentagon will be enormous, as would be the costs of replacing destroyed dams or severely damaged electric power systems. Once capital resources are raised and put to work, however, reconstruction projects take on the same stimulating significance for the economy that public works projects often do.

Assessment of the indirect economic consequences of terrorist attacks is a more complicated matter, in part because of the great diversity of possible targets. The overall economic losses generated by the September 11 attacks, while evidently severe, are difficult to establish, all the more so because the national economy had already entered a downturn. But in general, economic dislocations from discrete terrorist activities should be expected to obey the laws of routinization—however slowly in some cases—as people in the affected parts of the economy gradually return to their normally preferred lines of activity and expenditure.

Another indirect economic effect of national trauma is the process of capitalizing on public crisis for private gain. The plea on the part of airline companies for relief is not exactly a case in point, because the losses they suffered after September 11 were genuine; nevertheless, the possibilities of turning relief into gain are always present. The need to gird up for all aspects of counterterrorism will inevitably set off a scramble for government contracts in parts of the economy. This pattern was observable in past wartime situations: It persisted throughout the Cold War and it is likely to reappear during the coming years.

Prevention in particular looms as an extremely costly enterprise. Preventive measures may be sought at three points in the terrorist process: (1) at the source—that is, by seeking out and destroying terrorists where they live; (2) at the end of the line, by erecting defenses and hardening all known or conceivable targets; and (3) along the way, between source and event, by controlling movements of people and weapons at national borders and other points of entry.

The at-the-source alternative is attractive because, if successful, it prevents *all* sorts of terrorism. On the other hand, intelligence and military operations of this sort are very costly and constitute a significant drain on the nation's resources; it is also impossible to assure that eradication efforts will ever approach anything like completeness, given the secrecy and mobility of terrorists and their networks. In addition, even if eradicated, terrorist activities and organizations can regrow.

The attractiveness of the along-the-way strategy is similar, in that it intercepts persons with a possible diversity of purposes. But in this case as well, both

the cost and the impossibility of completeness are evident, given the vast movements of people and things that global commerce and tourism entail.

The attractiveness of the end-of-the-line strategy is the promise of direct security, but the multiplicity of possible targets (and the adaptive capacity of terrorists to shift them under changing circumstances) also raises the issues of cost and the impossibility of completeness.

Considerations of strategic prudence and the force of public opinion will probably dictate that the country pursue all three lines of prevention, albeit imperfectly, and settle for as much reduction in the probabilities of attack as possible. This will come at great cost to the nation. Prospects for continuing governmental budgetary surpluses over the next several years have all but evaporated, and even if assisted by other nations, the United States will likely bear the greatest part of the economic burden.

Within the United States, the question of who pays will be a continuous one. Even under normal circumstances, U.S. politics is fraught with ambiguities and conflicts over the respective costs to be borne by federal, regional, state, and local authorities. The defense against terrorism promises to make the uncertainties even more salient. Furthermore, while the fight against terrorism is manifestly a public and governmental responsibility, many if not most of the targets of terrorism are in the private sector. Given all these intersections, who prepares and who pays? More rational and less rational solutions to these dilemmas can be designed, but the nation must expect a significant residue of tugging and hauling, jockeying for position, and resentments over perceived off-loading.

Two other sets of derived consequences, also of uncertain dimensions, lie on the horizon. The first is the effect of a continuous, quasi-wartime effort on the balance and strength of the U.S. economy. Such an effort will involve significant reallocation of public expenditures and capital among different industrial sectors (especially those connected with defense), the prospect of governmental budgetary deficits, some impact on the pattern of imports and exports, and perhaps a greater sensitivity to inflation.

The second is the prospect of giving lower priority to some expenditures for programs in education, health, welfare, environmental protection, and other areas in the face of more urgent demands for military and homeland and defense expenditures. War efforts typically slow the progress of social programs (demands for which often follow wars in a flurry). The quasi-wartime exigencies associated with counterterrorist activities promise to be no exception.

Normalization and Cultural Memory

The natural history of recovery from disaster involves a diminution of emotional responses, a denial of the possibility of recurrence, and a return to routine activities, events, rhythms, and conflicts. These are, by and large, reasonable and

adaptive responses on the part of a population, because large-scale disasters are so rare.

Discrete acts of terrorism, if not soon repeated, should be expected to show the same tendency toward routinization. Indeed, we received messages from government and public leaders exhorting us to return to normal activities in the wake of the September 11 attacks, while at the same time stressing the need for vigilance and even warning of potential impending attacks.

Because terrorist attacks tend to be sudden, surprising, and of short duration, they are usually regarded as discrete events. In reality, however, they build upon one another, and any new attack is read, variably by different groups, in the context of the past history of such events.[4] One of the interpretative frames for reacting to the airborne attack on the World Trade Center, for example, was the memory of the unsuccessful effort to destroy it in 1993 by bomb planting. Reactions to anthrax episodes were strongly conditioned—and exaggerated—by their occurrence so soon after September 11.

Recommendation 9.8 (Research): Historical research on the interrelated sequencing of reactions, interpretations, and memories of terrorist events should be undertaken to deepen our theoretical and empirical understanding of those phenomena. Conceptual models such as path dependency (employed in economics and other fields) and the logic of value-added would guide the framing and conduct of this kind of research.

One final comment on the cultural uniqueness of the September 11 attacks should be ventured. Because those attacks were so dramatic and such a profound wound to the nation, they qualify as what social scientists and humanists recently have been calling a cultural trauma. Within a matter of days after the assault, it was appreciated in all quarters that these events would embed themselves deeply in the nation's memory and endure indefinitely. Unlike some other cultural traumas that are mainly negative—assassinations of national leaders or episodes of ethnic cleansing—September 11 already emerges not only as a deep scar on the nation's body but also as a moment of extreme heroism and pride. In the wake of the events, the nation has simultaneously experienced both deep mourning and a not-altogether-expected season of celebration.

A cultural trauma of this type can be expected to manifest a number of known characteristics:

- Indelibility, not only not forgotten but also incapable of being forgotten;
- Sacredness of the event, not in any specific religious sense but as a monumental instant in the history of the nation;

[4]The issue of repeated attacks and their consequences for behavioral reactions has been mentioned—less extreme reactions, greater possibilities of scapegoating and political protest, and a certain hardening of public attitudes.

• Deliberate efforts to remember the event and its heroes collectively, through commemorative ceremonies, public observation of anniversaries, and the erection of monuments; and

• Sustained public interest in the remembering process, including, down the line, some contestation among politically interested groups over *how* the remembering should be done.

Some future attacks may be of such magnitude and drama as to constitute additional cultural traumas for the nation. Even these, however, will be read and remembered in the cultural context established by September 11.

REFERENCES

Barton, Allen H. 1969. *Communities in Disaster: A Sociological Analysis of Collective Stress*, Doubleday and Co., New York.

Drabek, T.E. 1986. *Human System Responses to Disaster: An Inventory of Sociological Findings,* Springer-Verlag, New York.

Durkheim, Émile. 1949. *The Division of Labor in Society* (translated by George Simpson, originally published in 1891), The Free Press of Glencoe, New York.

Killian, L.M. 1951. "The Significance of Multiple-Group Membership in Disaster," *American Journal of Sociology*, Vol. 57, pp. 309-314.

Kreps, G.A., and S. I. Bosworth. 1993. "Disaster, Organizing, and Role Enactment: A Structural Approach," *American Journal of Sociology,* Vol. 99, pp. 428-463.

Lindell, Michael K., and Ronald W. Perry. 1992. *Behavioral Foundations of Community Emergency Management*, Hemisphere Publishing Corporation, Washington, D.C.

Liu, S., L.E. Quenemoen, J. Maililay, E. Noji, T. Sinks, and J. Mendlein. 1996. "Assessment of a Severe-Weather Warning System and Disaster Preparedness, Calhoun County, Alabama, 1994," *American Journal of Public Health,* Vol. 86-89.

Mileti, D.S., C. Fitzpatrick, and B.C. Farhar. 1990. *Risk Communication and Public Response to the Parkfield Earthquake Prediction Experiment*, Hazard Assessment Laboratory, Colorado State University, Fort Collins, Colo.

New York Times. 2001. "Armageddon Then and Now," Week in Review, December 23, p. 12.

New York Times. 2001. "Headlines from the Cutting Room Floor," Week in Review, December 23, pp. 1, 4.

O'Gorman, Frank. 1997. *The Long Eighteenth Century: Political and Social History 1688-1832*, Arnold Press, London.

Quarantelli, Enrico L. 1977. "Panic Behavior: Some Empirical Observations," *Human Responses to Tall Buildings,* Dowden, Hutchinson and Ross, Stroudsburg, Penn.

Smelser, Neil J. 1962. *Theory of Collective Behavior*, The Free Press, New York.

Smith, Adam. 1937. *An Inquiry into the Nature and Causes of the Wealth of Nations* (1776), The Modern Library, New York.

Spencer, Herbert. 1897. *The Principles of Sociology*, D. Appleton and Company, New York.

Tierney, Kathleen J., Michael K. Lindell, and Ronald W. Perry. 2001. *Facing the Unexpected: Disaster Preparedness and Response in the United States*, Joseph Henry Press, Washington, D.C.

Working Group on Natural Disaster Information Systems (Subcommittee on Natural Disaster Reduction). 2000. *Effective Disaster Warnings*, National Science and Technology Council, Office of the President of the United States, Washington, D.C.

10

Complex and Interdependent Systems

INTRODUCTION

The previous chapters of this report call for the use of systems analysis and systems engineering in countering terrorism. This effort can draw on bodies of knowledge already available in the United States and applicable immediately to dealing with terrorist threats. For example, DOD, NASA, and various intelligence agencies have directed systems techniques to highly complex, but ultimately successful, military and aerospace applications dating all the way back to the Apollo and Strategic Submarine programs and continuing to this day. Additionally, the Environmental Protection Agency has developed a methodology for risk analysis and prioritization of environmental threats, and private-sector analysts—in the financial services (www.riskmetrics.com) and geophysical exploration (MacKay, 1999) industries, for example—have used a wide variety of risk modeling and other systems methodologies to manage large-scale global operations.

While none of these techniques is an exact match for the counterterrorism challenges described in this report, there appears to be considerable near-term potential to extend these techniques to provide a strategic framework for addressing these threats. One near-term example is in the integration of current infrastructure models. DOD's Modeling and Simulation Office and DARPA, for example, have developed procedures and algorithms for distributed simulations that take advantage of multiple existing simulation capabilities in different organizations and include them in a broader framework to address questions that could not have been answered by any one of the simulation systems individually. These techniques have the potential to be adapted to a variety of models (cur-

rently or soon to be available) in areas of threat modeling and critical infrastructure to provide near-term improvements in developing vulnerability assessments and risk mitigation strategies.

Currently, however, the U.S. government's departments and agencies are in no position to make optimal use of available modeling and simulation technologies to support the creation of an overall strategy for their counterterrorism activities. They are not organized to assess terrorist threats, infrastructure vulnerabilities, and mitigation strategies from a systems perspective. Thus, although many initiatives have been proposed since September 11, and some—such as improving airport security, local emergency response, and seaport operations—are in early stages of implementation, they are often proceeding without the benefit of a systems approach. Specific examples of the value of systems approaches are also described in other chapters of this report, particularly Chapter 7, on transportation, and in Chapter 11, on crosscutting challenges.

While an overall systems approach is particularly important in the development of a national strategy for counterterrorism, there exist today models for particular infrastructures within the United States that have been produced by various government agencies and private industrial organizations. Aspects of energy distribution, power grids, air traffic control, and military support infrastructures have been analyzed and modeled to varying degrees of fidelity. In the near term, these models must be extended and expanded to provide better representation of specific critical infrastructures, and the models must be tested and evaluated against real-world data. A program to measure the interactions between various infrastructures must also be established. This effort will rely on determining the connectivity between infrastructures through analyses, model development, data collection, experiments, and model validation. At the same time a more detailed understanding of the implications of various threat scenarios for critical U.S. infrastructures must be established. The committee recognizes that it will never be possible to model the entire U.S. system in finite detail, but we can determine which components of our critical infrastructures are least robust; how an attack on one component of a particular infrastructure affects other systems; and which identified vulnerabilities within critical infrastructures are most vulnerable to a wide range of postulated threat scenarios.

A FRAMEWORK FOR A SYSTEMS APPROACH TO COUNTERTERRORISM

When modeling terrorist networks and homeland systems, knowledge of the associated "architectural" framework—including its characteristic state variables[1]—is essential. In Figure 10.1, threats from terrorist networks constitute a

[1]It should be noted that use of the term "state variable" is somewhat different from its use in, say, mathematics and control theory.

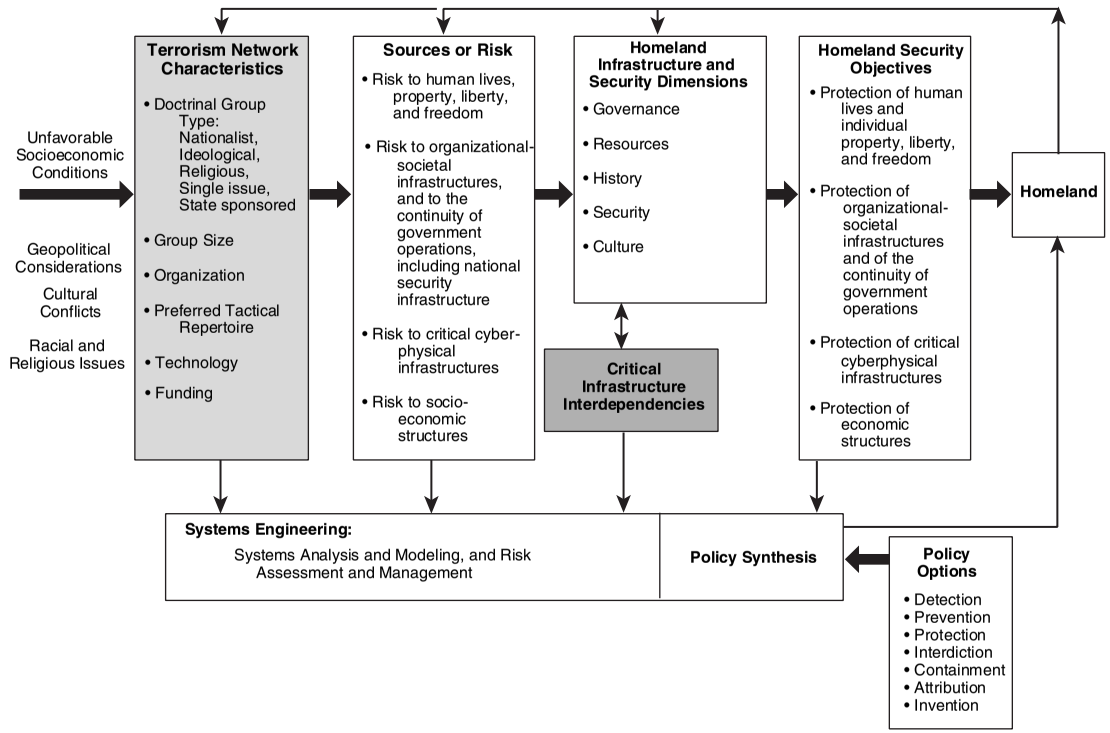

FIGURE 10.1 A framework for a systems approach to counterterrorism. SOURCE: Haimes (2002), p. 37. Adapted from Figure 2 in "A Roadmap for Modeling the Risks of Terrorism to the Homeland," *ASCE Journal of Infrastructure Systems,* Vol. 8, No. 2, June. Copyright 2002 by the American Society of Civil Engineers (ASCE). Reprinted by permission of the publisher, ASCE.

key input. These threats can be understood and modeled only when we identify and understand the societal environment, the geopolitical dynamics within which the terrorist networks are energized and operate, and the characteristics and limitations of the threatened infrastructure. The causal relationships among these inputs and outputs then enable the building of models that predict the efficacy of risk-management policy options.

Understanding counterterrorism as a "system of systems" is essential, because the outputs of the terrorism network, as shown in Figure 10.1, are the same four types of risk that constitute the inputs to the homeland security system. Terrorism network characteristics, the resulting potential sources of risk, and homeland infrastructure and security characteristics all contribute to the comprehensive effort needed to identify conceivable types of risk. Additional characteristics, such as the funding sources of the terrorist groups, the level of sophistication of these groups, and the driving forces that feed them (such as unfavorable socioeconomic conditions, geopolitical considerations, cultural conflicts, and racial and religious issues), are also essential to the risk analysis.

Four major risk classes to homeland security can be identified, as shown in Figure 10.1:

1. Risks to human lives and to individual property, liberty, and freedom;
2. Risks to organizational and societal infrastructures and to the continuity of government operations, including the military and intelligence-gathering infrastructure;
3. Risks to critical cyber and physical infrastructures; and
4. Risks to socioeconomic sectors.

An essential factor for sound decision making is identification of these and other sources of homeland risk at a sufficient level of detail. This will enable effective strategic and tactical planning.

SYSTEMS MANAGEMENT ISSUES

While systems engineering is essential to the successful design, development, and deployment of a complex system (Sage and Rouse, 1999), how well a system is operated once it is deployed is the concern of systems management.

The new Office of Homeland Security (OHS) is developing a strategic plan for the United States that will include the participation of many public and private organizations. To support the development of its plan, the OHS will need an overall management system that takes into account many of the governance, decision-making, and information systems and tools discussed below.

Governance and Decision Making

Lack of a shared understanding of the elements of governance by key stakeholders, especially in cross-organizational decision-making situations, can result in conflicts and possibly stalemates. Worse yet is when, because of ill-specified governance practices, there are critical decisions that no one sees the need for or that no one is responsible for making.

Several governance issues are of particular importance:

- What types of decisions must be made?
- Who can make which types of decisions?
- Who can delegate decision-making authority?
- How is decision making supported?

Often, the overriding question is, "Who decides who decides?" Who can resolve inevitable decision conflicts when multiple organizations perceive responsibility for a particular decision? On the other hand, when there are gaps between organizations, who should assure that key decisions are not lost in those gaps?

This question leads to an obvious issue: the respective responsibilities of various federal departments and agencies on threats to the U.S. infrastructure and, of course, to U.S. citizens and residents. Carter (2001-2002) has outlined the nature of the federal "architecture" for addressing terrorism. He concludes that the U.S. government lacks a managerial category for catastrophic terrorism per se—as opposed to its well-established categories for war, crime, or natural disaster. Further, state and local governments lack the resources and specialized knowledge to combat terrorism.

Thus, government at all levels lacks a framework for bringing responsibility, accountability, and resources together to deliver homeland security against terrorism. As Carter notes, "The federal government disperses executive authority so thoroughly that few individuals believe they are accountable for any of the government's key security outputs." The responsibilities of state and local organizations are similarly dispersed and fragmented.

These issues were recognized long before the terrorist acts of September 11, 2001. Studies of infrastructure vulnerabilities led to Presidential Decision Directive No. 63 (PDD63),[2] which describes these national vulnerabilities and provides guidelines for addressing and eliminating them. Lead agencies and tasks are specified for each of the components of the overall national infrastructure.

---

[2]For the full text of the white paper containing the Clinton administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998, see <http://www.nipc.gov/about/pdd63.htm>.

This sets the stage for addressing governance issues and needs but does not fully resolve them.

Information Systems and Tools

Beyond the important guidance provided by PDD63, as well as its classified companion PDD62, there is a substantial need for management information systems and tools. First of all, as noted by Carter, allocation of responsibilities must be finer-grained than specified in PDD63. The approach to allocation he proposes is characterized in Table 10.1.

Nevertheless, decision-making problems remain. These include overlapping organizational seams, which tend to produce conflicted decisions. Gaps between seams are much more subtle, because they can result in "lost" decisions—those that are simply unrecognized as needing to be addressed and resolved.

Problems of overlapping seams, and of gaps between them, suggest several opportunities for applying science and technology. But solutions should not eliminate those organizational seams, which provide valuable levels of resiliency—the inherent distribution of authority across federal, state, and local agencies, after all, is central to American life. Thus, complete integration is not only quite difficult, it is politically impossible and culturally undesirable.

Means for assessing current and emerging states of distributed responsibility are needed, and computer-based tools can be useful in modeling the decision-forcing phenomena. Such tools can also enable teams to access, create, or manipulate computational models—for example, of relationships and flows. Model building provides a good way to span the organizational boundaries often associated with complex decisions. And because technology currently exists for monitoring, cluster analysis, and portrayal of the nature of e-mails and attachments flowing in large organizations, this idea is by no means far-fetched.

The information systems and tools suggested above are portrayed in terms of technology-enabled capabilities. However, it is important to emphasize the essential need for scientific research, both to provide the knowledge upon which

TABLE 10.1 Agencies and Organizations versus Responsibilities

	Detection	Prevention	Protection	Interdiction	Containment	Attribution	Analysis and Invention
Org 1							
…							
Org N							

these capabilities may be based and to assess the consequences (including the behavioral, social, and economic impacts) of deploying them.

Systems Expertise for the OHS

As stated above, the U.S. government lacks the structure and framework for bringing responsibility, accountability, and resources together to secure the homeland against catastrophic terrorism. Moreover, a federal architect and national systems integrator across all departments and all levels of government is needed to develop and validate operating models in order to provide the prioritized decision making, planning, and training needs of governmental counterterrorism programs.

Recommendation 10.1: In order to define critical infrastructure vulnerabilities and enable better decision making within the federal government on priorities related to counterterrorism, the OHS should utilize a dedicated core of systems engineering and research expertise to conduct systems analyses, systems engineering, risk modeling and assessment, and related model development. This core of expertise should reside in the proposed Homeland Security Institute, the capabilities of which are described in Chapter 12.

OHS is in need of a range of services, including the development or integration of models and databases necessary for critical decision making and possibly the coordination of the design and development of data-acquisition networks to provide the inputs for these models and databases. An organization with all of the relevant expertise—expertise in policy analysis; intelligence collection; research and analysis of terrorist behavior; risk modeling, assessment, and management; threats from information, chemical, and biological warfare; critical infrastructures (such as electric power, communications, finance, water resources, health, food, and other major systems); and database standards and integration—does not exist.

Current modeling capabilities in priority areas for counterterrorism activities need to be assessed such that an overall modeling architecture for modeling and simulation can be developed. This architecture could be based on DOD's previous R&D efforts in this area, and it could be used to determine whether current models should be adapted for the counterterrorism mission or whether new models are required. The outputs from these models would help government agencies answer questions about strategic counterterrorism issues. For example, when the models are used to identify key critical infrastructure risks (e.g., information-security risks in the control systems (SCADA) for the power grid), information would be disseminated to the agencies so that they could undertake programs to mitigate these risks.

Finally, gaps and seams in the overall counterterrorism effort need to be identified such that better interfaces exist among federal, state, and local govern-

ment agencies, as well as the many public and private organizations that have operational responsibilities and relevant information and expertise. Systems analysis should be used as one tool to help identify these gaps and seams.

COUNTERTERRORISM THREAT MODELING[3]

The analysis of terrorist threats is a major input, as shown in Figure 10.1, to the risk analyses that must be performed to establish homeland security priorities. Currently, a large volume of pertinent information is collected by the U.S. intelligence community, but there is much work to do in organizing and integrating the information so it can be used for counterterrorism activites.

This section discusses some of the factors involved in the development of an appropriate risk analysis model. It sketches an illustrative model based on systems analysis, probability theory, and game theory—one that can be used to set priorities among the various threats and threat-reduction measures. These measures include short-term actions such as restricting access to an airplane cockpit; medium-term actions such as the manufacture and stockpiling of vaccines; and long-term actions such as investing in specific areas of scientific research and in the development of new technologies.

Comparison of such options is complicated because of massive uncertainty, but investment decisions must be made nonetheless. To inform such decisions, we first need a system framework that embraces the various infrastructures within the United States, the terrorist system, and their interactions. The committee lays out such a framework, sketches a model that represents it, and describes ways of dealing with uncertainty in the model's variables.

The System to Be Strengthened

An overall system description must describe connections between infrastructures, people, the national economy, and social values. All of these are vulnerable, in part from the myriad of interdependencies and in part from the openness of American society (Gilmore Commission, 2001). This modeling effort clearly must be approached in stages, with continuing improvements in scope and level of detail. And as the key threats become better understood, the evolution of this system description will lead to many near-term actions.

Ultimately, there is little we can do to avoid some level of discrete vulnerability. Still, we can seek to ensure to the degree possible that U.S. infrastructure systems as a whole, and certain critical subsystems, are robust, adaptive, and

[3]This section is based in part on a working paper of the Stanford Department of Management Science and Engineering (Guikema and Paté-Cornell, 2002) and a RAND working paper (Davis, 2002) being used in a project for the Defense Advanced Research Projects Agency.

resilient against a wide variety of terrorist attacks. This is akin to a "capabilities-based" approach to defense planning.[4]

In the face of massive uncertainty, a common impulse is to think of across-the-board defense improvements. But given our finite wealth, time, and ability to concentrate, we must make choices. Doing so requires using probability estimates or other methods for dealing with uncertainty. If probabilities are used—e.g., the probability of a given type of attack, of an installation's vulnerability, or of the capacity to rebuild or substitute for a damaged node—they typically cannot be obtained from empirical frequency distributions; the events are too uncommon or hypothetical. Instead, the probabilities must be derived using a combination of modeling, gaming, and analysis—all with a good deal of subjectivity. Further, the probabilities should change over time as our experience grows and our knowledge improves.

The Threat System to Be Weakened

In parallel with strengthening defenses, we can reduce the likelihood of various threats by destroying terrorist organizations where possible and, in some cases, by deterring elements of the terrorist organizations' larger systems. A terrorist network has numerous parts, each with different vulnerabilities and receptiveness to influence. A Bin Laden may not be deterrable, but other parts of the system—for example, an organization's financiers and state supporters—may well be. The segments of society from which the terrorists are drawn could be influenced by international actions and by attacks on terrorism ideology and tactics. Within the United States, those who assist terrorists may be dissuaded or caught. Finally, the terrorist actors themselves are often concerned about operational risk—they may be willing to risk their lives, but not in futile attacks. Thus, better defensive measures can help to deter or deflect.[5]

A Simple Game-Structured View

The overall system the committee is describing is dynamic. U.S. actions affect the terrorist system, and terrorist actions affect the United States. It is thus appropriate to view the problem analytically as a game, a simple version of which is shown in Figure 10.2. (It is simple by virtue of its not treating other countries or organizations explicitly.)

The state of the real world changes as both sides take actions and have

---

[4]See Rumsfeld (2001).

[5]For recent discussions of terrorist behaviors, see Lesser et al. (1999), Talbott and Chanda (2001), Tucker (2000), Moodie (1998), Roberts (1997), and the Monterey Institute's online bibliography at <http://cns.miis.edu/research/cbw/biblio.htm#terror>.

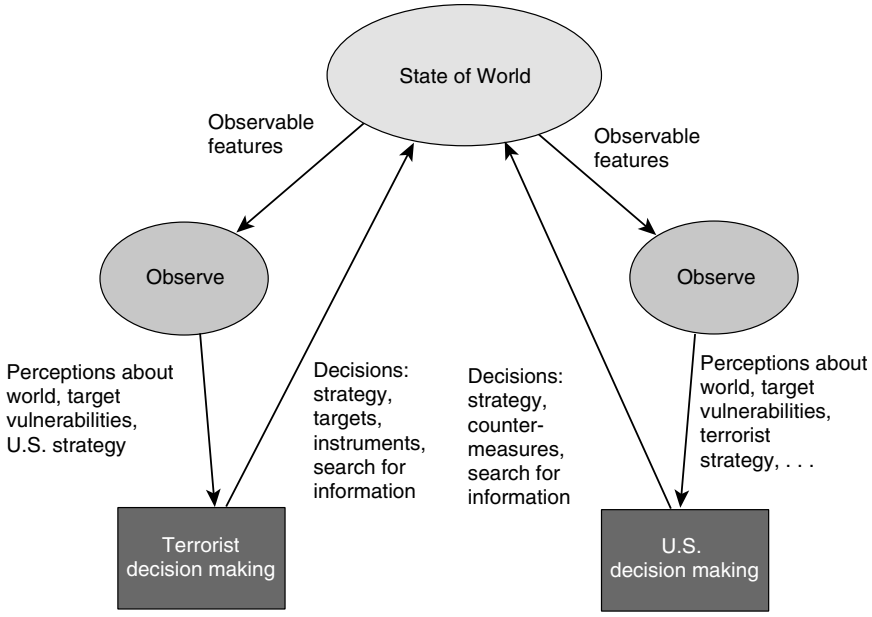

FIGURE 10.2 Perceptions and decisions on both the U.S. and the terrorist sides.
SOURCE: Paté-Cornell and Guikema (2002), by permission of the authors.

reactions. Thus, Figure 10.2 applies over and over again, for each iteration in time. The state of the single node related to terrorist decision making (bottom left in the figure), for example, is the result of a complex process that can be modeled through multiple levels of resolution. The same is true for U.S. decision making. Both sides make decisions, in part on the basis of their beliefs about the other side.

A System Model for Counterterrorism Defense

Figure 10.3 gives highlights of a prototype model that was recently built for analyzing counterterrorism defense in such a dynamic system. Although it is not a finished product, it illustrates a global approach that could be extended and used in real time to support protection decisions. Table 10.2 summarizes its variables and the values of those variables considered in the pilot study.

The model of Figure 10.3 is presented in terms of Bayesian-net influence diagrams.[6] Such a diagram includes not only a (directed) network of boxes and

[6]In other contexts, an influence diagram merely indicates what elements of a modeled system affect one another, without use of Bayesian nets. Such diagrams are a core element of the System Dynamics method introduced by MIT's Jay Forrester in the 1960s (see Sterman, 2000). Variants, sometimes referred to as cognitive maps, can characterize the reasoning of adversaries, for example.

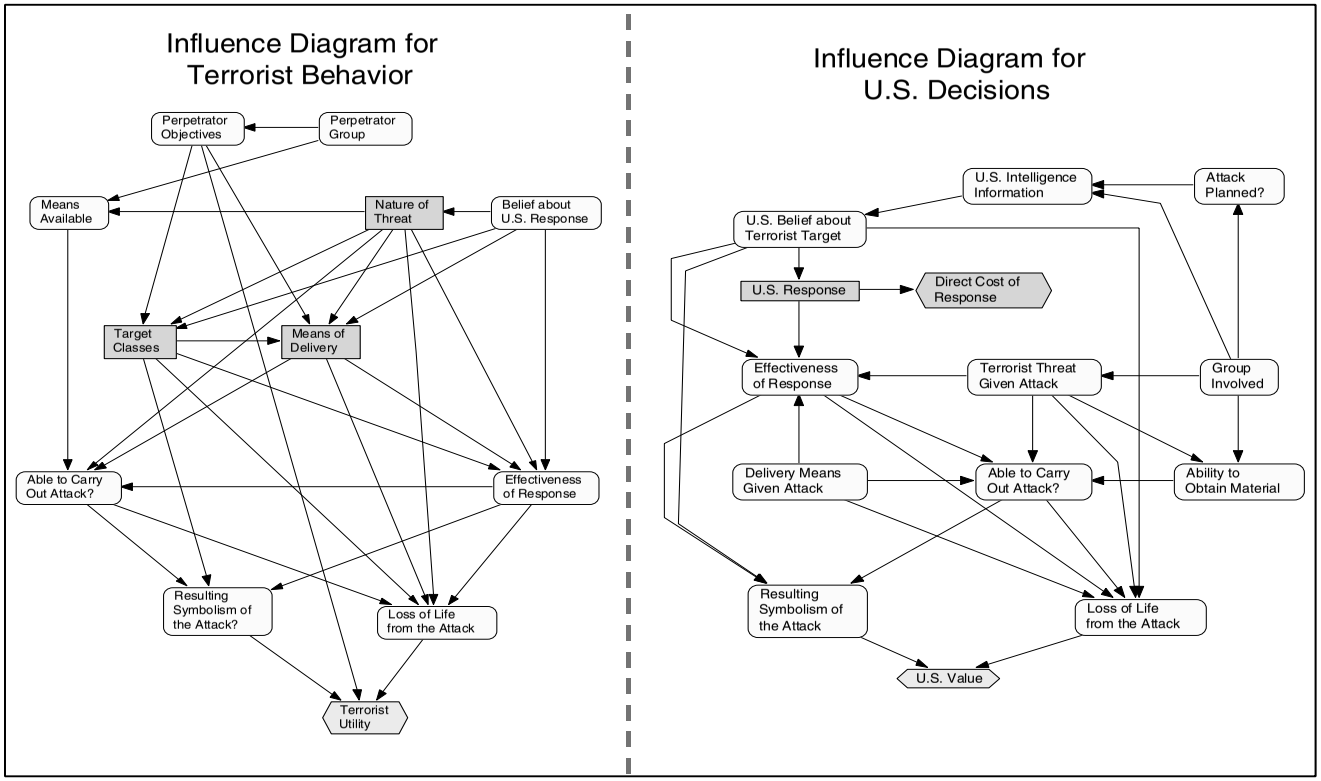

FIGURE 10.3 Single-period influence diagrams for terrorist and U.S. decisions. SOURCE: Paté-Cornell and Guikema (2002), by permission of the authors.

TABLE 10.2 Variables of Model Shown in Figure 10.3

Variable	Values (simplified sets for illustration)
Terrorist groups	Islamic fundamentalist networks or individuals; disgruntled American groups of individuals; foreigners with anti-U.S. dispositions
Objectives and preferences	Symbolism of target, number of casualties, destruction and economic losses, destabilization, etc., with different weights for each terrorist group
Available means	Terrorists' supply chain: cash, people, skills, materials, and communications
Nature of threat (weapon used)	Nuclear, biological, conventional (including assassination), propaganda, fear, etc.
Target class	Buildings, individuals, infrastructures, population groups, etc.
Delivery means	Ships, airplanes, people, etc.
Information (e.g., intelligence)	Nature of the signals gathered by U.S. intelligence regarding group activity, specific threats, targets, etc.
Countermeasures (shown as part of "U.S. response" in Figure 10.3)	Protective actions taken by the United States in the short term (such as freight screening); medium-term (stockpiling of vaccines); and long-term (hardening of targets). Impact on future terrorist threats.
Consequences (direct and indirect) of a successful attack	Outcome of attack scenario involving, for example, casualties; economic losses; political destabilization; loss of U.S. influence.
U.S. insider's assistance (not shown explicitly in Figure 10.3)	Whether or not accomplices within the U.S. system are available to facilitate penetration of protected sites (e.g., nuclear power plants, Air Force bases)

arrows, but also probability distributions, conditional dependencies, decision alternatives, the preferences (objectives) of the decision maker, and the potential consequences of different scenarios. Such diagrams thus include four types of variables: state variables describing the nominal states of key elements of the system and the uncertainties about those states (oval nodes); decision variables describing the spectrum of alternatives considered by terrorist or U.S. decision makers for important decisions over time (rectangular nodes); the value functions that represent the decision makers' preferences and value structures; and the resulting values of the outcomes of their decisions and actions (hexagonal nodes). The arrows represent the direction of the conditional probability structure. An inference engine based on Bayesian reasoning is then used to estimate the prob-

ability distribution of the outcomes, and to select the best alternative based on utilities (Shachter, 1986; Howard, 1999).

Figure 10.3 only shows a top-level view. For brevity, it does not highlight a number of factors that were important in the initial application of the model. For example, at any given moment, the terrorists' knowledge about target vulnerability, and their decisions about which targets to attack, may depend critically on insider information, on the results of prior reconnaissance, and on confusion resulting from U.S. countermeasures. In the wake of September 11, terrorist groups will probably hope for indirect and cascading effects of the sort studied in the United States under the rubric of effects-based targeting.

An important alternative to Bayesian methods, which also depends on system descriptions and diagrams such as those shown above, is called exploratory analysis (Lempert et al., 1996; Davis et al., 2001). It also treats the elements of the system problem as quite uncertain, but it uses multiresolution modeling to reduce the number of key uncertain inputs and then uses a combination of parametric and probabilistic methods to characterize the uncertainties and their consequences. It maintains visibility on how policy variables and the most critical of other variables affect the problem by treating those variables parametrically. Recent gains in computer power and modeling theory have now made such exploratory work feasible.

Developing Potential Threat Profiles

Clearly, to develop an effective decision-making tool would require substantial effort by many individuals working at a variety of operational agencies. But methodologies suggested here and in the references provide a potential path for doing so—that is, for developing the necessary framework for modeling and analyzing terrorist threats and their relative risks to the United States.

Given that such models can be built, how can they be used? The objective of the pilot model sketched in Figure 10.3 was to suggest the following:

- Priorities for strengthening elements of the U.S. infrastructure, networks, and socioeconomic components;
- Priorities for efforts to reduce the overall threat; and
- Priorities for research and intelligence-gathering that could improve the quality of judgments on these matters.

Recommendation 10.2: Those federal agencies with counterterrorism responsibilities should, in coordination with the intelligence communities, conduct a series of threat assessments and red-team activities in order to develop profiles of potential threats to critical U.S. infrastructures. These threat profiles would be used in conjunction with validated simulation models of the infrastructures to establish system vulnerabilities and levels of risk.

The goal of these analyses would be to establish significant risk-reduction measures and operational improvements, including techniques for hardening the infrastructure and procedures for training local responders.

INFRASTRUCTURE MODELING

Introduction

It is clear that the critical infrastructure of the United States—defined as the nation's systems of electric power, telecommunications, gas and oil production, storage and transportation, banking and finance, transportation, water supply, and emergency services—presents significant targets for terrorists, and recent events show that the number and magnitudes of these threats are increasing. Thus modeling U.S. critical infrastructure vulnerabilities—particularly for such objectives as identifying patterns of anomalous behavior, finding weak points in the infrastructure, training personnel, and helping to maintain continuity of operations following terrorist attack—will be of great national importance.

Infrastructure Interactions

To achieve efficiencies of production, consumption, and reliability, the critical infrastructure's large distributed systems are organized into networks of interacting elements, as illustrated in Figure 10.4. Interactions might take the form, for example, of material flows (such as oil or commodities) or information flows (such as sensor readings or command-and-control messages). The links are designed and the systems are operated in such a way that decisions based on local incentives and information lead to collective, networkwide benefits.

But the links that promote collective gains also serve as the conduits through which disturbances, whether initiated by nature, human error, or terrorists, are propagated to neighboring systems. As an example, in January 1991 a fiber cable was accidentally cut, blocking 60 percent of long-distance calls in and out of New York City. This single cut also disabled air-traffic-control functions in New York, Washington, D.C., and Boston, which depend on telephone lines for voice and data, and it disrupted operations of the New York Mercantile Exchange and several commodity exchanges (Neumann, 1995).

Fortunately, most system failures—whether triggered by natural or human-made disturbances—are substantially contained in space and time. On occasion, however, disturbances are amplified as they propagate, leading to a catastrophic failure characterized by cascading faults. The major power failure in the Pacific Northwest on August 10, 1996, is one example of cascading faults leading to such a catastrophic failure. Not surprisingly, these rare but catastrophic events are of great interest to terrorists and to those trying to check the terrorists.

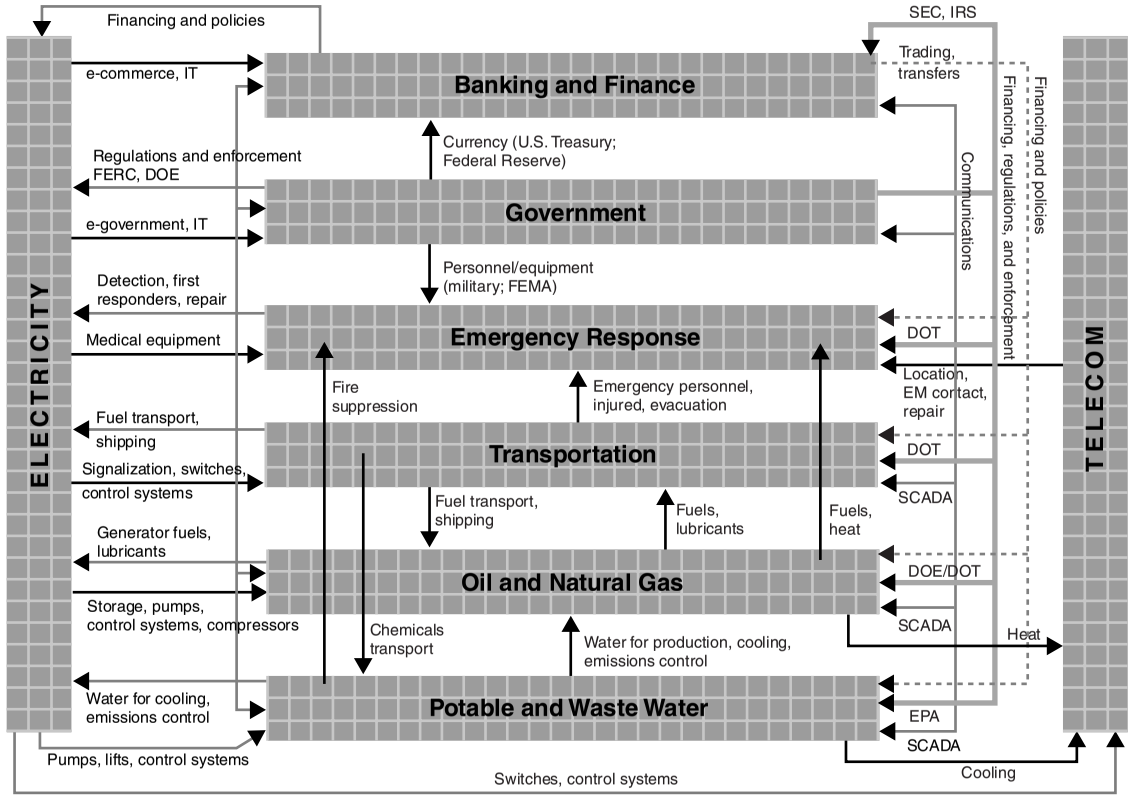

FIGURE 10.4 Critical infrastructure interdependencies. SOURCE: Heller (2002), by permission of the author.

The vulnerabilities of a system are not necessarily constant. The susceptibility of the electric power grid to disruption continually changes as loads ebb and flow and as generation resources come on line, are utilized, or made unavailable. There are also persistent vulnerabilities in both hardware and software. For example, the transmission bottlenecks of Paths 15 and 26 connecting Northern and Southern California are well known (Houseman and Martin, 2001), and, as shown by Project Eligible Receiver, computers controlling electric power grids are accessible, and subject to manipulation, by anyone with hacker knowledge (Gertz, 1998; Myers, 1998).

Similar vulnerabilities apply to telecommunications—the public telephone and Internet systems, for instance, and the dependence of one on the other (the Internet uses leased telephone lines for much of its physical network). This story is told with remarkable clarity in the NRC report *Trust in Cyberspace* (Computer Science and Telecommunications Board, 1999).

A direct way to address vulnerable transmission bottlenecks and make the grid more robust is to build additional transmission capacity, but there are indications that redundancy has a dark side (in addition to increased costs). The likelihood of hidden failures in any large-scale system increases as the number of components increases. Modeling techniques are only now emerging for the analysis of such hidden failures (see, for example, Wang and Thorp, 2001).

Still, the interdependencies among any of these systems are not well understood, and few models exist to bolster our understanding. Moreover, though underlying features common to these networks suggest the possibility of a unifying mathematical theory, in the current stage of knowledge we must admit that the similarity between, say, a blackout in interconnected power networks and a meltdown on the Internet is metaphorical rather than structural.

Models of discipline-specific phenomena rely on corresponding domain experts, who generally do a respectable job. But while it is at the seams, or interfaces, between disciplines where modeling must address terrorist threats, these experts often find it difficult to work at the seams. Communicating across disciplines requires domain experts to learn one another's languages in order to pose significant questions and usefully interpret the answers.

Computational simulation is commonly needed, especially for modeling at the seams, and this will most often demand the use of high-performance computers. Given the necessary fidelity of the simulations, the complexity of the models, their usually stochastic nature (which requires much repetition), the massive amounts of data, and the need for advanced visualization and software-management tools to validate the results, only high-performing computing will do. Consequently, development and operation of the most extensive models can only be performed using a few specialized facilities.

DOD, notably the Defense Modeling and Simulation Office, has a good deal of experience in this area, particularly with large federations of models and distributed operations. This experience, as well as that of other organizations,

can be applied immediately to government efforts on developing and validating simulation systems specifically aimed at counterterrorism applications.

However, seasoned practitioners would be the first to acknowledge the challenges in this domain. Additional research is needed in the validation area, but salvation—to the extent that it is possible—will depend on refining the theory and science of modeling, not on after-the-fact testing procedures. There is broad consensus among system modelers that quality must be designed in from the outset and established module-by-module during development.

Advanced computational techniques, identification of interdependencies among infrastructure elements, and development of software and data-analysis capabilities that make use of the latest developments in computer hardware are also required. The ability to test models against real-world data to determine model fidelity for particular infrastructures and the interdependencies between different infrastructures is critical. Models must be developed and verified using real-world data.

Data Issues for Infrastructure Modeling

Modeling of the U.S. critical infrastructure requires significant capabilities for integrating data measured in diverse units of space and time, and it must address the limitations of many current data sources that were developed originally for stand-alone systems. Integration is limited, however, not only by the frequent incompatibility of different data sets but also by imprecision in the definitions that embrace them all (i.e., lack of adequate metadata). This situation will persist into the foreseeable future unless there is a significant data-management effort—and particularly the development of tools and methodologies for effective database integration on a large scale.

The commonly cited example of the failure of the NASA Mars mission in 1999 (Madnick, 2001), caused by an erroneous attempt to integrate two databases (one with English units and the other with metric units), is just one example of inadequate database integration. Counterterrorism applications will require the integration of data from Web sources, fielded instrumentation, legacy applications in database-management systems, and many other sources. Clearly, most of these systems were not designed to work together, and much effort will thus be required to establish the data definitions for successful integration and model use.

Many efforts are currently under way to develop the necessary metadata and associated standards. They include projects of the International Organization for Standardization, the FAA, and sections of the U.S. national security communities—notably the intelligence community Metadata Standard program[7] and the DOD Modeling and Simulation Knowledge and Data Integration initiative. These

[7]See <www.xml.saic.com/icml/> for more information.

projects are proceeding rapidly, but similar efforts have not been widely implemented in other federal, state, and local agencies regarding databases that are highly relevant for critical infrastructure modeling and counterterrorism programs. Much more work is required, then, to develop and implement viable metadata standards that are sufficiently robust to enable the required database integration.

Extending Modeling and Analysis Capabilities and Enabling Interoperation Among Databases

There are two primary conclusions of this section: First, the requirements of R&D programs for protecting the U.S. critical infrastructure from catastrophic terrorism, as well as the related needs of agency operations, will not be met by the current generation of models. Furthermore, no central organization is charged with the development and implementation of the necessary models and staffed with the appropriate domain experts.

Current models are designed to analyze individual systems and thus are unable to provide realistic, decision-quality information about the likely effects of terrorist acts on the overall critical infrastructure. Improving the situation should be a high priority for federal counterterrorism programs since many of the disciplines underlying large-scale systems-modeling issues will require further basic research. (The National Science Foundation (NSF) is a logical home to foster such research needs, many of which are discussed in the next section of this chapter.)

Second, although there are many private and public databases that contain information potentially relevant to counterterrorism programs, they lack the necessary context definitions (i.e., metadata) and access tools to enable interoperation with other databases and the extraction of meaningful and timely information. Although elsewhere in the U.S. government efforts are under way to develop metadata standards that would greatly improve integration and interoperability, national homeland security efforts will require that programs establishing the relevant databases are supported and funded to ensure that metadata standards for counterterrorism applications are implemented. Homeland security needs should be a driver for new efforts in this area that address the current limits in data coverage, quality, timeliness, and supporting database-management technology.

Recommendation 10.3: A governmentwide effort should be made to leverage existing modeling and analysis capabilities and, where appropriate, to develop new capabilities to model critical infrastructures and related interdependencies. In so doing, the federal government should collaborate with commercial organizations that have system models relevant to the homeland security missions—notably in the areas of threat assessment and critical infrastructure—in order to identify candidates for near-term model-integration initiatives.

The capabilities and quality of existing models of government and commercial operations need to be assessed. New models may have to be built and validated in some areas. The results of these efforts, together with new methods, some of which may have to be developed, should be used to construct integrated models that can improve our understanding of the vulnerabilities of the infrastructures and their interdependencies, i.e., what needs to be defended. This understanding can be used in turn to develop sensor deployment and defensive strategies, the merit of which can be indicated by the model and validated by red-team efforts of the type described in Recommendation 10.2.

Recommendation 10.4: The federal government, working with the various commercial organizations that have been identified with homeland-security-related missions, should identify counterterrorism-related databases and establish metadata standards and assess tools for integrating diverse bits of data.

To conduct the analyses on which models are based, a rational data structure is needed. Efforts toward achieving this structure are under way in some government organizations. These efforts, however, have pointed to the need for additional funding, some for the organizations operating the various databases in order to establish the necessary metadata standards, and some to develop access tools for database interoperation.

MODELING CHALLENGES FOR COUNTERTERRORISM

The preceding sections have emphasized the critical importance of models in the systems approach to counterterrorism, and they have also noted some of the deficiencies of current modeling technologies. This section describes two methods of model development and operation that appear to offer significant potential for analyzing the complexities of counterterrorism applications. As such, they should be a significant part of the research agenda.

Complex Adaptive Systems and Agent-Based Models

Complex adaptive systems involve phenomena that may be characterized by the interactions of numerous individual agents or elements, which tend to self-organize at increasingly higher levels. This process results in evolutionary, emergent, and adaptive properties that are not exhibited by the individual agents themselves. For example, an animal may be an agent in a formation of a herd of animals, and herds of animals may become a species, and the species may be part of a particular ecosystem. There is a clear analogy here to the characteristics of our society's critical infrastructure and its associated adaptation, emergence, and evolution.

Complex adaptive systems obtain data and information from their internal

and external environments alike. They find patterns, and ultimately process and represent them as internal models; these can then used by analysts to predict the potential outcome of future decisions. Further, in complex adaptive systems these internal models are subjected to revision as the impacts of decisions provide feedback. This often results in self-organization into a higher-level complex system (Axelrod and Cohen, 1999).

A general rule for complex systems is that we cannot create a model that accurately predicts the outcomes of the actual system. However, we can create a model that accurately simulates the processes that the system will use in order to create a given output. Awareness of the potential for such models has profound implications for organizational efforts that are intended for such purposes as homeland security.

System Dynamics-Based Models

System dynamics models are used for representing whole federations (systems) of systems. They take a top-down approach to system analysis by compressing the many variables of a large, complicated system of systems into a relatively small number of overall attributes, called aggregate state variables. According to Sterman (2000), characteristics of these models include the following:

- *State-determined.* The aggregate state variables span and define all key variables within the system.
- *Feedback-driven dynamics.* The dynamics of the overall system arise not from exogenous shocks but rather from feedback between the state variables.
- *Nonlinear.* The model structure can produce highly nonlinear responses, giving rise to complex, even chaotic, dynamics.
- *Boundary defined by system-level problem or issue.* Only the system states and feedback paths necessary to replicate and investigate a given system-level problem are modeled.
- *Emphasis on policy design for system control.* Because these systems are focused on social or organizational problems, system dynamics models emphasize the design and implementation of policies that can improve problematic system performance.

Risk Modeling, Assessment, and Management Process

The entire process of risk assessment and management (both of which stem from risk modeling) is a synthesis of the empirical and the normative, of the quantitative and the qualitative, and of objective and subjective evidence.

In risk assessment, according to Kaplan and Garrick (1981), the analyst often attempts to answer the following three questions:

- What can go wrong?
- What is the likelihood that it will go wrong?
- What are the consequences?

Answers to these questions help risk analysts to identify, measure, quantify, and evaluate risks and their consequences. Risk management builds on the risk-assessment process by seeking answers to a second set of three questions:

- What can be done and what options are available?
- What are the trade-offs in terms of all costs, benefits, and risks?
- What are the impacts of current management decisions on future options?

A systems-based risk-management approach that harmonizes overall system management must also address the four sources of failure: organizational, human, hardware, and software (Haimes, 1998). This chapter has largely addressed possible ways of reducing failure in the latter two, but doing so in the first two could well be the greater challenge.

A central quandary facing the development of system-level counterterrorism modeling is the large gap between what a systems analysis says stakeholders should do, and what they actually do. Simply put, assume that the systems modelers get it exactly right and produce models that capture important dynamics and indicate important policies that should (and should not) be followed. Three layers of issues then compromise the results of these models and the effective policies and actions presumably based on them:

1. Sterman (1989) has used the term "misperception of feedback" for the cluster of problems pertaining to a single human actor who, ideally, first comes to understand and then effectively manages system-level complexity. Repeatedly, in case and experimental situations alike, human actors manage complex systems at suboptimal levels, even when perfect information concerning the system and its dynamic complexity is available to them through system simulations and analyses. Similarly, individual government officials could well make ineffective or even counterproductive choices on antiterrorism actions.

2. Senge (1990) and others have focused attention on a related set of issues centering on how organizations do (or do not) learn about system-level complexity. For over a decade, corporate America and key divisions of federal, state, and local governments have been striving to become more effective learning organizations. But their behaviors, even with perfect information, parallel that of the individual. Perhaps the threat of massive damage inflicted by deliberate terror will motivate government agencies to learn by means other than direct trial-and-error experimentation.

3. Finally, we need to address the cognitive and organizational issues in-

volved when multiple, networked agencies operate in a complex intergovernmental bureaucracy to address a problem such as terrorism.

Long-Term Systems Engineering and Research Needs

Federal agencies, industry consortia, and other groups addressing counterterrorism will need to develop systems-level approaches for evaluating the costs, benefits, and risks associated with homeland protection. In addition, a significant new research program in systems analysis and systems engineering for counterterrorism will be needed to develop the modeling concepts and implementations that are essential for understanding critical U.S. infrastructures. The need for improved modeling concepts applies not only to infrastructure, however, but also to the entire spectrum of science and technology for counterterrorism. The National Science Foundation (NSF) is a logical home for such a research program.

Studies will be needed in the spirit of Figure 10.1, which depicts the myriad perspectives of the homeland's system of systems (its governance, economy, and infrastructures) as well as those of the terrorist networks. Such studies will enable a greater understanding of the nature of external threats, along with the strengths and weaknesses of the U.S. critical infrastructure, so that effective policies can be formulated.

The development of concepts and computational methodologies to enhance system-of-systems research and integration would allow us to address the organizational abilities needed to execute high-level systems management. In particular, approaches for agent-based and equation-based (e.g., system dynamics) modeling would enable representation of terrorist and critical infrastructure characteristics. Research would also support the development of methodologies to improve understanding of the interconnectedness and interdependencies among critical infrastructures and to better understand, model, assess, and manage the risks to homeland security from physical, economic, social, and psychological perspectives.

Finally, the development and use of simulators and learning environments will be key supports for the analysis of counterterrorism policy. System-level insights are often counterintuitive, are not easily learned by trial and error, and have outcomes that may only be known in the long run. Simulators linked to learning environments can help systems managers develop and implement robust policies without experiencing costly system failures.

Recommendation 10.5: To support the necessary S&T, federal agencies should establish new mechanisms for funding counterterrorism research and pilot projects at various research institutions in order to support efforts at the national, regional, and local levels. In particular, the federal government should establish a long-term, multidisciplinary systems engineering and research agenda to support future modeling challenges, educational

opportunities, and projects aimed at developing an overall systems approach to counterterrorism. The agenda should include the following:

- **System-of-systems perspectives for homeland security;**
- **Agent-based and system dynamics modeling;**
- **Analysis of risk assessment and management from multiple perspectives, including the risk of potentially extreme and catastrophic events;**
- **Modeling of interdependencies among critical infrastructures; and**
- **Development of simulators and learning environments.**

Research projects should involve many domains of expertise; a single disciplinary perspective should not dominate the agenda. NSF would be an appropriate lead agency for such a research effort, but other federal research agencies, such as the Defense Threat Reduction Agency, DARPA, and the Intelligence Community's Advanced Research and Development Activity, have relevant expertise and should develop companion programs to support the long-term research agenda.

IMPLICATIONS FOR EDUCATION

The development of effective counterterrorism strategies relies on the pursuit of specific science and technology goals as well as on a systems approach (including study of those who would attack the United States) within which to apply the results. This suggests a need for systems-level thinking in education and, more specifically, a provision for educational degrees focused on systems, to help create a cadre of people who understand the interconnectedness of our society's many parts.

Degree programs at the graduate level are needed to produce leaders fully cognizant of the issues of systems and their complexity—people who can operate at the interfaces and offer an integrated vision of, say, engineering and political systems. Such degree programs will be characterized by a highly interdisciplinary course of study, which can be difficult to organize within the departmental structure of universities.[8]

In addition to people who have received an education specifically focused on

[8]This issue was framed by Kennedy (1997) in his insightful book *Academic Duty*. In the final chapter, he asks: "Can the universities really make a difference with respect to the Big Problems facing us?" His list of challenges ranges from disarmament to genetic testing, but although these problems are intellectually exciting and analytically demanding, they do not come in disciplinary packages. Instead, these real, complex, and large-scale problems demand the involvement of graduates—possibly the product of "re-engineered" university departments, according to Kennedy—who are not only well trained in their fields but also skillful in systems thinking and comfortable working in a highly interdisciplinary environment.

systems-level tools and thinking, tackling counterterrorism problems will require the people who come out of other graduate programs to be exposed to a broad background of ideas. Graduates of law and public policy programs, for example, will need to be better prepared to apply their skills in areas with substantial scientific and technological content, while science and engineering professionals will have to learn how to identify policy constraints and possibilities and devise political strategies that take the interests of all stakeholders into account.

The education of future leaders is important, but existing leaders will also need to embrace systems approaches to today's problems in order to make deep contributions to the nation's holistic responses to the threat of terrorism. Business and military leaders are traditionally required to engage in continuing education courses, which could provide opportunities to update them on advances in systems analysis and on the types of problems that will benefit from systems-level thinking and tools.

Recommendation 10.6: Government agencies that fund university research should enhance their support of research projects that feature systems analysis and systems engineering, in part to help produce new integrative departments and future leaders who think across the traditional academic boundaries and who can address the complex scientific and technological issues discussed above.

REFERENCES

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission). 2001. *Third Annual Report to the President and the Congress*, prepared for the Department of Defense, RAND, Santa Monica, Calif., December 15. Available online at <www.rand.org/nsrd/terrpanel/terror3-screen.pdf>.

Axelrod, Robert, and Michael D. Cohen. 2000. *Harnessing Complexity: Organizational Implications of a Scientific Frontier*, Free Press, New York.

Carter, Ashton B. 2001-2002. "The Architecture of Government in the Face of Terrorism," *International Security*, Vol. 26, No. 3, pp. 5-23, Winter.

Casti, John L. 1996. *Would-Be Worlds: How Simulation Is Changing the Face of Science*, John Wiley & Sons, New York.

Chankong, Vira, and Yacov Y. Haimes. 1983. *Multiobjective Decision Making: Theory and Methodology,* Elsevier-North Holland, New York.

Computer Science and Telecommunications Board, National Research Council. 1999. *Trust in Cyberspace*, National Academy Press, Washington, D.C.

Critical Infrastructure Assurance Office. 1998. *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, The White House, Washington, D.C., May 22. Available online at <http://www.info-sec.com/ciao/paper598.pdf>.

Davis, Paul K. 2002. "Key Elements of a Framework for the 'Influencing Component' of Counter-Terrorism," working paper in a project for the Defense Advanced Research Projects Agency (DARPA), RAND, Santa Monica, Calif., May 24.

Davis, Paul K., James H. Bigelow, and Jimmie McEver. 2001. *Exploratory Analysis and a Case History of Multiresolution, Multiperspective Modeling*, RP-925, RAND, Santa Monica, Calif. (This is a volume of reprinted journal articles.)

Gertz, Bill. 1998. "Infowar Game Shut Down U.S. Power Grid, Disabled Pacific Command," *Washington Times*, April 17, p. A3.

Haimes, Yacov Y. 1998. *Risk Modeling, Assessment, and Management* (Wiley Series in Systems Engineering), John Wiley & Sons, New York.

Haimes, Yacov Y. 2002. "A Roadmap for Modeling the Risks of Terrorism to the Homeland," *ASCE Journal of Infrastructure Systems*, Vol. 8, No. 2, June, pp. 35-41.

Haimes, Yacov Y., and Pu Jiang. 2001. "Leontief-Based Model of Risk in Complex Interconnected Infrastructures," *ASCE Journal of Infrastructure Systems*, Vol. 7, No. 1, March, pp. 1-12.

Heller, Miriam. 2002. "Critical Infrastructure Interdependencies: A System Approach to Research Needs," Infrastructure and Information Systems, National Science Foundation, presentation to the National Academies Committee on Science and Technology for Countering Terrorism: Panel on Systems Analysis and Systems Engineering, February 14.

Hillestad, Richard, and Paul K. Davis. 1998. *Resource Allocation for the New Defense Strategy: The DynaRank Decision Support System*, MR-996-OSD, RAND, Santa Monica, Calif. Available online at <www.rand.org/publications/MR/MR996/index.html>.

Houseman, R., and E. Dee Martin. 2001. *Protecting America's Critical Energy Infrastructure from Terrorist Attack*, Bracewell and Patterson, L.L.P., Houston, Tex., November 7.

Howard, R.A. 1999. "From Influence to Relevance and Knowledge," *Influence Diagrams, Belief Nets, and Decision Analysis* (Wiley Series in Probability and Mathematical Statistics), R.M. Oliver and J.Q. Smith, eds. John Wiley & Sons, New York.

Kaplan, Stan, and B. John Garrick. 1981. "On the Quantitative Definition of Risk," *Risk Analysis*, Vol. 1, No. 1, pp. 11-27.

Keeney, Ralph L., and H. Raiffa. 1993. *Decisions with Multiple Objectives: Preferences and Value Trade-Offs,* Cambridge University Press, New York.

Keeney, Ralph L. 1976. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs* (Wiley Series in Probability and Mathematical Statistics), John Wiley & Sons, New York.

Kennedy, Donald. 1997. *Academic Duty*, Harvard University Press, Cambridge, Mass.

Lempert, Robert J., Michael E. Schlesinger, and Steven C. Bankes. 1996. "When We Don't Know the Costs or the Benefits: Adaptive Strategies for Abating Climate Change," *Climatic Change*, Vol. 33, No. 2, pp. 235-274.

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini. 1999. *Countering the New Terrorism*, prepared for the U.S. Air Force, RAND, Santa Monica, Calif.

MacKay, James A., Ian Lerche, and John A. MacKay. 1999. *Economic Risk in Hydrocarbon Exploration*, Academic Press, San Diego, Calif.

Madnick, Stuart E. 2001. "The Misguided Silver Bullet: What XML Will and Will NOT Do to Help Information Integration," *Proceedings of the Third International Conference on Information Integration and Web-Based Applications and Services (IIWAS2001),* held in Linz, Austria, September 10-12.

Moodie, Michael. 1998. *Chemical and Biological Weapons: Will Deterrence Work?* (The Deterrence Series), Chemical and Biological Arms Control Institute, Washington, D.C., March.

Myers, Laura. 1998. "Pentagon Has Computers Hacked," Associated Press, April 17. Available online at <www.connectingpointlv.com/pentagon_has_computers_hacked.htm>.

Neumann, Peter G. 1995. *Computer Related Risks*, Addison-Wesley, Reading, Mass.

Paté-Cornell, M. Elisabeth, and Seth D. Guikema. 2002. "Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures," submitted for publication in *Military Operations Research*; working paper of the Department of Management and Science and Engineering, Stanford University, Stanford, Calif.

Renaldi, Steven M., James P. Peerenboom, and Terry K. Kelly. 2001. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, Vol. 21, No. 6, December, pp. 11-25.

Roberts, Bradley, ed. 1997. *Terrorism with Chemical and Biological Weapons: Calibrating Risks and Responses,* Chemical and Biological Arms Control Institute, Washington, D.C.

Rumsfeld, Donald H. 2001. *Quadrennial Defense Review Report,* Department of Defense, Washington, D.C., September 30. Available online at <www.comw.org/qdr/qdr2001.pdf>.

Sage, Andrew P., and William B. Rouse, eds. 1999. *Handbook of Systems Engineering and Management*, John Wiley & Sons, New York.

Senge, Peter M. 1990. *The Fifth Discipline: The Art and Practice of the Learning Organization*, Currency/Doubleday, New York.

Shachter, Ross D. 1986. "Evaluating Influence Diagrams," *Operations Research*, Vol. 34, No. 6, November-December, pp. 871-882.

Sterman, John D. 1989. "Misperceptions of Feedback in Dynamic Decision Making," *Organizational Behavior and Human Decision Processes,* Vol. 43, No. 3, pp. 301-335.

Sterman, John D. 2000. *Business Dynamics: Systems Thinking and Modeling for a Complex World,* Irwin Professional Publishing Co./McGraw-Hill Professional Books, New York.

Talbott, Strobe, and Nayan Chanda, eds. 2001. *The Age of Terror: America and the World After September 11,* Basic Books, New York.

Tucker, Jonathan B., ed. 2000. *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, MIT Press, Cambridge, Mass.

U.S. Environmental Protection Agency. 2002. *Lessons Learned on Planning and Scoping for Environmental Risk Assessments*, Washington D.C., January.

Vatis, Michael A. 2001a. *Combating Terrorism: A Compendium of Recent Counter Terrorism Recommendations from Authoritative Commissions and Subject Matter Experts*, Institute for Security Technology Studies at Dartmouth College, Hanover, N.H., September 16. Available online at <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cbt_ter1.pdf>.

Vatis, Michael A. 2001b. *Cyber Attacks During the War on Terrorism: A Predictive Analysis*, Institute for Security Technology Studies at Dartmouth College, Hanover, N.H., September 22. Available online at <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>.

Wang, Hongye, and James S. Thorp. 2001. "Optimal Locations for Protection System Enhancement: A Simulation of Cascading Outages," *IEEE Transactions on Power Delivery,* Vol. 16, No. 4, October, pp. 528-533.

11

The Significance of Crosscutting Challenges and Technologies

INTRODUCTION

This report discusses in detail the impact of potential terrorist attacks on our major systems—information, energy, transportation, and power, among others, as well as on our cities—with conventional, biological, chemical, nuclear, and information-warfare weapons.

An even more daunting set of challenges comes from the fact that the country's major systems—energy and information, for example—are integrated and interoperable to a significant degree. Terrorists may seek to achieve their objectives by taking advantage of such couplings. They could attack a system at a point selected to produce serious reverberations throughout many of the other systems, thereby maximizing the damage from a single action. Or they could simultaneously attack critical nodes within several linked infrastructures to produce enormous overall damage to the nation—to its systems and its citizens.

A significant array of technology is already available—much of it developed by the DOD and DOE—that can be adapted to improve homeland security. But dedicated research and development carried out over the next decade must greatly expand this array in order to make the nation's infrastructures and people more secure. These technological challenges, many of which are discussed in Chapters 2 to 10, can be met through an expanded, focused, and sustained set of research and development programs. Some of these programs recur in many of the chapters because efforts that contribute to the response to terrorism have some common technical elements. For this reason, these common elements deserve specific attention in this chapter, which addresses seven such crosscutting issues:

1. The need for the application and continued development of systems analysis and modeling capabilities to aid in threat assessment, in identification of infrastructure vulnerabilities and interdependencies, and in planning and decision making (particularly for threat detection, identification, and response coordination);

2. The development of standards and techniques to allow for the integrated management of data regardless of their source;

3. The utilization and development of sensors and sensor networks for the detection of conventional, biological, chemical, nuclear, and information-warfare weapons. To be effective and acceptable for operational use, these systems must have high sensitivity in detecting various threat agents yet must also function with low false-positive and false-negative rates;

4. The need for the use and continued development of robotic platforms to support mobile sensor networks for threat detection and intelligence collection. Robotic technologies can also assist humans in such activities as ordnance disposal, decontamination, debris removal, and fire-fighting;

5. The need to harden and protect the supervisory control and data acquisition (SCADA) systems that are widely used for operational control and monitoring of most components of the nation's basic infrastructures.

6. The need to control access to our physical and information systems, thereby increasing security, while minimizing the impact of security measures on system performance. The committee focuses on biometrics as a promising set of technologies for this purpose.

7. All systems within the United States are operated or controlled at some level by humans. The design and deployment of systems to counter terrorism, being dependent on human command and control, must likewise take human factors and organizational-behavior principles into account.

The committee refers to these issues as "crosscutting" because they recur as ways to lessen many different vulnerabilities, but they could also be called "systems" issues because they are strongly interrelated. For example, improved techniques for data management will be a critical enabler for systems modeling, sensor networks, robotics, and biometrics. Systems analysis will lead to a better understanding of how to improve SCADA systems. And of course understanding human factors will be an essential step in successfully implementing any new counterterrorism technology.

The federal government will need to determine priorities, perform research, and support the implementation of technologies in all of these crosscutting areas, as well as other such areas that may emerge in the future. But because of the interdisciplinary nature of these topics, it is often not clear where the information to support decisions in these areas will come from. In Chapter 12, the committee discusses the need for a Homeland Security Institute to provide the needed technical analysis and support.

The remaining sections of this chapter discuss in greater detail the seven crosscutting issues listed above. The chapter concludes with a discussion of the kinds of research and development efforts that are needed, together with their associated structural and funding considerations—particularly within the U.S. government—to make an effective and aggressive science-and-technology agenda for counterterrorism a reality.

SYSTEMS ANALYSIS AND MODELING

Our nation's infrastructures are individually complex and tightly linked, so a terrorist attack has the potential to produce manifold effects in multiple seemingly independent systems. This means that in modeling the nation's infrastructures and assessing any threats against them we must take a methodical and coordinated approach, not only to exploring each system's vulnerabilities but also to analyzing the overall picture.

Modeling and simulation are especially useful for these purposes, and they could make important contributions to counterterrorism research at both the macro and micro levels. At the largest scale, simulations might be able to reveal the vulnerability of whole infrastructures—and of networks of infrastructures. For example, the air transportation system depends heavily on fuel supplies (for airlines and for ground transportation for getting people and resources to/from airports), power (electricity for the airport concourses, ground maintenance, general lighting, and air traffic control), and communications networks; what happens when one (or two) of the elements are disengaged from the system? Many such examples exist: What exactly will the effects be on the transportation system if a major petroleum refinery is put out of commission? How severely will firefighting capabilities be limited if part of a city's water system is shut down?

Even on smaller scales, modeling and simulation are important tools that can provide useful perspectives on how chemical plumes, radioactive fallout, or spore clouds might disperse through the air and how hazardous material spills might spread over land or in water.[1] A particularly important area will be modeling relevant to bioterrorism, as there are a large number of potential biological agents, and a great deal of terror could be generated by a biological attack. Modeling can help examine how diseases would spread for a range of different incubation periods and transmission dynamics, as well as take into account key variables like climate, population, and migration. Understanding realistic as well as worst-case circumstances is essential. For this work, the expertise in building these kinds of

[1]Modeling the behavior of contaminants could be done through computational simulations or through experiments on small model physical systems.

models and the knowledge of key input parameters is limited for human, animal, and plant pathogens, so increasing the pool of experts and performing research to determine how potential biological agents behave will be vital for planning efforts.

Finally, modeling and simulation can also be invaluable in disaster planning and training, allowing for principal players and staff to rehearse emergency procedures and gain experience in decision making under crisis conditions.

Many models and simulations already exist, but they would have to be modified to account for the different dynamics of systems, people, and social organizations under the difficult and unusual conditions of terrorism. These special needs stem in part from the diversity of potential agents and the numerous kinds of terror they generate and in part from the behavior of terrorists, which cannot usually be modeled as a probability distribution (as in conventional models), although the *consequences* of a terrorist attack do have stochastic elements. Still, many of the new systems-analysis tools could be dual use: The study of terrorist attacks might also be of value in better understanding medical, fire, weather, and other emergency situations. Conversely, critical assessment of previous acts of sabotage or other illegal forms of tampering, entering, or destruction of components of our infrastructure could be useful in developing case studies for training exercises and providing real-world data to validate new models. As a general rule, the essential elements of large-scale analyses, modeling, and simulation are well understood. However, useful output is very much dependent on a keen grasp of the physical system being simulated, knowledge of its most appropriate models, and access to reliable data—or at least reliable distributions of key variables. These needs are even more intense in analyzing the interconnectedness of systems. Because the simulations would be multidisciplinary, they would require considerable expertise across several domains, likely to be manifested in a sizable team of experts.

Such multidisciplinary efforts, at least in the past, have been easier said than done. While the current state of the art for the analysis and modeling of critical infrastructure is reasonably good, it is focused only on single aspects. For example, there are models of the electric power grid, models of various telecommunications networks, hydrologic models of river basins and dams, and so on. A number of modeling efforts have been funded by DOD's Defense Threat Reduction Agency, and are currently under development, to analyze potential threats to critical infrastructures within the United States, particularly those used by DOD to support operations. However, models describing *interactions* among various dimensions of critical infrastructure are almost totally lacking. Research efforts are currently under way to develop such models, but these efforts are small and in their initial stages. Clearly, in the overall development of scientific and technological capabilities for countering terrorism—which will probably target multiple aspects of critical infrastructures—modeling the interactions among systems should receive higher priority.

Most U.S. government departments and agencies are not organized to assess terrorist threats, infrastructure vulnerabilities, and mitigation strategies from a systems perspective—at least not at present. But that could change. Various threat and infrastructure models must be developed, and used in combination with intelligence data, to perform analyses by which high-risk paths and associated attack access-points could be determined. Such results would permit formulation of effective threat mitigation strategies. And they could contain the seeds of their own improvement and contribute to threat prevention: Analysis-derived knowledge of the attack paths deemed to pose the greatest risk would in turn enable determination of what types of terrorist activity intelligence data should be sought.

Strengthening the government's ability to execute the modeling and analyses described in this section depends not only on the application of existing capabilities to counterterrorism problems, but also on the development of new capabilities. A systems modeling and analysis research agenda would include a focus on system perspectives for homeland security, modeling and analysis of interdependencies among critical infrastructures, agent-based and system dynamics modeling, development of simulators and learning environments, and risk assessment and management from a multiobjective perspective, including risks up to and including potentially extreme and catastrophic events. (See Chapter 10 for more on techniques for systems analysis and modeling.)

INTEGRATED DATA MANAGEMENT

Modeling of the many diverse systems and infrastructures in the United States requires capabilities for managing data collected over widely different scales of space and time. The structural characteristics of power plants, pipelines, and reservoirs, for example, obviously do not change rapidly, while many commercial applications (such as energy trading) require real-time updates. Integrating such dissimilar data for the modeling and analysis of counterterrorism programs—themselves having highly time-critical components—is a major challenge.

Many data types must coexist in these applications. Necessary data include structured text (such as tables and system logs), unstructured text (documents), geographic features (maps, for example), time-series data (such as financial histories), video surveillance, and other kinds of data. Furthermore, these data can describe phenomena on very different spatial and temporal scales, from national levels and time periods of decades to very local phenomena with time scales of seconds and minutes. The system models must also be able to work on multiple levels of abstraction, selecting the level of detail in the data necessary for their particular applications.

Because commercial database-management systems currently do not address all of the above data types with reasonably high quality of performance, a

new generation of database-management-system technology will be required. The following issues are critical to establishing the relevant databases drawn from the multiple sources needed for counterterrorism system modeling and decision making:

- Quantity and relevance,
- Timeliness,
- Capabilities for data and database integration,
- Data models and database management architectures, and
- Data evolution.

Ideally, the development of models for large-scale systems should work backwards: from an understanding of the nature of the desired results, through the model, back to the required data. Given the increasing level and sophistication of counterterrorism threats to the United States and the consequent importance of activities involving counterterrorism-related model development, it will be possible to initiate selected data-collection efforts for obtaining further information about critical infrastructures and other relevant systems. However, because of the cost and time required for data collection, future modeling efforts must rely (at least in part) on data sources originally designed to serve other purposes. The use of current data resources for counterterrorism, however, requires the development of significant capabilities for data filtering, quality control, and other procedures to avoid inefficiency and information overload.

In a similar spirit, one of the major applications of database-management systems for countering terrorism will be data mining—the analysis of historical and current online data, often from disparate information sources, to discern patterns. Much work remains to be done, however, before attaining that capability. Today's commercial technology is highly dependent on clean, well-structured data, such as credit card transactions and cell-phone records, which might be scarce or nonexistent for suspected criminals and terrorists; thus the capacity to process other kinds of data will be needed. Moreover, nonstructured data such as text, images, and video are not especially well handled by commercial technology, although promising research in this area is currently under way. (For more discussion of data mining and information fusion, see Chapter 5, Information Technology.)

One major beneficiary of improved information management technologies would be the agencies responsible for gathering and analyzing intelligence data (including the FBI, CIA, and NSA). Currently one of their significant problems is managing a flood of data that may be relevant to their efforts to track suspected terrorists and their activities. There are well-known examples in which planned terrorist activities went undetected despite the fact that evidence was available to spot it—the relevant evidence was just one needle in a huge haystack. The use of sophisticated data-mining tools for the analysis of intelligence on nuclear smug-

gling and illicit weapons development programs will be particularly important in efforts to protect the nation from terrorist attacks using nuclear devices.

Another potential application of improved database systems is identification of trusted users of various systems. For example, in April 2002 the U.S. Customs Service launched the Customs-Trade Partnership Against Terrorism (C-TPAT).[2] C-TPAT "requires importers to take steps to assess, evolve and communicate new practices that ensure tighter security of cargo and enhanced security throughout the entire supply chain. In return, their goods and conveyances will receive expedited processing into the United States."[3] The goal is to provide an incentive to shippers to improve their own security procedures. In this case, good data and data analyses are essential for understanding normal patterns of shipping—and, thus, to know who to trust and who to scrutinize more carefully because of unusual or suspect patterns.

A trusted-fliers program has also been proposed and has been advocated by Governor Tom Ridge, director of the Office of Homeland Security. Frequent airline travelers would provide information about themselves to enable the airlines or the government to perform a background check on them and to know more about the characteristics and circumstances of passenger traffic. The advantage to the "trusted" traveler in providing this information would presumably be faster processing through security checkpoints if the background check indicated a low risk. More important, the information provided by travelers, coupled with data from other public and private sources, could allow the airlines and security authorities to gain a better understanding of normal patterns of travel and to spot unusual and suspect combinations of passengers on single flights and on multiple flights.

Some skepticism about whether this sort of data mining program would be possible or effective has been expressed by Congress, TSA, and the airlines.[4] Among the issues: What is the scope of the data that would be gathered? Who would be the users? What legal structures would protect the system's integrity and limit the potential for misuse? There are also systems-level technical issues that would affect the implementation of such programs.[5] To be sure, highly

---

[2]More details about C-TPAT are available on the U.S. Customs Service Web site at <http://www.customs.gov/enforcem/tpat.htm>.

[3]U.S. Customs Service press release of April 16, 2002.

[4]See Miller, Bill. 2002. "Ridge Pushes Fast-Track 'Trusted Fliers' Screening; Lawmakers, Airline Groups Express Doubts," *Washington Post*, p. A04, April 23.

[5]The issues associated with identity systems in general are discussed in *IDs—Not That Easy: Questions About Nationwide Identity Systems*, Computer Science and Telecommunications Board, National Research Council, 2002. The issues will also be explored further in an upcoming CSTB report specifically addressing authentication technologies; see <http://cstb.org/project_ authentication>.

sophisticated data management systems and decision-processing capabilities would be necessary to assemble and evaluate the needed data and to interpret and use the results. A goal of any of these trusted user programs would be to more effectively deploy screening resources, but good data management systems would be necessary to track the trusted users and to provide assurance that they really were trustworthy. Other new technologies, such as biometrics, might also be necessary to allow accurate identification of individuals who qualify as "trusted." However, biometrics, as discussed later in this section, are far from foolproof; for example, physical characteristics vary with age, and the data are subject to the time and conditions under which they were gathered.

Also, data mining has major privacy implications. Efforts to address these implications and mitigate their negative aspects include data-mining algorithms that discover general trends without requiring full disclosure of individuals' data records. Still, this zero-knowledge approach has limits. Attempts to identify terrorists could regularly require that an intelligence agency ask other government agencies and content providers for data on connections between individuals. (See Chapter 5 for more on privacy issues.)

Even in a nonterrorism context, data mining could save lives. For example, public health officials could collect and analyze real-time data describing admissions to hospital emergency rooms, monitor purchases of medications, inspect school-attendance records, and integrate this information with background information about the residence and job locations of affected patients both to pinpoint a biological outbreak and identify others at risk.

The development of database-management standards, though generally a lengthy process, is clearly needed. Such standards can be developed—possibly by industry/government agency consortia—if the members perceive sufficient value for their respective constituencies. In some cases, the government may assume funding responsibility. However, these standards efforts may not be successful if they are not well aligned with commercial markets, whose evolution—for the understanding of linked critical infrastructures and operational systems—would be a significant step toward developing data-collection systems and standards for counterterrorism applications.

SENSORS AND SENSOR NETWORKS

Because homeland defense against terrorist-delivered weapons of mass destruction will involve the entire spectrum of military and federal, state, and local government personnel, as well as volunteer organizations, the scenarios under which sensors will be needed and the protocols for their use may be as varied as each group's specific mission. The DOD and DOE have long been active in developing sensors, but these devices were intended largely for the protection of battlefield troops and the units that support them.

There are some important differences in the basic characteristics of military-

battlefield sensors and those for homeland defense. Established procedures, pre-engagement vaccination, and protective gear are well defined for the military battlefield scenario, but with the exception of some emergency response personnel, these are virtually nonexistent in the civilian sector. Further, military operations are generally conducted with the benefit of some intelligence data, giving some a priori specificity to the type of chemical, biological, or nuclear threat likely to be encountered. By contrast, terrorist use of weapons of mass destruction is less predictable. Finally, military operations may tolerate exposure levels that hurt but do not cripple unit effectiveness, whereas protection of the health of the civilian population to the maximum extent possible is a political mandate.

Nevertheless, sensors developed for battlefield detection of chemical, biological, and nuclear weapons represent a good starting point. But to meet the needs of homeland defense, it will be necessary to have sensors that provide the lowest achievable false-alarm rate, operate against the widest possible number of agents, and offer significantly improved sensitivity, specificity, and area coverage.

Because chemical, biological, and nuclear weapons each pose different threat scenarios, differences in sensors and their operational protocols must be considered.

Chemical weapons are point- or area-release, and their health impacts are generally seen immediately. However, they may be detectable before actual deployment. Trace amounts of chemical contaminant can be detected on the package containing the weapon and even on the individual transporting it. Current sensor capabilities are fairly limited; in many cases, the best "technology" for practical use continues to be trained dogs, which provide broad-spectrum high-sensitivity sensing. Manufactured sensors are often designed for use in specific environments and to be selective for only one or two chemicals. The development of new sensor systems for chemical agents will require advances in a number of different subsystems, including sample collection and processing, presentation of the chemicals to the sensor, sensor arrays with molecular recognition, sophisticated signal processing, and amplification of the transduction events. The precise chemical signals that provoke responses in dogs remain uncertain, and basic research to study how animal species accomplish both detection and identification of trace chemicals could yield new concepts for manufacturing better sensor systems. (See Chapter 4 for more on chemical sensors.)

Biological weapons can also be point- or area-release, but their health impacts may not become apparent for days or weeks. Further, it is problematic whether trace amounts of a biological agent will be discernible, so that the first opportunity to detect it may be at release. Thus the rapid diagnosis, treatment, and recognition of the weapon that caused the illness is very important. Equally important is the flow of rapid and reliable information throughout the health-care community, particularly in the early stages of recognition of a bioterrorist attack.

The classic means of surveillance of biological agents is to identify patients

with an unusual disease or syndrome and to then establish the nature of the pathogen by standard laboratory diagnosis. Physical sensors that screen for aerosolized particles, and molecular probes that establish the nature of the organism, would complement the classic process and permit quicker analyses. There is also the possibility of symptomatic surveillance—real-time screening in hospital emergency rooms of syndromes such as flulike illness, diarrhea, and rashes and spots. By feeding such data into sophisticated computer models, it may be possible to detect subtle fluctuations in symptomatic admissions, suggesting that something above the background rate of illness, such as a bioterrorist attack, is occurring.

One of the most exciting possibilities for early detection of a biological outbreak is preclinical diagnosis. With the elucidation of the DNA sequence of the human genome, it may be possible to examine selective patterns of gene mutation induced by different biological agents in humans long before the actual organism has been detected. As we learn more about the pathogenesis of different agents and the specific bodily responses mounted against them, it may turn out that each pathogen induces a unique molecular signature in the host gene-expression response. Thus, using DNA chips, it may someday be possible, without ever having to culture suspected agents, to know what type and perhaps what species we are encountering—and to commence focused and rapid treatment accordingly. (See Chapter 3 for more on detection of biological outbreaks.)

An important line of defense in a layered system of homeland protection is the detection and interdiction of illicit nuclear weapons and special nuclear material (SNM), as well as the detection and disruption of illicit weapons development programs. Sensors and sensor networks can contribute to this defense effort by providing technical means for detecting the movement of SNM, especially highly enriched uranium (HEU), either in weapons or as contraband, through border transit points and around critical U.S. assets such as ports, cities, and other high-value facilities. A national detection network could consist of several types of sensors: large numbers of simple counters that indicate the presence of radiation, backed up by smaller numbers of spectroscopic instruments to identify specific isotopic signatures. The technical challenge for the deployment of both types of sensors is the differentiation of signals of interest from the background of naturally occurring radioactivity and medical/industrial radioisotopes.

The presence of certain types of penetrating radiation is a signature of most (but not all) SNM. Passive detection of gamma rays and/or neutrons can be an effective technique in some circumstances for revealing the presence of illicit SNM or improvised nuclear devices (INDs), though passive monitoring of these materials would require large-area detectors for acceptable sensitivity. In other cases, active interrogation methods using neutron detectors and pulsed neutron sources may be required. Active systems are more complex and costly than passive detectors. Additionally, some materials (those with high atomic number) can be detected indirectly by gamma radiography. While shielding of SNM can

interfere with the signals produced by all of these detection methods, the systems could still serve as a useful first indicator of a wide spectrum of potential threats. In the near term, improvements in neutron interrogation sources (i.e., neutron generators) and detectors for HEU would be a very useful step toward increasing our detection capabilities. (See Chapter 2 for more on sensors of nuclear materials.)

In addition to detection of chemical, biological, and nuclear agents or weapons, sensor systems can also be used to produce images. In particular, remote sensing technologies, such as light detection and ranging (LIDAR), synthetic aperture radar (SAR), and high-resolution satellite imagery, can be used for surveillence or during emergency response and cleanup efforts.[6]

Whatever type of attack the sensors are designed to prevent or respond to, the roles that sensor systems play can be described in terms of four specific categories—threat warning; incident response; treatment; and recovery and attribution—each with its own set of requirements:

- *Threat warning* covers point-of-entry monitoring for preattack detection, as well as area monitoring of presumed target areas. Simply because the number of sensors required for area monitoring is great, it is necessary that they be low-cost, small, fixed in place, and highly sensitive (as opposed to selective). Also, maximum utility from area monitoring will require networking the sensors, thereby allowing for higher-level evaluation of a potential threat.
- *Incident response* scenarios, by contrast, require handheld portable sensors and minimal training for operators. Both point sensors (for site characterization) and short-range standoff sensors (for site evaluation prior to entry) will be of value. Incident response will occur at a critical time for evaluating and controlling the severity of the attack, but this will also be the time of weakest coordination as personnel from federal, state, and local governments come onto the scene. A mechanism for networking data from sensors carried by these people would allow a single picture of the threat to evolve more quickly.
- For *treatment*, the sensors' greatest contribution will be made in the aftermath of a biological attack. They should be able to provide quick and accurate diagnoses, without the hours or days of time lag associated with standard culture-growth techniques.
- For *recovery* and *attribution*, the speed at which information is available is usually less important than the accuracy of the data. For recovery, sensors would be useful for monitoring the level of contamination at a site during and after cleanup activities. For attribution, the goal would be the use of sensors in

[6]After 9/11, LIDAR technologies allowed engineers to start evaluating the dimensions of debris piles and the zones of heat and fire at the World Trade Center even when smoke still surrounded the site.

forensic investigations to determine the source of a terrorist attack or to assign responsibility.

Recent research and development, focusing most heavily on portable sensors for chemical and biological agents, has followed two basic paths. The first is a repackaging of standard laboratory-analysis techniques for field use, and it includes various methods of spectroscopy. The second basic path has been in the introduction of new affinity-based sensors, in which the chemical or biological agent is selectively bound to a surface through use of a specialized surface coating; the presence or absence of the agent on the surface is then measured by one of several mechanical, electrical, or optical transduction methods. The sensitivity, selectivity, quantification, and time response of these affinity-based sensors are functions of the specialized coatings and signal-transduction methods used.

Spectroscopy methods—the first path—tend to be more general-purpose, with a single instrument being useful for detection of a number of agents. In contrast, to use affinity-based instruments for detection of multiple agents, an array of sensors is needed where the elements of the array receive a variety of coatings, each specialized to allow detection of a specific chemical or biological agent.

Either way, to carry sensor-system performance to the level needed, homeland defense will require not only continued improvement in basic sensor performance but also a better definition and understanding of *overall* performance—when many sensors are networked together. A number of factors will contribute to effective functioning of sensor networks. Communications protocols will be needed, and network architecture issues associated with connectivity, bandwidth allocation, signal processing, and data fusion must also be addressed

In particular, algorithms for detection in the presence of significant clutter must be developed, with a focus on achieving excellent detection capability while minimizing false alarms. In many instances, the impact of false alarms will depend on circumstances. The trade-offs between false positives and false negatives and the consequences of each must take into account how the system can be used most effectively. Issues will include the system in which the sensors are installed (e.g., Are there backup or alternate security checks?), the users of the outputs (e.g., first responders, scientists supervising recovery efforts), and the time scales on which decisions about what to do with the results must be made.

The next important step is to address the detection of weapons of mass destruction from a systems-engineering perspective, which spans the capture/collection of the sample, preparation of the sample, reliable delivery of the sample to the sensor, sensor interrogation (including background and metric verification), analysis of the signal, and reporting of the data from individual sensors. This perspective can be enhanced to include redundancy issues and other performance enhancements achieved from multiple networked sensors. Several other attributes will accrue from this system-design approach:

- Establishment of standards—covering response time and field stability/durability, for example—for detection of weapons of mass destruction;
- Use of two-level sensor systems in which a low-false-alarm-rate sensor—one with low specificity—triggers a second sensor with a higher false-alarm rate but high specificity;
- Use of multiple sensors and reasoning algorithms to obtain lower overall false-alarm probability, predict contamination spread, and provide guidance for recovery actions; and
- Use of networked sensors to provide wide-area protection of high-threat targets.

Also important is the continued development of individual sensor modalities. Significant work on chemical and biological sensors in particular is a relatively recent phenomenon. As these efforts proceed and as new data-analysis algorithms are applied to sensor outputs, improvements may be expected in many of these instruments' sensitivity, selectivity, false-alarm probability, size, power, and cost. In addition to the need for continued basic sensor work for point-of-entry monitoring and incident-response applications, equally critical technological and economic challenges will involve developing affinity-based sensors that can be cost-effectively networked to provide wide-area monitoring.

AUTONOMOUS MOBILE ROBOTIC TECHNOLOGIES

Robotic technologies can impact all phases of counterterrorism, including detection, prevention, and response. Robots' abilities to sense and manipulate the environment with great precision, in the absence of such human limitations as physical vulnerability, fear, boredom, and discomfort, make them ideal tools for extending operational reach. Robots can serve homeland-defense missions (including surveillance and protection of population centers, facilities, and assets, and rescue or cleanup in response to an attack) as well as tactical/offensive missions (such as intelligence collection, demining, and direct action). (See Chapters 4 and 8 for more on possible counterterrorism applications of robotic technologies.)

Ground robots may be loosely described as small (<50 lb), medium (51 to 1,000 lb), and large (>1,000 lb). Small robots are light and compact enough to be carried by humans, and it is expected that their inherent ease of handling, transport, and relatively low cost will result in their proliferation. Several small-robot prototypes have been developed under the DARPA Tactical Mobile Robotics (TMR) project and other government programs. Though their small size severely limits their operating range, duration, and mobility in outdoor or unstructured terrain, they are critical for reaching otherwise inaccessible spaces. Applications for such robots include intrusive intelligence-gathering missions (in which small size is critical); area sampling for nuclear, biological, and chemical contamination; close-in surveillance; and urban search-and-rescue operations.

Medium-size robots have greater mobility, energy reserves, and space for additional hardware such as sensors, manipulators, communications gear, and payloads. These robots are transportable by light vehicles—including pickup trucks, vans, small trailers, and high-mobility, multipurpose wheeled vehicles (HMMWVs)—that would be widely available to many potential users. Their current applications include explosive-ordnance disposal (with dedicated manipulators and payloads for removing or disabling unexploded devices), physical security (asset/facility monitoring), hazardous-waste inspection/remediation systems, and law enforcement operations. New initiatives under the DARPA/Army Future Combat Systems and Office of Naval Research Gladiator programs suggest that in the next 5 years vehicle platforms of this size may also serve as forward scouts, sentries, surveillance and target-acquisition platforms, communication relays, resupply/logistics vehicles, and even firing platforms.

Large robots will also have value for counterterrorism missions. Teleoperated or semiautonomous, they can be used for mine clearing, obstacle breaching, construction, fire-fighting, and rubble removal, particularly in areas contaminated by chemical, biological, or nuclear weapons.

The ability of a robot to perform a specific mission will depend on the robotic system's level and "distribution" (whether on-board or off-board) of autonomy. These factors depend, in turn, on the expected integrity of the operator–robot communications link, the maximum length of time the robot might be out of contact with the operator, the robot's knowledge of its location in the world and with respect to the operator, the robot's knowledge of its internal health, and the robot's knowledge of its environment.

The basic types of system autonomy include:

- *Teleoperated systems*, which primarily use the intelligence of a human operator to operate the system during execution of a mission;
- *Scripted autonomous systems*, in which the guidance, navigation, and control (GN&C) systems are typically autonomous but the mission profile is significantly constrained;
- *Supervised autonomous systems*, which include a human operator (via a communications link) who assists in the interpretation of sensor information and provides situational awareness and mission guidance to the robot; and
- *Intelligent autonomous systems*, which use robot-embedded software for incorporating many of the attributes of human intelligence.

From these basic descriptions, the level of robot autonomy can be viewed as a composite of the level of guidance and control, the level of autonomous planning and tasking, the level of situational awareness (i.e., perception), and the level of self-awareness (diagnosis).

The level of guidance and control is characterized by the degree to which a robot has the ability to create a desired motion without human involvement. Where teleoperation of a robot assumes a "drive" camera and communication

link for direct operator control, autonomous/adaptive GN&C allows the robotic system to automatically adjust to changes in the robotic-system configuration (e.g., mass properties, failures) or changes in the operating environment (e.g., obstacles, lighting conditions). Additional research in guidance technology is required to enable autonomous systems to perform at levels similar to what is achievable by a human operator or pilot when given the same degree of situational awareness.

Robot planning and decision making are characterized by the extent to which the robot can plan its mission activities, motion, usage of payloads, and specific goals to be achieved without human involvement. This must be accomplished within certain limits, which may include specific mission rules and constraints on robot consumables (e.g., power, fuel, memory). Most common today are systems that plan robot routes (path planning) or schedule devices (automated scheduling). Several government S&T programs have demonstrated either dynamic path planning (that is, in environments without fixed infrastructure) or automated, continuous device scheduling. Activity planning, which involves the coordination of multiple robot subsystems, is a critical research area for the future.

Robots typically communicate data to a central command-and-control site via uplink and receive commands via downlink. Teleoperated robots have requirements for high-bandwidth links (including video), while semiautonomous robots do not. For systems of cooperating robots, the need for maintaining reliable network connectivity will be critical. Point-to-point links are defined by operating frequency, data rate, range, transmitter power, and receiver sensitivity. The optimal choice of frequencies used in the point-to-point links will be environment-dependent and must be traded off with other factors, such as range and data rate. In any case, robot control links must be robust in the presence of multipath interference. A variety of strategies for mitigating multipath interference exist, including spread spectrum. For tactical applications, communication links must also satisfy detection, interception, jamming, and encryption requirements.

Where groups of robots must collaborate, base-station based and peer-to-peer networks can be considered. A base-station-based architecture is characterized by a number of nodes communicating with a central hub. Peer-to-peer mobile ad hoc network (MANET) architecture may be more appropriate for dynamic environments (characterized by moving robots). MANET architectures are reconfigurable over time and space and do not have a single point of failure.

SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEMS

Specialized computer software systems, known as supervisory control and data acquisition (SCADA) systems, are widely used to control many essential real-time processes, including the generation and distribution of electric power, the management of oil and natural gas pipelines, and the monitoring of engineer-

ing systems in buildings, petrochemical facilities, and manufacturing plants. But today's SCADA systems have been designed with minimal attention to security. For example, data are often sent in the clear, and protocols for accepting commands are open, with no authentication required. Control channels are often wireless, or they are leased lines that pass through commercial telecommunications facilities. Thus there is little protection against the forgery of messages. And data corruption—not unlikely in these SCADA systems, much of whose technology is old—could be entirely crippling.

In addition, because deregulation has meant placing a premium on using existing capacity more efficiently, interconnections to shift supply from one location to another have increased, making SCADA systems more indispensable than ever. As one example, the electric-power grid has become more heterogeneous in terms of the number and types of power-generation devices—solar cells, microturbines, and many other sources all contribute to the network from far-flung locations. Thus, problems of distributed dynamic control in a complex, highly interactive system, controlled in real time, have become major issues in operating the power grid reliably, even under routine conditions.

Making the present systems more secure, moreover, is not simply a question of installing additional layers of technology. Given the real-time nature of SCADA, timing is quite important to system performance and optimal efficiency; operations can demand millisecond accuracy. But security add-ons in such an environment can complicate timing estimates and severely degrade SCADA performance.

Several issues must be addressed in the effort to improve the security of SCADA technologies. First, there is a need for much additional research and modeling on the existing SCADA systems, especially those that monitor networks such as pipelines or power grids, in order to understand their vulnerabilities. Some of this modeling and analysis must be undertaken by the operators themselves, and indeed this has begun since September 11; the chemical industry, for one, reports that SCADA systems in refineries have been under review. There is also a role for government at both the national and state levels—for example, in detecting vulnerabilities in present systems through comprehensive gaming (red teaming) analysis.

Second, investments will have to be made if existing SCADA technologies are to be upgraded and new ones deployed. Federal and state governments should offer incentives that encourage the appropriate private sector investments.

Third, the government must work with industry associations on standards that will enhance both the technology and its security. The National Institute of Standards and Technology, which has long played such a role at the federal level, should lead this effort.

SCADA systems are discussed further in Chapter 5 ("Information Technology") and Chapter 6 ("Energy Systems").

BIOMETRICS

Every society exists somewhere on the spectrum between complete openness and total restriction of behavior and movement. In the United States, we are proud of our society's extremely open nature, but that asset is also a basic element of its vulnerability to terrorism.

An obvious solution is increased physical and information-technology security, though the appropriate level of security should not be uniform throughout the country. It would depend on the type of facility or system being guarded, the potential damage if an intrusion occurs, and the degree to which security interferes with effective functioning of the system. Clearly, the rules for nuclear power plants should be different from those for buses.

One developing set of technologies that could play a role across the board—ranging from major to minor, depending on the specific case—is biometrics. In authorizing participants in any particular system—physical or IT security alike—biometrics may provide alternatives to picture IDs, magnetic entry cards, or passwords.

Biometrics uses behavioral and physiological characteristics—including fingerprints, irises, written signatures, faces, voices, and hand shape—to authenticate the identity of an individual. These characteristics are distinctive but not necessarily unique, and they can vary over time and conditions of collection and may change with medical condition, advancing age, or the onset of puberty. Still, biometric identification may provide a higher level of confidence for the authentication of identity than can devices such as passwords. And, as opposed to other authentication tokens that might be used (such as keys), biometric measures cannot easily be stolen or mimicked. However, biometrics must be part of a multifactor authentication scheme rather than a one-stop solution. Biometric authentication is most applicable to sensitive applications in which the security risk of a false positive (an imposter being accepted as legitimate) is much higher than that of a false negative (an authorized individual being rejected as illegitimate). Several U.S. government projects are currently aimed at improving the distinctiveness of individual measures and exploring "biometric data fusion" for combining multiple measures. Such advances would allow for almost one-to-one mappings of measure sets to individuals, making the technology exceedingly reliable but also more subject to privacy abuses.[7]

On a less invasive level, biometrics at more or less its present state could enhance the protective value of more traditional security systems. While the technological elements behind barriers, fences, locks, perimeters, and other physical ways of safeguarding a location—as well as nonphysical approaches such as

[7]Authentication technologies (including biometrics) and their implications for privacy will be explored in depth in a forthcoming CSTB report from the Committee on Authentication Technologies and Their Privacy Implications; see information available online at <http://cstb.org/project_authentication>.

background checks—may not be new or exciting, they complement approaches such as biometrics. The joint use of traditional and newer technologies might thus allow exploitation of the latter while minimizing their need for potentially intrusive refinements.

HUMAN AND ORGANIZATIONAL FACTORS

The organizing principle of this report is that our nation's store of scientific and technological knowledge—as it exists and as it must be improved—is a key resource in efforts to counter the threat of terrorism. This knowledge is the basis for effective intelligence and military operations against terrorism, for securing our borders and other points of entry, and for making inaccessible the many targets of terrorist activities.

However, technology is not the sole solution to any problem. Virtually all technologies—including those discussed in this report—are subject to the reality that human agents and social organizations are necessary to implement and operate them. Decision makers oversee warning systems, human agents administer detectors, relief efforts following chemical or biological attack require the collective efforts of the nation's health machinery, and precision warfare is a highly orchestrated human activity. A key aspect in the effective deployment of any of the technologies discussed in this report is the ease and effectiveness of use of information and other technical outputs by the people they are intended to support. Thus design and deployment of the systems must take human, social, and organizational factors into account.

In efforts to counter terrorism, the human interface with technology appears at three junctures:

- *Those who are recruited to administer the technologies of detection, prevention, and response to attack not only have to be expert but also trustworthy and loyal.* Few forms of sabotage are more effective than sabotage from within. Guaranteeing this side of security, however, can become a matter of government compulsivity and a potential source of inefficiency and ineffectiveness. Some kind of equilibrium, which takes into account both the value of prudence and the dangers of overkill, is required.
- *All types of counterterrorism-related technological systems require the mobilization of organizational machinery.* In many cases, their missions take place under crisis conditions, which multiply the probabilities of accidents, breakdowns of communication, lack of coordination, errors of judgment, and jurisdictional conflicts. There is no sure cure for such failures, but advanced training and instruction of agents, as well as comprehensive planning for contingencies and backup strategies, are essential.
- *Sometimes the applications of science and technology in the interests of security run counter to cherished individual and political values.* Wholesale

detection efforts at airport terminals and other hubs of transportation are simultaneously experienced as comforting and as costly, inefficient, irritating, and invasive. The use of high-tech identifying and truth-detecting devices may have similar alienating effects. Surveillance of telephones, credit records, and personal movements in the interests of security also raises serious questions about privacy and civil liberties. The systems perspective that should be used to determine criteria for deployment of technologies must embrace this reality as well; there are many ways to remedy the vulnerabilities of our nation's critical infrastructures, and the best solutions must reflect a balance between the desire for security and human values.

Often, the weakest part of the system is the (frequently neglected) human link. Overlooking the human element can make it more difficult for staff members to do their jobs and, ironically, significantly reduce the effectiveness of the security technologies. In the worst case, the entire system may be rendered useless. Thus, human-centric design and an improved understanding of the factors that contribute to systematic human errors are essential.

Most people are inherently helpful and dependable and are responsive in the face of unforeseen circumstances. We must take into account their strengths—the attributes that no technology could duplicate—while avoiding, to the maximum extent possible, the creation of jobs that are tedious and unrewarding. This must be a basic element of our systems approach. We need to allow for defense in depth (multiple layers) to compensate for human error, of course, but good system design should be characterized by human roles in which vigilance and interest are heightened, thereby making errors less likely.

Such human factors in design must apply equally well to the operators of the security system and to those who encounter it.

COORDINATION OF PROGRAMS ON CROSSCUTTING TECHNOLOGIES

The nation's capabilities for pursuing an expanded and coordinated S&T agenda for the crosscutting technologies identified in this chapter are considerable. A number of programs with broad applicability to these technologies have already been established within DOD, DOE, NSF, and NASA, and relevant research is under way at these agencies, in the national laboratories, and at scores of research universities. For example, in recent years, as concern about terrorism has grown and as the post-Cold War powers have focused on safeguarding nuclear materials, the DOE national laboratories have already begun researching sensors and other detection technologies, as well as data management, visualization, and modeling pertinent to counterterrorism. The DOE laboratories also have expertise in both the physical and biological sciences, as is needed for such crosscutting R&D initiatives, and are performing advanced work in the key fields of

information technology and nanoscale science. Similarly, important and relevant activities are occurring throughout other government agencies.

A mechanism is needed for coordinating all of this work in crosscutting areas across agencies. The logical approach would be to use a National Science and Technology Council (NSTC) subcommittee. The NSTC was established in 1993, and one of its objectives "is the establishment of clear national goals for Federal science and technology investments."[8] Subcommittees of the NSTC are often formed in areas such as climate change, biotechnology, and nanoscale science, engineering, and technology, where multiple agencies need to work together toward a common set of goals. Such subcommittees make decisions about programs and provide OMB with the information necessary to produce budget crosscuts showing the amount of resources and types of programs devoted to a specific area across the federal government.

Recommendation 11.1: The National Science and Technology Council should establish a Subcommittee for Counterterrorism Research and Development to, among other tasks, coordinate federal work on crosscutting technologies such as modeling and simulation, data management, sensors and sensor networks, and robotics. The subcommittee should have participation from the highest levels of the relevant agencies.

CONCLUSIONS

This chapter has outlined the potential impact of seven crosscutting areas—systems analysis and modeling, integrated data management, sensors and sensor networks, robotic technologies, SCADA systems, biometrics, and human factors—on counterterrorism efforts. The realization of this potential will depend on a program of directed basic and applied research and will require an expansion and coordination of existing S&T programs and funding if the government's work is to produce effective tools for countering terrorism and ensuring homeland security.

There are three problems with the current level of effort. First, it is too small. It is clear that solutions for current vulnerabilities and the ability to tackle future problems lie in innovations and discoveries in the biological sciences, physical sciences, and all fields of engineering, as well as at the interfaces of these disciplines and in the relevant social sciences. Therefore a balance of investments is critical, across different time horizons as well as across numerous disciplines. The government's underinvestment in the physical sciences and engineering has

[8]National Science and Technology Council Web site: <http://www.ostp.gov/NSTC/html/NSTC_Home.html>.

been documented in a variety of reports[9] and is discussed further in the section on universities in Chapter 13.

A second problem with the current level of effort is its focus. Programs are tied to the existing missions of the agencies, as is appropriate. This means that while some of the R&D may be applicable to the technologies for homeland security, the present federal effort does not add up to the research and development program that is needed. In robotics, for example, NSF has long had a relatively small program conducted at several universities and focused on fundamental research. NASA has funded robotics R&D that supports its missions in space. DOD has invested heavily, through the individual armed services and DARPA, in unmanned aircraft for sensing and surveillance. Historically, DOE's efforts in robotics have been associated with nuclear materials handling, although recently the agency's laboratories have initiated some substantial programs that may contribute to improved homeland security in many ways. Private-sector investments in robotics follow a similar pattern—for example, the automotive companies are investing in robotic R&D that will support their production and assembly lines, and energy and water providers are developing robots useful for monitoring fuels pipelines and aqueducts. The work under way is productive and important new technologies are being developed, but even added together, these public and private investments will not produce robots that can be adapted and deployed for many purposes in homeland security—such as surveillance, detection, and postdisaster monitoring and recovery.

The same pattern—R&D investments that are significant but not directly focused on homeland security needs—exists in the other areas of crosscutting technologies and techniques discussed in this report. Each agency has molded its programs in the context of its own objectives.

The third problem with present R&D efforts in these fields is that the programs are directed to issues largely in the domain or purview of the federal government—defense, space, and nuclear security and stockpile maintenance being prototypical examples. The crosscutting R&D efforts that will serve home-

---

[9]Data on and analysis of the federal budget for science and technology are available from a number of sources, including National Research Council, Board on Science, Technology, and Economic Policy, 2001, *Trends in Federal Support of Research and Graduate Education,* National Academy Press, Washington, D.C.; Committee on Science, Engineering, and Public Policy, National Research Council, 2001, *Observations on the President's Fiscal Year 2002 Federal Science and Technology Budget,* National Academy Press, Washington, D.C.; American Association for the Advancement of Science, 2001, *AAAS Report XXVI: Research and Development FY 2002,* American Association for the Advancement of Science, Washington, D.C.; American Association for the Advancement of Science, 2002, *Congressional Action on Research and Development in the FY 2002 Budget*, presentation materials from the Alliance for Science and Technology Research in America (ASTRA), Washington, D.C., available online at <http://www.cra.org/govaffairs/budget/astra.pdf>; and National Science Board, National Science Foundation, 2002, *Science and Engineering Indicators—2002,* U.S. Government Printing Office, Washington, D.C.

land security require collaborations with end users at the state and local levels of government so that programs can take into account the needs of these users, like technologies for first responders. Further, federal programs must be designed with an understanding of the critical role industry will play as a developer, producer, and user of counterterrorism technologies. Important questions include who the consumer of these technologies will be, whether there will be a commercial market for new products, and what role government procurement can productively play.

Despite these problems, the nation's research system, with vast and diverse capabilities spread among universities, national and federal laboratories, and industry, provides a unique infrastructure and sound basis for mounting aggressive programs in the kinds of crosscutting R&D discussed in this chapter. The challenge for government leaders is to harness this capacity for the creation of a greatly expanded and coordinated national S&T agenda for counterterrorism. This will require a commitment to providing significant new funding and to sustaining the programs over a number of years.

12

Equipping the Federal Government to Counter Terrorism

INTRODUCTION

The mere articulation of a science and technology agenda to combat terrorism will do nothing to enhance the security of our country. We must *act* on that agenda, responding with creativity and effectiveness to a dramatically new kind of threat, one not faced before in the nation's history. Existing technologies must be deployed and new technologies must be invented. Federal responsibilities and authorities need to be clarified. Existing institutions may gain capabilities, and some new missions could require the founding of new institutions. Obstacles to using our most potent resources for countering catastrophic terrorism must be identified and overcome.

This report does not purport to offer an enduring technological strategy for countering terrorism. The threat the nation faces is so multifaceted, so subject to changes (both in national vulnerabilities and in potential terrorists' intentions) that a strategy to meet just the already-evident threats would be shortsighted. Furthermore, the best research and development program is of little value if what is learned along the way is not implemented in a timely and strategic fashion. This places great responsibility not only on the nation's research community but also on the leaders of government agencies, who must access and utilize systematic thinking, managerial agility, and technical imagination. Specifically, we must be positioned to anticipate the terrorist threats, devise ways to make them less likely or less damaging, set priorities among the ever-changing array of threats, and, through innovation, reduce the dangers that our society and its people face.

The events of 9/11 dramatized U.S. vulnerability to terrorism and coalesced

a national will to act, but earlier experiences and analyses may also help shape our responses to the present dangers. A number of high-level commissions, most of them established after the first terrorist attack on the World Trade Center in 1993, not only addressed terrorist threats but also specifically called attention to the critical importance of science and technology in addressing them.[1] The committee has drawn upon these prior reports because they reflect careful thinking and precedents, as well as concern about the proper organization and coordination of governmental action against terrorism.

All these studies not only underscore the importance of science and technology (S&T) in countering terrorism but also conclude, as did this committee, that the government will have to change how it sets goals for scientific and engineering programs and manages technology development if science and technology are to be effectively applied to that purpose. Repeatedly, these reports—including those of the Gilmore Commission, the Bremer Commission, the Hart/Rudman Commission, and the Marsh Commission—have noted the importance of developing a national strategy for combating terrorism and the need for organizing government to better implement it.

The Gilmore Commission (2000) concluded that "the United States has no coherent, functional national strategy for combating terrorism" and recommended that "the next President should develop and present one to the Congress within one year of assuming office."[2] It presented attributes of a "comprehensive and functional strategy for combating terrorism" and urged that it be "appropriately resourced and based on measurable performance objectives." But the commission believed that government was poorly positioned to devise such a strategy. The "organization of the federal government's programs for combating terrorism," it wrote, "is fragmented, uncoordinated, and politically unaccountable."[3] It

---

[1]*Second Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Gilmore Commission, December 2000); *Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Gilmore Commission, December 2001); *Countering the Changing Threat of International Terrorism* (National Commission on Terrorism) (Bremer Commission, September 2000); *Road Map for National Security: Imperative for Change* (U.S. Commission on National Security/21st Century) (Hart-Rudman Commission, Phase III, February 2001); *Critical Foundations* (The President's Commission on Critical Infrastructure) (Marsh Commission, Fall 1997). Also see *Combating Proliferation of Weapons of Mass Destruction* (Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction) (Deutch Commission, Spring 1999); *Preparing for the 21st Century—An Appraisal of U.S. Intelligence* (Commission on the Roles and Capabilities of the United States Intelligence Community) (Brown Commission, March 1996); *Joint Task Force on Intelligence and Law Enforcement Report to the Attorney General and Director of Central Intelligence* (Richards/Rindskopf Report, May 1995).

[2]Gilmore Commission Second Annual Report, 2000, at p. 2.

[3]*Ibid.*, Finding 2, at 4.

noted that there was a need for a national office to "establish a clear set of priorities for research and development for combating terrorism, including long-range programs" and to "coordinate the development of nationally recognized standards for equipment, training, and laboratory protocols and techniques, with the ultimate objective being official certification."[4]

The Bremer Commission (2000) recommended that "the President should establish a comprehensive and coordinated long-term research and development program for catastrophic terrorism."[5] The Hart-Rudman Commission report (2001) laid out the factors driving the need for such a program: "The inadequacies of our systems of research and education pose a greater threat to U.S. national security over the next quarter-century than any potential conventional war that we might imagine. We recommend that the role of the President's Science Advisor be elevated to oversee . . . critical tasks such as . . . the institution of better inventory stewardship over the nation's science and technology assets."[6] The President's Commission on Critical Infrastructure (Marsh Commission, 1997) focused on better use of existing technology and on new research to expand capabilities: "The Commission believes that some of the basic technology needed to improve infrastructure protection already exists, but needs to be widely deployed. In other areas, additional research effort is needed."[7]

These quotes merely exemplify the many findings and recommendations of previous high-level reports, which reflected a common set of concerns about the government's ability to organize its actions against terrorism. Unfortunately, they were largely ignored until 9/11. This chapter is therefore predicated on the assumption that the government *must now act immediately* to create the necessary structures for formulating, funding, overseeing, and managing a sustained and successful national program.

In this chapter, the committee focuses on factors that affect the government's capacity to implement a national strategy for the use of science and technology to counter terrorism. In the first section below, it discusses the issues that drive the need for coordination across the federal government and the capabilities needed for effectively defining priorities and managing programs. It then briefly discusses the role of federal agencies in executing their respective portions of the overall strategy (more details about specific actions for particular agencies can be found in Chapters 2 to 10 of this report).

---

[4]*Ibid.,* "Specific Functional Recommendations," at 9.
[5]Bremer Commission Report, September 2000, at v.
[6]Hart-Rudman Commission Report, 2001, at ix.
[7]Marsh Commission Report, 1997, at 8.

MANAGING THE FEDERAL GOVERNMENT'S PROGRAM OF SCIENCE AND TECHNOLOGY FOR COUNTERING TERRORISM

Current Situation

The structure of federal agencies is the product of history, to a large extent the result of the Cold War and of the traditional distinction between the responsibility for national security and the responsibility for domestic policy. Federal agencies are structured to deal with problems that can be partitioned into war or criminal justice, national or foreign affairs, short-term or long-term strategy, and public or private duty. Given this compartmentalization, the federal government is not appropriately organized to carry out an S&T agenda for countering catastrophic terrorism. Making the task even harder, the S&T resources are in one set of agencies and the homeland-defense missions in another; federal and state responsibilities are overlapping; and the critical infrastructure systems owned and operated by the private sector are attractive terrorist targets. It is clear that the task of designing S&T efforts to counter terrorism, of assigning responsibilities among federal agencies, and of monitoring and managing their performance is daunting indeed.

Issues Driving the Need for Coordination Across the Federal Government

A number of factors are driving the need for an unprecedented level of coordination across the federal government. One important factor is the minimal overlap between the agencies that have historically performed innovative research that could now be applied to counterterrorism and the agencies with operational missions in homeland security. This issue is discussed in the penultimate section of this chapter, on the role of the federal agencies in developing and using science and technology for countering terrorism.

Another factor driving the need for coordination of counterterrorism activities in the federal government is the crosscutting nature and broad applicability of many of the most relevant technologies. This issue is discussed at length in Chapter 11. One example of a crosscutting technology is sensor networks, which have the potential to mitigate a variety of threats and to facilitate rapid response to a variety of attacks. Yet the research needed to build a viable system of sensors occurs in many fields (chemistry, biology, physics, and information technology, among others), is supported by many agencies (such as NSF, DARPA, and DOE), is performed in multiple sectors (universities, national laboratories, industry), and ultimately must be deployed as one element in an integrated security system.

A third factor contributing to the need for government coordination is the complex and diverse nature of the systems that may be terrorist targets. A systems approach must be taken in order to understand the vulnerabilities and define the S&T goals even within just one system, such as the electric power grid

or the shipping system (see the discussions in Chapters 6 and 7). Yet none of these systems operates in isolation, and the government will need new capabilities to understand the impact of the linkages between them and to make informed decisions about national priorities across all potential targets. This effort will require the creation of testable models of elements of the nation's critical infrastructure, utilization of red teams to evaluate the performance of protective measures, promulgation of standards to allow interoperability of counterterrorism technologies, development of testbeds, and research to improve implementation and deployment. How the government might gain these capabilities is discussed in more detail later in this chapter.

The final factor that points to the federal government's need to pull together a coherent strategy for counterterrorism activities is this: Success will depend critically on the efforts not only of the federal government but also of state and local governments, private industry, and universities. The relationships among these sectors involve a complex set of issues that are discussed in Chapter 13 of this report.

Strengthening the Federal Government's Ability to Determine How S&T Can Be Used to Counter Terrorism

One approach to addressing the need for coordination could be to ask Congress to restructure the federal agencies to reflect the close working relationships that are required. On June 6, 2002, President Bush released a plan intended to do just that.[8] He proposed that a new cabinet-level Department of Homeland Security be formed as a conglomeration of existing agencies and programs.[9] In the interim, the Office of Homeland Security (OHS) "will continue to coordinate the federal government's homeland security efforts and to advise the President on a comprehensive Homeland Security strategy."[10]

Below, the committee discusses a number of the factors affecting the government's ability to determine a counterterrorism strategy and efficiently

---

[8]The President's June 6, 2002 "Address to the Nation on the New Department of Homeland Security" is available online at <http://www.whitehouse.gov/news/releases/2002/06/20020606-8.html>.

[9]The mission of the proposed Department of Homeland Security would be to "prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, and minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States." The department would be organized into four divisions: Information Analysis and Infrastructure Protection; Chemical, Biological, Radiological, and Nuclear Countermeasures; Border and Transportation Security; and Emergency Preparedness and Response (the Homeland Security Act of 2002, available online at <http://www.whitehouse.gov/deptofhomeland/bill/index.html>).

[10]"White House proposal for the Department of Homeland Security," p. 4. Available online at <http://www.whitehouse.gov/deptofhomeland/book.pdf>.

execute such a strategy. While the proposed new department has the potential to facilitate closer relationships between key agencies and to improve the federal government's ability to pursue a coherent set of counterterrorism programs and actions, the process for congressional action on this plan and the resulting transfer of authority and functions to a new department will take time. In addition, the key requirement for an effective contribution to the nation's safety from science, engineering, and medicine depends not on the government's organization chart but on the depth and quality of the technical skills in the responsible agencies and their ability to tap the top talent in the country. This problem will remain unchanged, at least in the short term, by the proposed reorganization.

The committee agrees, however, that the need for a coordinated effort is urgent, so its comments and recommendations are based primarily on the current situation, in which OHS is responsible for organizing the federal government's homeland security strategy. However, the issues discussed and the suggestions made about strengthening the government's capabilities for setting priorities, coordinating programs, and deploying technology are not specific to the current situation. When or if a new department is formed, the actions proposed below would strengthen its ability to carry out its mission.

Cooperation Between OHS, OMB, and OSTP

After reviewing the past commission and congressional reports, consulting with government officials responsible for managing science and technology programs, and learning from the lessons manifest in the earlier chapters of this report, the committee concluded that the existing organization for coordinating counterterrorism research and utilizing the results is indeed inadequate. Responsibilities are unclear; authority is insufficiently specified; and the conception, execution, and evaluation of counterterrorism research and development are inadequately focused and coordinated.[11]

Nevertheless, essential institutions for ensuring that critical science and technology contributions are made to homeland security efforts are in place, though some improvements to existing capabilities and processes are required.

One such institution is the Office of Homeland Security, which was created by Executive Order of the President on October 8, 2001.[12] OHS is located in the

[11]The GAO in its September 2001 report noted that the management of counterterrorism research and development is "self governing and highly dependent on voluntary coordination mechanisms" (General Accounting Office, 2001, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-82, September, p. 82).

[12]Executive Order Establishing the Office of Homeland Security and the Homeland Security Council, October 8, 2001; available online at <http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html>.

White House and is currently responsible for creating the overall homeland-security plan.[13,14] A second key institution is the Office of Science and Technology Policy (OSTP), a statutory agency within the Executive Office of the President (EOP) which assists the President with the science and technology aspects of a broad range of policy issues, collaborates with the Office of Management and Budget (OMB) in evaluating and structuring the S&T components of the federal budget, and has close links with numerous sources of expert S&T advice from outside government.[15] A third important institution is the OMB, which has the authority to manage the budget process for the EOP and ensures that all of the President's priorities are reflected in the budgets of the cabinet departments and other agencies of the government.

Among these offices, the logical partitioning of responsibility is that OHS would develop the overall strategy for homeland security, including its S&T components. OSTP would assist OHS in generating these S&T components,

---

[13]Specifically, the Executive Order states, "The mission of the Office shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks." The status of this mission was described by Mitchell E. Daniels, Jr., director of the OMB, in testimony on April 11, 2002, to the Senate Governmental Affairs Committee:

> We have been building that strategy on many fronts, and it is our intention to prepare a document this summer that will summarize that strategy in one place. This strategy will meet four key tests:
>
> • The strategy for homeland security will be comprehensive and will integrate the full range of homeland security activities into a single, mutually supporting plan.
> • The strategy will be a national strategy, not just a federal government strategy, as the threat posed by terrorism does not fall solely within the jurisdiction of the federal government. To defeat terrorism, the federal government must work with states and localities and the private sector.
> • The strategy will outline a long-term plan to strengthen homeland security.
> • Finally, the strategy will include measures by which we can evaluate progress and allocate resources. These objectives will set the goals for federal departments and agencies. They will also give guidance to state and local governments and the private sector.
>
> While the Office of Homeland Security coordinates, consults with, and provides advice to OMB and agencies throughout the government, Governor Ridge does not have operational authority over any federal agency. The roll-out of the Homeland Security Advisory System is illustrative of how the Governor coordinated with various agencies, but ultimately handed over the operational aspects of the final product to a Department . . . .

[14]The OHS director, Governor Tom Ridge, is officially designated as the Assistant to the President for Homeland Security. Given Governor Ridge's authority, together with his already-close relationship with the President, the advice of OHS is influential with OMB and the departments and agencies. OHS is also the President's voice in communicating to the public about government activities in homeland security.

[15]OSTP is a statutory office in the EOP and is led by a director who also serves as the President's science advisor.

work with the federal agencies (through the National Science and Technology Council and the Homeland Security Council), and tap into the expert advice available from the President's Council of Advisors on Science and Technology, from the federal S&T agencies, and from the S&T communities at large. OMB would support execution of the strategy, subject to the President's direction and the many trade-offs that must be made with the rest of the federal government's activities. This system is already in place to some extent, but for it to function most efficiently, OHS needs access to new analytical capabilities, OSTP should be strengthened, and closer linkages could be developed between all three offices.

The Role of OHS in the S&T Strategy for Homeland Security

Development of a strategy for harnessing science and technology to counter terrorism was not listed as one of OHS's major responsibilities in the Executive Order[16] creating OHS, notwithstanding the highly technical nature of much of the work. This Executive Order also fails to document a formal role for OSTP in homeland security, and the director of OSTP was not explicitly named as a participant in OHS activities. However, despite the absence of S&T and OSTP in the Executive Order, the importance of science and technology and the need for close collaboration between OHS and OSTP is evident to all parties; it is already being addressed to a certain extent through voluntary collaboration between Governor Tom Ridge, the director of OHS, and John Marburger, the director of OSTP.

As Congress and the administration move forward on a potential new Department of Homeland Security, they have a chance to create a structure and a culture in the new department that will allow science and technology to be used efficiently in counterterrorism programs.

Recommendation 12.1: An Undersecretary for Technology will be needed in the proposed new Department of Homeland Security to provide a focal point for guiding key research and technology development programs across the department, and most importantly, engaging commitments from the major science, engineering, and medical science agencies that will remain outside the proposed new department.

In addition, this undersecretary could work closely with OSTP, perhaps through the National Science and Technology Council, on coordinating those multiagency projects and their linkages to related programs devoted primarily to other high-priority national objectives. This undersecretary would have responsibility not only for homeland security-related technology, but also for all technical elements of the agencies that are located in the department. (For example, if

[16]Executive Order 13228, October 8, 2001.

the Coast Guard is part of the new department, the undersecretary would have to pay serious attention to research and development programs for new search and rescue tools or oil spill cleanup methods as well as to counterterrorism-related programs.)

In the meantime, a primary task of the OHS is development of a national strategy for homeland security. The first draft of that strategy is scheduled to be produced in July 2002. The committee commends OHS's efforts in this area and specifically applauds its decision to include a section on science and technology for countering terrorism. The strategy, once complete, will go to the President for his approval, and thus the objectives and programs outlined in the OHS plan will become presidential priorities. This high-level focus on and endorsement of these objectives is vital to ensuring that the government is able to execute the appropriate programs through which science and engineering can contribute to homeland security efforts. As presidential priorities, these programs will be supported in the budgets of the relevant agencies, will be identified in OMB's crosscutting budget analyses describing counterterrorism activities, and will be appropriately justified and defended during the budget process.

Need for Analytical Capabilities to Support Decisions About Homeland Security Priorities and Programs

The national homeland security strategy currently under development in OHS is an important first step toward a national counterterrorism plan, but the threats, vulnerabilities, and available solutions will be constantly changing, and the federal government will continually be faced with the challenge of identifying new problems and new opportunities for strengthening the nation and the even more difficult task of prioritizing potential government actions. In this section, the committee discusses the information and capabilities the federal government will need access to in order to continually assess priorities and programs in this changing environment.

In light of the technical nature of the threats, as discussed throughout this report, it is clear that the government has insufficient capability to undertake scenario-based threat assessments, systems modeling of critical infrastructures, red teaming, economic and policy analysis of alternative counterterrorism policies, and development of testbeds, standards, and protocols to facilitate technology development and deployment. This inadequacy has been recognized by others, the Gilmore Commission in particular. Its report recommends the establishment of a national office that, among its other responsibilities, "should provide direction on priorities for research and development, and related test and evaluation for combating terrorism, as well as for developing nationally recognized standards for equipment and laboratory protocols and techniques, with the ultimate objective being official certification."[17]

[17]The Gilmore Commission (2000), at 5, 9.

Recommendation 12.2: A Homeland Security Institute to provide technical analysis and support should be established to serve the organization that sets priorities for homeland security; this Institute would perform the following functions:

- **Systems analysis, risk analysis, and simulation and modeling to determine the vulnerabilities of the nation's critical infrastructures and the effectiveness of the systems deployed to reduce them.[18]**
- **Sophisticated economic and policy analysis to assess the distributed costs and benefits of alternative approaches to enhancing security.**
- **Red teaming to evaluate the effectiveness of measures deployed to enhance the security of target institutions, facilities, and infrastructure.**
- **Identification of instances when common standards and protocols are necessary to ensure interoperability and effective utilization of tools developed for field operators and first responders. The institute would cooperate with relevant federal agencies, such as NIST, in the development of these standards.**
- **Assistance for agencies in establishing testbeds to evaluate the effectiveness of technologies under development and to assess the appropriateness of such technologies for deployment.**
- **Design of metrics and use of these metrics to evaluate the effectiveness of homeland security programs throughout the government agencies and at national laboratories.**
- **Design of and support for the conduct of exercises and simulations.**

This recommended Homeland Security Institute should be a dedicated, contracted, not-for-profit organization.

It is essential that the federal government have access to these capabilities so that it can make effective decisions about priorities and programs for counterterrorism, whether the capabilities support a strengthened OHS or a new Department of Homeland Security. However, the number of people needed to provide the breadth and depth of technical expertise for performing the above functions would be significant, and neither OHS nor OSTP is large enough to house such a group internally. Therefore the committee is recommending that the above functions be located in a dedicated, not-for-profit security technical analysis and support institute.

This is not the first time that the establishment of a research corporation has

[18]In particular, capability is needed for looking at scenarios in which the nation is exposed to multiple threats simultaneously (as discussed in Chapter 10) and in which the links between elements of the U.S. infrastructure are exploited. The modeling and analyses would not compete with the work of federal agencies but rather would be used to complement those efforts and to test whether the multiagency programs aimed at identifying critical vulnerabilities and mitigating these problems are proceeding correctly.

been proposed to support governmental counterterrorism activities. Shortly after 9/11, Joseph S. Nye recommended that the then-proposed Office of Homeland Security be supported by a new research corporation, specifically commissioned to deal with terrorism.[19]

Nonprofit, independent, or contractor-operated technical organizations have been providing dedicated, sole-source analytic support to national security agencies and the Department of Defense for a number of years. Examples include the MITRE Corporation, Project Air Force at the RAND Corporation, the Institute for Defense Analyses, and the Aerospace Corporation.[20] A primary advantage of these sorts of quasi-governmental organizations is that they are structured and managed to provide support for decision making by government officials by quickly providing important information based on a deep understanding of the technical issues relevant to those decisions. They also have the ability, as non-governmental bodies, to subcontract work without the constraints of the government's procurement regulations and to establish their own hiring and compensation criteria. In that way, they are able to attract the highly specialized talent required to perform the tasks described in Recommendation 12.2.

The technical support supplied by the proposed institute would provide essential input for decision making about programs and deployment activities for counterterrorism efforts. However, OHS does not currently have the procurement authority needed for creating and utilizing such an organization. The new Department of Homeland Security would have this authority, but this department does not exist yet. The legislation required to give OHS the needed authority, or the formation of the new department, would take some time, but waiting for either process to conclude before forming the institute would be inappropriate, given the urgency of the counterterrorism tasks facing OHS and the federal government. There are a number of mechanisms that would allow work to begin quickly on putting together the staff and facilities for the institute. One would be to utilize an existing contractor-operated technical organization that already provides support to government agencies. Another would be to assign the tasks to an existing unit within a relevant agency. Yet another would be to have an agency or office with the necessary procurement authority begin to create the institute from scratch. Which approach will work most efficiently should be determined by the administration and Congress, but it is important to recognize that the various tasks listed above for the institute are related, and a good deal of the value of the

---

[19]Nye, Joseph S. 2001. "How to Protect the Homeland," *New York Times,* Editorial, September 25. He cites as a precedent for this proposed research corporation the organizations established to deal with nuclear threats of the Cold War era.

[20]These institutions are organized as federally funded research and development centers (FFRDCs), but it is the capabilities and mode of work that the committee sees as necessary; no view is expressed here on whether an FFRDC is the right formal structure.

institute will be in the leveraging of expertise and results across the institute and in synergies from interactions between people working on different tasks or on the same tasks for different areas of vulnerability. Thus the responsibilities proposed for the institute should not be assigned to different organizations.

Recommendation 12.3: The administration and Congress should develop a transitional plan that allows the Homeland Security Institute described in Recommendation 12.2 to be created as quickly as possible.

The organization responsible for determining the administration's national counterterrorism strategy will be the primary customer of the Homeland Security Institute; currently this is OHS. The technical nature of the institute's responsibilities and outputs implies that OHS should rely heavily on OSTP for help in finding staff for the institute and assigning its tasks. However, to take full advantage of the institute, OHS will need some in-house technical and analytic expertise. In the longer term, if the new Department of Homeland Security is formed, the committee would expect that the institute would report to the department's Undersecretary for Technology.

The Role of OSTP in the S&T Strategy for Homeland Security

OSTP is the only unit in the EOP with the capability to digest the S&T needs for counterterrorism and to interact with the science and technology community within and outside the federal government. Thus, OSTP has a critical role to play in support of OHS. As discussed above, OSTP will provide OHS with access to existing science and engineering expertise within the EOP and will help OHS staff and utilize the Homeland Security Institute. Mechanisms for cooperation between the OHS and OSTP are being developed; for example, a senior OSTP staff member is serving on the OHS staff and a memorandum of understanding is in place defining a cooperative relationship between OHS and OSTP. OSTP is clearly willing to provide OHS with as much assistance as possible; the present director has given homeland security a top priority in the work of OSTP, and he has asked the President's Council of Advisors on Science and Technology (PCAST) to give these issues priority attention as well.

More remains to be done, however, to ensure that OSTP is able to play its critical role in supporting OHS's work. For example, OSTP needs to be able to tap the expertise of all relevant agencies—including those represented on the Homeland Security Council and other agencies responsible for science and technology research and development—to develop research priorities.

Recommendation 12.4: The Director of OSTP should lead an interagency process to develop the S&T research priorities for counterterrorism. These priorities should be responsive to and aligned with the overall counterterrorism agenda developed by OHS, and budget guidance should be pro-

mulgated to the agencies to support their participation in programs that support these priorities.

The National Science and Technology Council (NSTC) is a natural place for relevant agencies to come together to discuss S&T for counterterrorism. However, the committee is concerned that NSTC does not currently appear to be as active as would be necessary to effectively carry out key coordinating discussions. A revitalized NSTC Committee on National Security or a new NSTC subcommittee on counterterrorism research and development, with participation from the highest levels of relevant agencies, would help OSTP and the agencies provide coordinated input to OHS and OMB.

To effectively lead interagency discussions about counterterrorism priorities and coordination of programs, the director of OSTP must be recognized as being the representative of the President's decisions and views on science and technology in this area. By giving him the title of Assistant to the President for Science and Technology,[21,22] the President could make it clear that the director of OSTP acts with his authority. This designation would allow the director, when interacting with the agencies, to have the stature and influence needed to ensure that programs in support of the science and technology elements of EOP's priorities for homeland security are given the necessary attention.

Another factor that would help the OSTP director effectively support the communication of Presidential priorities is assuring that the OSTP has access to the people and resources needed to provide scientific, engineering, and technical expertise in the wide range of disciplines that are relevant to counterterrorism. The need for increased capabilities in the life sciences area is particularly apparent.

The Role of OMB in the S&T Strategy for Homeland Security

The budgeting process for counterterrorism investments is beginning to develop transparency and consistency through the process required by Congress and reported in OMB's *Annual Report to Congress on Combating Terrorism,* typically prepared each August.[23] However, the definition of "research" and

---

[21]"Assistant to the President" is a title that President George H.W. Bush gave to D. Allan Bromley, his science advisor, and that was continued for Bromley's successors in that administration and for President Clinton's science advisors as well.

[22]This recommendation was also made by the Hart-Rudman Commission (Hart-Rudman, at ix).

[23]OMB's *Annual Report to Congress on Combating Terrorism* fulfills legislative requirements that the Administration provide information on executive branch funding for combating terrorism, domestic preparedness (primarily defense against weapons of mass destruction), and national security. The most recent version of the report was released in August 2001 and is available online at <http://www.whitehouse.gov/omb/legislative/nsd_annual_report2001.pdf>.

assurance of its consistent interpretation across the agencies need more work. Categories like "critical infrastructure protection" are not distinct from "counterterrorism," so that the funding representation is not unique. Further refinement of the budgeting process at all stages, together with tighter coordination within the EOP, will help assure the coherence of agency programs and their conformity with Presidential priorities. OMB must also work with and support OSTP in coordinating agency activities and offering budget guidance.

Recommendation 12.5: OMB's *Annual Report to Congress on Combating Terrorism* should include a description of progress toward achieving the goals of the S&T agenda for countering terrorism as well as actual budget appropriations in suitable activity categories and by agency. In addition, OMB should prepare and issue jointly with OSTP an annual budget crosscut describing how the present and proposed budgets reflect the S&T priorities for countering terrorism. A joint letter would be transmitted to Congress, with the budget proposed the following January.

Enhancing the Importance of S&T in the Homeland Security Council

The same Executive Order that created OHS also formed the Homeland Security Council (HSC), which is responsible for advising the President on homeland security and coordinating and executing the nation's corresponding strategy. The members of the HSC are the President, the Vice President, 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 Federal Emergency Management Agency, the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, and the Director of the Office of Homeland Security.

This list does not include the Secretary of Energy and the Secretary of Commerce, who are only invited to "meetings pertaining to their responsibilities." But the Department of Energy has responsibility for a $6 billion physical science and technology program. It is the steward of the national laboratory system within which much of the critical research and testing capability of the country resides. DOE, through the National Nuclear Security Administration, also has stewardship responsibility for the nation's nuclear stockpile, which is critical to international control of nuclear weapons-grade material. The Department of Commerce, among its other responsibilities, is home for the National Institute of Science and Technology. NIST undertakes critical testing and standards-development activities that can enable the early deployment of technologies to counter terrorism for use by federal agencies, local first responders, and the private sector. Both the Department of Energy and the Department of Commerce clearly have critical roles to play in the defense of the homeland and in counterterrorism activities in general.

Recommendation 12.6: The Secretary of Energy and the Secretary of Commerce should be accorded full membership on the Homeland Security Council.

As argued above, this committee believes that science and technology efforts should be a major element in homeland defense. To assure that the effort is properly coordinated, the Director of OSTP must be at least on a par with other leaders of the nation's S&T enterprise and thus should be accorded full membership in the Homeland Security Council.

Congressional Capabilities for Supporting the S&T Strategy for Homeland Security

Congress is a key partner of the executive branch in the federal government's management of counterterrorism programs. Thus Congress needs access to many of the same resources that support EOP. In particular, it needs analytic capabilities to support appropriations and legislative decisions for counterterrorism programs, and it needs to be able to understand their funding situations.

As noted above, many agencies have responsibilities for performing research or deploying technologies for homeland security. Thus when presidential budget proposals are transmitted to Congress, they are atomized in the present committee structure and Congress, as a whole, loses an integrated picture of the entire budget as it relates to counterterrorism. While a new Department of Homeland Security, and a corresponding reorganization of congressional committees, may reduce the number of agencies and committees whose budgets are supporting programs relevant to homeland security, the activities will still be spread across a fairly wide range of departments. Thus it will always be important for Congress to be able to determine its own view of the proper balance of resources and missions among agencies both within and outside a Department of Homeland Security.

Other commission reports have made general comments on the fact that Congress's organization can impede its ability to deal with national-security priorities.[24] This committee addressed more specific concerns—that is, how Congress can receive an integrated, coherent, and comprehensive representation of the entire federal budget as it relates to science and technology for counter-

[24]For example, the Deutch Commission Report (1999, at 7) notes that "Congressional-executive interaction is complicated by the number of congressional committees that now have oversight and budgetary authority over proliferation-related programs. Oversight from at least twenty committees heightens the need for coherent, continuous consultation between the branches." Hart-Rudman (2001, at xvii) recommended that Congress perform a thorough review of its relationship to national security and its own committee structure, and the commission further recommended the merger of appropriations subcommittees with their respective authorizing committees.

terrorism. Recommendation 12.5, on strengthening and expanding OMB's *Annual Report to Congress on Combating Terrorism,* is motivated in part by the value to Congress of receiving this information. Another report that will help Congress better understand the range of counterterrorism activities under way is the recent report to Congress by the Congressional Research Service.[25]

Congress could also benefit from an internal source of objective, reliable, expert advice on S&T in order to competently perform its appropriations and oversight roles. Congress needs access to information that allows it to judge various S&T programs based on their goals and objectives, accomplishments and progress, and unsolved issues. (For example, the ability to monitor progress in sensor research and its application to counterterrorism would be useful.) Analytic capability could also be used to reestablish connectivity in the separated budget items supporting the overall homeland security objectives defined by the administration. One mechanism for building this desirable institutional capacity could be the establishment of an entity within the Congressional Budget Office.

THE ROLE OF THE FEDERAL AGENCIES IN DEVELOPING AND USING SCIENCE AND TECHNOLOGY FOR COUNTERING TERRORISM

Federal agencies are of course currently providing a critical source of expertise for OHS and OSTP as they formulate the national homeland-security strategy, but the most important responsibility of the federal agencies will be in executing this strategy. They will need to ensure that focus is maintained on critical counterterrorism-related research areas and that results lead quickly to new technology in support of well-understood goals. This will have to be a government-wide effort, as the agencies that can perform innovative research in counterterrorism-related areas are often not the same agencies that have operational missions in homeland security.

Institutions such as NIH, NSF, the Department of Energy and its national laboratory system, the Department of Commerce's NIST, and the Department of Defense together play a key role in performing and funding research in support of diverse national needs. However, with the exception of the Department of Defense, the nuclear programs of the Department of Energy, and the NIH work on its recently expanded mission in bioterrorism, these S&T agencies are not involved in the front line of research on homeland defense.

Instead, the task of implementing technologies to protect the nation is distributed among many agencies—FEMA, the Coast Guard, Customs, Immigration and Naturalization, the new Transportation Security Administration in DOT,

[25]Genevieve J. Knezo. 2001. *Federal Research and Development for Counter Terrorism: Organization, Funding, and Options*, November 26 (updated January 3, 2002) (Order Code RL31202).

the FBI, the U.S. Postal Service, parts of the Department of Agriculture that deal with food production and safety, and state government and municipal agencies—that often have limited experience with advanced and highly creative research and development and limited resources available for such programs.

Thus a key challenge for the federal government will be in ensuring productive interaction between these two groups of agencies. The institutions overseeing the research will need information about what sorts of technologies and operational performance levels are required for practical counterterrorism systems, and the organizations making decisions about deployment will need to understand the capabilities and limitations of new technologies and the possibilities for systems integration. Furthermore, to ensure that these interactions are constructive and that appropriate expertise is available to make key decisions about programs and technologies, some agencies may need new or enhanced capabilities and experiences.

For example, some agencies have a limited tradition of creating or managing complex research programs. Yet they are already being tasked with making decisions about which existing technologies provide the best immediate protection and determining which technologies will be needed next. The Department of Transportation and its new Transportation Security Administration are in this situation. The committee of course does not suggest that all research on transportation security go through TSA, but TSA as a user agency should have the ability to support research programs and technology development activities when necessary and the expertise and the experience to contribute to and learn from programs being performed elsewhere.

Recommendation 12.7: Agencies with homeland security missions and substantial responsibilities for procuring and fielding solutions dependent on technology should have systems analysis and systems engineering capabilities and the expertise to set up and manage programs for which they fund contract research.

Some or all of the agencies responsible for setting technology requirements and deploying technologies may move into a new Department of Homeland Security so that they can more effectively coordinate their work with one another, but they will still be organizationally separated from the government's largest and most advanced science, engineering, and medical science programs. The deploying agencies will still need the expertise and mechanisms to communicate their needs to the researchers and to utilize the results of such programs.

Facilitation of technology development will be a complicated task for many agencies. It is very difficult to define the goals for such programs, support the necessary scientific and engineering research, facilitate the maturation of technologies into robust products, and eventually ensure that these products are implemented by appropriate users. Also, technology development often requires some

high-risk/high-payoff programs, which many agencies are not comfortable with or experienced in selecting or managing.

A number of program characteristics should be key elements of agencies' efforts to develop technologies specifically in support of counterterrorism objectives. One is the promotion of interdisciplinary research, another is a focus on maturation and dissemination of innovations, and a third is the building of productive links to the academic, industrial, and government research communities. In some areas, such as work on technologies for preventing or responding to attacks using chemical, biological, and nuclear weapons, it will be important for agencies to be able to take goals with classified applications and translate them into general, unclassified problems that can be tackled by a broad research community in an open forum. In all cases a highly creative and flexible management approach is required.

One governmental institution that successfully developed programs with the above characteristics was the Advanced Research Projects Agency (ARPA, now DARPA). ARPA supported focused (and often high-risk) research that laid the groundwork for important new technologies. ARPA's achievements often were the result of the efforts of visionary, proactive, and empowered program managers who were able to fund projects in ways that extended beyond the government's conventional peer-review and competitive-award processes. Agencies such as NIH that will have to expand and adjust their systems to go beyond research in order to address technology development and its deployment for counterterrorism would do well to consider developing units or programs that have some of the above characteristics.

In addition to near-term, technology-focused programs, the government will need to invest in research with longer-term payoffs. Many federal agencies—including NIH, NSF, DOE, NASA, and the armed services research offices (ARO, ONR, AFOSR)—have the mission, experience, and infrastructure to support this sort of basic research and innovation. In addition a number of government laboratories, such as NIST, NRL, ARL and AFRL, as well as the DOE and NASA national laboratories, have the capability to perform basic research in relevant areas and can also contribute. All of these agencies should be given the resources to press ahead on a broad front in areas of science and technology that could enhance knowledge and the nation's capacity to meet counterterrorism needs in both the near term and the future. Specific research programs for these agencies are discussed in Chapters 2-10.

Since government agencies will not only be performing counterterrorism-related research but also funding such research at other institutions, it will be essential for the federal government to have the ability to sort through and evaluate a large number of proposals for research and for technologies and identify those with specific promise. (The administration and the supporting agencies are already finding the screening of such proposals a significant burden.) Decision making about both internal and external projects must be informed by systems

approaches. Many ideas that seem attractive in isolation will fail to meet critical needs when they are evaluated in terms of policy priorities and a systems context.

In many homeland security efforts, the national laboratories have a critical role to play, if their programs and unique capabilities can be focused on supporting OHS objectives. These programs should focus on the systems engineering elements of counterterrorism problems; for example, they are well positioned to examine issues relating to the development of effective sensor *systems* rather than just working on an individual sensor technology. The national laboratories also have the facilities to perform and facilitate both classified and unclassified research and to coordinate results from both types of programs.

The Department of Defense also has a great reservoir of relevant programs, experience, and expertise to be tapped in the application of science and technology for homeland security. How DOD's technology base can best contribute to the overall national technology effort that is the subject of this report has not been determined, but the Office of Homeland Security, the Department of Homeland Security (if formed), and other federal agencies should carefully coordinate their own technology efforts with relevant DOD programs. For example, the Defense Advanced Research Projects Agency, the Defense Threat Reduction Agency, the Joint Services Chemical and Biological Defense Program, and the U.S. Army Medical Research Institute of Infectious Diseases all are and will be carrying out large-scale science and engineering efforts closely related to domestic counterterrorism activities.

In addition to these research and development activities, some of the technical tools and experiences that arise in the normal course of DOD's principal mission of conducting joint military operations against foreign opponents may also be appropriate for aspects of homeland security. For example, DOD will be developing technology for detection of and protection from chemical and biological threats as a necessary part of its principal mission. Deployed forces are a prime target of terrorists, and DOD's protective efforts (called "force protection" by DOD) have much of the same technical content as homeland security. The DOD also will have a role to play in support of counterterrorist efforts within the United States and has taken some preliminary steps to adapt its structures to make this contribution. A Northern Command has been established with the explicit mission of "defending the U.S. and supporting the full range of military assistance to civil authorities."[26] Such support would range from shooting down commandeered airliners to providing airlifts to convey supplies for disaster relief. Given the likely scale of the DOD efforts and the overall size and quality of the

[26]From a description of Unified Command Plan revisions announced April 17, 2002, and scheduled to take place on October 1, 2002. Information about the Unified Command Plan is available online at <http://www.dod.gov/specials/unifiedcommand/>.

DOD technology and industrial base, it is important to find a role that makes the best use of the national defense asset for homeland security.

Difficulty Implementing Parts of the Research Agenda in This Report

In its descriptions of how science and technology can contribute to counterterrorism efforts, this report outlines a wide range of actions that the agencies should consider taking. However, in some of the critical areas, the committee was not able to identify an appropriate government agency with the capabilities or the mission to take the lead in formulating and funding research or to translate resulting technologies into effective, deployed systems. In these cases, examples of which follow, the committee concluded that enhancement or restructuring of institutional capacity at an operating agency will be required:

- Many groups have recognized that most of the transportation modes are not supported by an operational capability to define and manage a research program for protection against catastrophic terrorism. Thus Congress has established the Transportation Security Administration, and this new agency will have a multibillion-dollar budget and tens of thousands of employees. But at present, it has no advanced research capability, little experience in high-tech systems acquisition, and insufficient capability to do the required systems analysis, put needed technology programs in place, and manage them to success. (See Chapter 7.)
- Food production and supplies must of course be safeguarded from terrorist attack. But the current food production and inspection system is not designed to provide security against or to recognize intentional attacks. The Department of Agriculture needs the capacity to perform and fund research on plant and animal diseases and to develop and deploy surveillance systems. An agricultural equivalent of the Centers for Disease Control and Prevention might be an appropriate approach. (See Chapters 3 and 4.)
- First responders and emergency operations centers will need guidance from the federal government on relevant technologies (such as sensors and protective gear), on training exercises and simulations to prepare personnel and test systems, and on protocols for identifying and responding to different kinds of attacks. The Federal Emergency Management Agency (FEMA) has a preexisting relationship with local police, fire, and rescue squads owing to a history of working together on disaster-response efforts, so it would be the logical coordinator between the federal government, particularly OHS, and local groups. However, FEMA will need to drastically expand its experience and programs in homeland security and counterterrorism and to draw heavily on expertise in other agencies in order to provide first responders and emergency operations centers with the necessary information and tools, especially if it is to place greater emphasis on preparing for and anticipating terrorist events. (See Chapter 8.)

• Traditional market mechanisms for the development of new vaccines are failing to provide products for responding to bioterrorism. The Department of Health and Human Services should explore new mechanisms to facilitate the development and production of such vaccines. A national orphan vaccine center, perhaps created as a government-owned, contractor-operated facility, might be necessary to bring potential vaccines to the stage at which they can be licensed. Such a center could help coordinate extramural research and development activities among public and private institutions, perform its own research in critical areas, and coordinate and oversee the clinical trials and animal model work on which licensing would be based. A production facility for orphan vaccines would also be needed. (See Chapter 3.)

• Information security is identified in this study, as it was by the President's Commission on Critical Infrastructure, as a major element in the nation's vulnerabilities, but no agency or department has the primary mission to foster progress in this field. DARPA and NSF created much of the science base for the Internet and for computer science in general, and other agencies—DOE, DOD, FBI, and NASA in particular—have made important contributions to computer-network technology. But the security of commercial computers is left largely to the private sector, and the present weakness in this area is a consequence of minimal market demand for it in the past. Coordination of agency efforts in this area is important, as is building a federal infrastructure to tap the intellectual and fiscal resources of private industry. (See Chapter 5.)

REFERENCES

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission). 2000. *Second Annual Report to the President and the Congress,* December 15.

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission). 2001. *Third Annual Report to the President and the Congress,* December 15.

Carter, Ashton B. 2001-02. "The Architecture of Government in the Face of Terrorism," *International Security,* Vol. 26, No. 2, Winter, pp. 5-23.

Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (Deutch Commission). 1999. *Combating Proliferation of Weapons of Mass Destruction,* July 14.

Commission on the Roles and Capabilities of the United States Intelligence Community (Brown Commission). 1996. *Preparing for the 21st Century—An Appraisal of U.S. Intelligence,* March.

General Accounting Office. 2001. *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-82. September.

Homeland Security Council. 2001. *Homeland Security Presidential Directive–1, Subject: Organization and Operation of the Homeland Security Council,* October 29.

Joint Task Force on Intelligence and Law Enforcement (Richards/Rindskopf Report). 1995. *Report to the Attorney General and Director of Central Intelligence,* May.

Knezo, Genevieve J. 2001. *Federal Research and Development for Counter Terrorism: Organization, Funding, and Options,* Congressional Research Service, November 26 (updated January 3, 2002), Order Code RL31202.

Knezo, Genevieve J. 2002. *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education,* Congressional Research Service, April 8. Available online at <http://www.fas.org/irp/crs/RL31354.pdf>.

National Commission on Terrorism (Bremer Commission). 2000. *Countering the Changing Threat of International Terrorism,* September.

Nye, Joseph S. 2001. "How to Protect the Homeland," *New York Times,* September 25.

Office of Management and Budget. 2001. *Annual Report to Congress on Combating Terrorism,* August. Available online at <http://www.whitehouse.gov/omb/legislative/nsd_annual_report2001.pdf>.

The President's Commission on Critical Infrastructure Protection (Marsh Commission). 1997. *Critical Foundations,* October.

U.S. Commission on National Security/21st Century (Hart-Rudman Commission, Phase III). 2001. *Road Map for National Security: Imperative for Change,* February 15.

13

Essential Partners in a National Strategy: States and Cities, Industry, and Universities

The federal government must take the lead in the national counterterrorism effort, but effective use of existing technologies, research and development activities, and deployment of new approaches to mitigating the nation's vulnerabilities will depend critically on close cooperation with other entities. This chapter briefly addresses some of the key issues in the federal government's relationships with the cities and states, private industry, and the universities.

STATES AND CITIES

The immediate effects of terrorist attacks are felt at the local level, so state, county, and municipal governments will be the first responders and must manage the immediate crisis and longer-term recovery. Thus much of the financial burden for preparing for attacks falls to these regional institutions. If the federal government is to provide much of the information and technologies they require, a more collaborative relationship between federal agencies and local and state governments will be needed. For example, first responders organized at the local level will be the customers for some of the technologies developed and deployed through the nation's counterterrorist efforts.

Only a few federal agencies are experienced at working with state and local governments, but their knowledge and experience can be leveraged as part of the solution. FEMA, which has been assigned a lead role in coordinating the federal government's interactions with first responders all over the country,[1] has a preex-

[1]Federal Emergency Management Agency. 2002. Statement of Bruce Baughman, Office of National Preparedness, FEMA, Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, U.S. House of Representatives, April 11. Available online at <http://www.fema.gov/library/baughman041102.htm>.

isting relationship with many of these groups in the context of disaster response efforts. The Department of Transportation undertakes many programs in conjunction with state and local transportation agencies, and it would be sensible to broaden these relationships to encompass homeland security work in the transportation field. However most agencies are not prepared to accommodate the wide variety of fairly distinct requirements the states and cities will have in technology-based preparations for terrorist incidents.[2] This problem is often exacerbated by perceived conflicts between the interests of the cities and those of the states, and the difficulties inherent in overlapping jurisdictions.[3]

A great deal more work must be undertaken to bring cities, counties, and states into effective partnership in the federal government's counterterrorism efforts. It is a federal responsibility to contribute to the research and development work necessary to enable new counterterrorism technologies to be tested and relevant standards to be set. However, local governments must be involved from the very beginning, so that the design of standards and the development of procedures are informed by the experience and insight of the first responders. Cooperation and coordination will be needed at the state and local levels to facilitate participation in the federal programs and to allow the results of these programs to be effectively disseminated and utilized. Many relevant counterterrorism standards and protocols (such as decontamination guidelines for anthrax) are yet to be determined, and professional associations (e.g., the National Fire Protection Association) and associations for state or local governments (e.g., the U.S. Conference of Mayors) must be identified and engaged so that productive interaction between federal agencies and front-line users can proceed.[4] As potential standards and protocols are developed, they will have to be tested in pilot programs in various municipalities and the results shared nationwide.

In addition to effectively utilizing the results of federal programs, it will be important for states to support their own programs, guided by information from the federal level. Some states have offices that allocate state resources to re-

---

[2]OMB's *Annual Report to Congress on Combating Terrorism*, FY2001, includes agency-by-agency discussions (in Part 5) on coordination. Most of them center on how an individual agency coordinates with other federal agencies. However, some agency discussions—such as those for FEMA, HHS, DOE, and EPA—do mention state coordination efforts as well. There is no systematic treatment, however, on how federal R&D for counterterrorism—as managed overall—is coordinated with any state-level R&D. Governor Tom Ridge, the current Director of the Office of Homeland Security, has stated that he is responsible for a *national* strategy to combat terrorism, meaning it is one that embraces all levels of government as well as the private sector.

[3]In addition to city and state governments, county-level institutions (such as sheriff's departments) and special-purpose authorities (such as port authorities handling air and sea facilities) also may have responsibilities for emergency preparation and response.

[4]For example, the federal government has worked effectively with national police associations on standards for bulletproof vests.

search and other science and technology activities, while in other states it is not clear who within the state has responsibility and authority for initiating research and development activities to meet specific needs. Representatives of state research and development programs have to be identified and brought into relationships with the federal government through institutional arrangements such as those of the Technical Support Working Group.

Recommendation 13.1: The OSTP intergovernmental panel for coordination of S&T by the federal and state governments should be charged with developing effective federal-state linkages for the exchange of information to support the funding, performance, and evaluation of S&T related to counterterrorism.

INDUSTRY

The nation has reassessed its overall vulnerability to terrorism since the events of 9/11, but the nature of the risk to any single company or even industry is very difficult to predict, much less quantify. Yet the private sector is where much of the activity to increase national preparedness against terrorism must occur. Companies will be the developers of new security technologies and, because they own and operate many of the potential targets within the critical infrastructures, will also be among the users and beneficiaries of new approaches and products. Companies make a considerable investment in research and development activities (industry financed two-thirds of such activities in the United States in 2000). For the United States to take advantage of the significant scientific and technical expertise residing in the private sector, and to overcome the market disincentive for single firms to invest in improving their security, the federal government must explore creative and flexible ways to motivate industry to develop and adopt counterterrorism technologies.

For the government and private sector to work together on increasing homeland security, effective public–private partnerships and cooperative projects must occur. There are many models for government–industry collaboration—cooperative research and development agreements, the NIST Advanced Technology Program, and the Small Business Innovative Research program, to cite a few. And a more expansive patent policy, as in the Bayh-Dole Act of 1980, is critical in providing private sector incentives.

Other ways to encourage industry's participation in the drive to protect the nation from terrorism include mandating involvement through federal regulation, providing government subsidies or tax relief, and exploiting insurance markets. Codes and standards promulgated through various professional organizations or through local regulations, perhaps in close cooperation with federal agencies such as NIST, may also encourage the implementation of technologies that can enhance public protection. Overall, a new pattern of public-private partnership—

with a more sophisticated and balanced use of incentives, regulatory coercion, and voluntary agreement—is needed.

Recommendation 13.2: To maximize industry involvement in research on counterterrorism technologies and in their deployment, broad government–industry dialogue on a variety of topics is needed. These include counterterrorism research agendas, implementation of technologies, antitrust exemptions, indemnification, the role of regulation and subsidies, government procurement and acquisition rules, dual-use technologies, codes and standards, and policies related to insurance. The purpose of the dialogue is to inform law, regulation, and the federal research strategy, and OHS should identify for each industrial sector a suitable forum for this dialogue.

Effective government–industry communication in a number of sectors will be vital for responding to the vulnerabilities and developing the solutions identified earlier in this report. For example, the pharmaceutical industry will be a critical component of the national strategy to protect against bioterrorism, the IT industry will be a key player in any plan to improve cybersecurity, and the energy industry could be a significant beneficiary of new technologies. An example of how government–industry dialogue and cooperation can bring significant benefits to both groups and to the public can be seen in the Health Effects Institute, a successful co-funded partnership between the EPA and industry.

Before implementing new approaches, the federal government must understand how incentives and regulations might drive behavior and consider how changes in laws might affect international competitiveness. In some sectors, private investment in counterterrorism technologies may actually provide a competitive advantage. The committee did not have the opportunity or the expertise to fully explore the myriad options for government policy in these areas, but it briefly discusses below some relevant issues in four areas: commercial value for counterterrorism technologies, indemnification from legal risks, select antitrust exemptions, and government procurement and acquisition rules.

Commercial Value for Counterterrorism Technologies

Most firms are highly competitive and operate with narrow profit margins; they are understandably reluctant to make major investments against unknown risks if their competitors are not doing the same. Trying to compel industry to reduce its vulnerabilities to catastrophic terrorism through massive subsidies or draconian regulations is neither an efficient nor a politically viable approach.

A more effective approach is to give the private sector the widest possible latitude for innovation and, where appropriate, to design R&D strategies in which commercial uses and security uses of technologies rest on a common base of investment. Companies then have the potential to address vulnerabilities while increasing the robustness of public and private infrastructures against unintended

and natural failures, improving the reliability of systems and quality of services, and, in some cases, increasing productivity. In the military, this approach is called a dual-use strategy, and it will be essential to increasing capability rapidly and moving toward technologies that will ultimately be affordable to implement.

Opportunities for dual-use solutions may not be as rare as one might suppose. For example:

- Technology developed to protect and monitor the food supply against intentional contamination by terrorists may also be useful for improving our ability to catch and respond to unintentional contamination caused by bacteria, spoilage, or processing errors.
- Sensor and filtering technologies designed to protect buildings against chemical attack will be useful in monitoring building ventilation systems for other types of pollution and for improving indoor air quality, and may also allow more efficient control of these systems.
- Techniques to detect biological infections prior to clinical symptoms would help slow outbreaks of all infectious diseases, not just those introduced into the population maliciously.
- A security system concept for shipping containers whereby shippers certified as having secure loading facilities are granted faster passage through key megaports has a variety of possible collateral benefits, including a decline in the use of containers for the movement of contraband and an increase in the overall efficiency of the shipping system.
- Improved security architecture and cryptography that can protect SCADA systems and other critical infrastructures, such as telecommunication systems, would enhance commercial security (i.e., reduce cybercrime) and help protect privacy. More robust network architectures could increase the reliability of important systems.
- Technologies already developed for responding to natural hazards (e.g., earthquake, flood, hurricane, wind, and fire) could be adopted for homeland security and counterterrorism efforts.
- Low-cost electronic accelerators developed as sources of radiation for detection of nuclear or explosive materials could also be used to replace intense radioactivity sources currently used in commerce and medicine.
- Biometric identification technologies could be useful for commercial security, and authentication methods could facilitate e-commerce.

Homeland security is a national concern, but it does not necessarily represent a large business opportunity. The size of the market for counterterrorism technologies is ill defined, and the identity of customers is unclear. Unlike in the defense industry, the federal government is not the sole, or even primary, customer; potential users include private companies, first responders at the state and local levels, and a large variety of federal government agencies. The broader the

potential applications and benefits of new technologies, the greater the likelihood that the market will support their production and reward their developers.

Indemnification

In many cases, up-front cost may not be the only factor holding industry back from investing in counterterrorism-related areas. Firms may also be unwilling to undertake certain efforts unless they are indemnified against the considerable risks involved.

A prime example is the research, development, manufacture, and distribution of new pharmaceuticals to be used against biological agents. These activities contain many risks, and indemnification provisions may be necessary to overcome what are otherwise seen as formidable obstacles. The development and distribution of vaccines needed to protect against diseases that no longer exist (or are unlikely to occur naturally), such as smallpox, is a particularly well-documented example. (This problem of orphan vaccine development is discussed in Chapter 3.)

Similar concerns have been raised in the context of secure transportation systems for cargo. Intermodal cooperation all along the logistics chain is needed, but many participants would probably opt out if their participation would expose them to substantial liability in the event of system failure.

Another area where liability is a potential issue is in vulnerability analysis. To make decisions based on the relative likelihood of various terrorist events, the government must understand where weaknesses lie in private-sector systems and products. But, absent some form of indemnification, many firms will be reluctant, for legal reasons, to share with government their proprietary knowledge of their own vulnerabilities.

Antitrust Exemptions

It is possible that current antitrust regulations could inhibit the necessary development of counterterrorism technologies. For example, it might be in the nation's interest to allow all the firms in an industry (such as electricity generation or chemical manufacturing) to confer on how they might most economically make modifications so that the critical and often interoperable infrastructure they operate can be protected. Unless the companies are able to share this information, it could be difficult for the industry to reach agreement with government on public and private investment in appropriate research and development and work on needed standards. Thus, supervised antitrust exceptions may be needed in a variety of industries.

Government has passed limited antitrust exemptions before—e.g., in the energy crises of the 1970s. And bills are currently being considered to provide similar exemptions to support work on critical infrastructure protection and to

support the development of new vaccines. In the former area, the exemption is for "gathering and analyzing critical infrastructure information in order to better understand security problems related to critical infrastructure and protected systems, and interdependencies of critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability of critical infrastructure and protected systems."[5] In the biotechnology area, the objective is to facilitate cooperation on precompetitive research to support the development of new vaccines for combating various bioterrorist threats.[6]

Government Procurement and Acquisition Rules

Some of the disincentives for private investment have their origin in the government's own acquisition rules and regulations, which are not designed to provide the speed of procurement or the flexibility that will be needed for development and continuous improvement of counterterrorism technologies. The required procedures are time-consuming, and the bureaucracy is daunting, especially for small companies (where much of the nation's innovation occurs). The grants selection process in use at many agencies presents similar issues: The applications take months to solicit, write, and process, and the overall portfolio tends to emphasize low-risk proposals. This situation particularly discourages researchers in dynamic fields like biotechnology.

A study should be conducted, in collaboration with Congress, on whether and how these regulations might be streamlined when the high-priority needs of counterterrorism conflict with them. OSTP, through PCAST, might explore this issue and determine how such a study might be conducted. Prior reports have also recognized how daunting the government's acquisition process can be, and they have suggested that it might be appropriate for procurement to be simplified when in pursuit of urgent national goals.[7]

The committee notes that while improving the ability of the government to access the best research and technology available in the private sector (and at universities) is very important, so too is enabling agencies to make good deci-

---

[5]The Critical Infrastructure Information Security Act of 2001 (S. 1456). This act defines "critical infrastructure" broadly to include essential physical and cyberbased systems and services, including telecommunications (voice and data transmission and Internet), electrical power, gas and oil storage and transportation, banking and finance, transportation, water supply, and emergency services (including medical, fire, and police services).

[6]The Tauzin bill, Public Health Security and Bioterrorism Response Act of 2001, H.R. 3448, at Section 401.

[7]The Hart-Rudman Commission (2001) (at xiii) recommended reforms to security-related procurements, including: "Establish and employ a two-track acquisition system, one for major acquisitions and a 'fast track' for a modest number of potential breakthrough systems, especially those in the area of command and control."

sions about what to acquire. It is vital that they be well positioned to utilize tools, like testbeds and standards, that allow the evaluation of research results and new products. The ultimate goal, after all, is acquiring and deploying *effective* technologies for countering terrorism.[8]

UNIVERSITIES

Terrorism will be a threat to U.S. security for the foreseeable future, and as defenses improve, terrorists' abilities to circumvent them will also improve. It is essential that we balance the short-term investments in technology intended to solve problems that are defined today with a longer-term program in fundamental science designed to lay foundations for future threats that we cannot presently define. These long-term programs require the engagement of the nation's research universities.

In addition to providing a locus for creative research, universities also play a unique role in support of counterterrorism by educating and training students who will become the next generation of informed and engaged citizens, scholars in all disciplines, and professionals and leaders in all fields (including, of course, science and engineering) who will help us face the tremendous challenge of making the nation safer. Universities can also be a source of local expertise and are often well placed to bridge the gap between federal programs and the needs of state and city governments. State university systems in particular are an important asset for the nation, and with only a modest amount of additional faculty training, these universities could serve as a source of advice and assistance in emergency-response situations (e.g., labs to provide analytical capabilities in a biological or chemical attack, or technical support and forensics in a cyberattack).

Thus, both in the application of existing ideas and the discovery of new ones, the government will need to strengthen its partnership with the nation's research universities. Yet there are a cluster of challenges confronting universities, from a declining number of students in the sciences and engineering to the tension between openness and national security on sensitive research topics, that could prove obstructive. Below, the committee discusses some areas in which the universities have essential contributions to make to counterterrorism efforts and outlines some of the more critical challenges to their ability to make those contributions.

---

[8]For example, when introducing a bill that included FAA exemption from certain procurement regulations, Senator McCain said, "Although we acknowledge that procurement reform is important, even essential, that alone does not do enough. Without changing the basic mission and structure of the organization, procurement reform would merely be a way of allowing an agency to make bad purchasing decisions even faster." (Statements of Introduced Bills and Joint Resolutions (Senate, September 13, 1995), at 2.)

Examples of Critical Long-Term Research Needs

The delay between basic discoveries in science and their transformation into working technologies relevant to national security can be many years.[9] However, the current technological strength of the United States is based on past investment and successes in research, and continued flexible and creative programs in fundamental science and engineering disciplines can not only create new technical solutions, but also provide new ways to use existing technologies. Below is a list of examples of areas in which basic research can be expected to produce results with far-reaching implications for counterterrorism efforts. While these examples include problems that may not be soluble within 5 or 10 years, the set is representative of the type of fundamental challenges that are facing researchers today.

• *Understanding the mechanisms of human pathogenesis, response, and healing.* The four classes of weapons of greatest concern in counterterrorism are nuclear, chemical, biological, and radiological. To the extent that we can blunt the injuries caused by these weapons, we help to limit the impact of terrorism. All four produce pathologies that we understand incompletely or not at all. In addition, new weapons (e.g., new types of pathogens, new ways of using chemical to cause harm, electromagnetic weapons) may be designed by terrorists in the future and could pose yet more complicated problems. If we can understand the fundamental mechanisms of human pathology, self-defense, and self-repair, we will be in a much stronger position to respond quickly and effectively to new threats. (See Chapter 3.)

• *Sensors networks.* A great deal of research on sensor technologies is already under way. However, for research in this area to be useful—that is, for it to provide results that eventually lead to products that can be deployed for counterterrorism and other applications—the selection of sensor capabilities must be informed by systems research on the building of effective sensor networks. Work in this area will require a better understanding of the performance characteristics of individual sensors in real-world environments, of how groups of sensors or different types of sensors can complement each other, and of how outputs from sensors can be productively analyzed to provide information to users. Once the criteria for sensor performance are in hand, many fields, including chemistry, biology, physics, computer science, and electrical engineering, can contribute to the development of more effective sensor networks. Researchers in basic science have some unique opportunities here; for example, increased understanding of the superior olfactory capability of some animals could be used to improve the capabilities of manufactured sensors. (See Chapters 2, 3, 4, and 11.)

[9]Quantum mechanics was formulated in 1925; radar and the atom bomb were developed 15 and 20 years later.

- *Extraction of understanding from large quantities of data.* Intelligence gathering often depends on tracking very large numbers of people and very large flows of information (financial transfers, movements of people and goods) and searching for small cues suggesting hostile activities. A range of methods exists for collecting different types of information, but the ability to cross-reference or compare the different types and the ability to find the tiny amount of relevant information in this flood of data is still quite limited. The ability to use very large databases that will collect information over time and look for unexpected patterns (changes in behavior of individuals, formation of groups, patterns of training or purchasing) is an application of the broad subject of understanding and manipulating heterogeneous datasets. The fusion of applied mathematics and information technology required to build competence in this area will be immensely useful in intelligence and in a broad range of other areas. (See Chapters 5 and 11.)
- *Human behavior and system design.* The response of people to terrorist attacks is not well understood. Particularly useful would be a better understanding of how people react during and soon after an attack so that planning can be done on how to communicate warnings and other instructions during crises. Behavioral research is also needed so that appropriate, informed decisions about deployment of new counterterrorism technologies can be made. Whether a security system will be effective depends on how the system is used, by whom, and for what ends. If the primary purpose is deterrence, the needed technical capabilities of the system are different than if it is for warning of potential attacks or for controlling access to an area. The background of users could also vary widely (e.g., border security guards, first responders, or decontamination specialists), so user interfaces must also be based on the best human factors research. (See Chapters 9 and 11.)
- *Understanding complex, adaptive systems.* Our ability to predict and evaluate threats and vulnerabilities is often based largely on human intuition, and humans are limited in the amount of information that they can absorb and in their ability to deal with complex, highly nonlinear systems. New ways of understanding and modeling complex systems would have broad application in counterterrorism (including for intelligence gathering, cybersecurity, modeling the spread of diseases or contaminants, strengthening the energy system, and for defense applications) and in many other areas. Research in systems analysis and systems engineering, and new educational programs in these areas, are needed. (See Chapters 10 and 11.)
- *Intelligent, adaptive power grid.* The electrical supply system is a vital infrastructure vulnerable to cascading failures if important components of the power grid are damaged or destroyed. An intelligent, adaptive power grid would reduce vulnerability by providing the system with the ability to fail gracefully, which would help minimize damage to components and enable more rapid recovery of power. However, a deeper understanding of the failure mechanisms of the

grid are needed, and a wide array of new technologies would have to be developed before the power grid can be made more resilient. Many fields of science and engineering would have a role to play in building operations models and intelligence that could differentiate between a single component failure and concurrent or closely coupled serial failures and in developing systems for adaptive islanding, in which fast-acting sensors and controls are used to isolate parts of the grid. (See Chapter 6.)

• *Replacing humans in hazardous situations.* Robotics is a field where progress has been steady, but the ambitious goal of developing replacements for humans seems as far away now as it did 20 years ago. The understanding of biological systems is now affording some exceptionally interesting opportunities to mimic biological systems; imaginative concepts (linked "swarms" or "families" of robots or unmanned systems) suggest new ways to think about the potential and performance of highly versatile, nonliving systems. Success in this area would lead to assistants or replacements for humans in the hazardous circumstances that will be encountered in dealing with terrorism. (See Chapter 11.)

• *Reliable computer code and secure computer systems.* Buggy code underlies many reliability problems and computer security problems. No attempt to secure systems and networks can succeed if it does not take into account this basic fact. Dealing with buggy code is arguably the oldest unsolved problem in computer science, and there is no particular reason to think that it can be solved now by any sort of crash project. Two areas of research seem to be particularly important in a security context: security-oriented tools for system development and trustworthy system upgrades and bug patches. But a fundamental approach to computer security requires that new architectures and tools for their implementation that are provably secure must be the long-term basic research goal. (See Chapter 5.)

In all of these areas, the immense basic research capability that resides in the nation's universities will play a key role in advancing our understanding in critical disciplines.

The committee does not suggest that these examples are the only or the most valuable contributions that a vital, decentralized, innovative research enterprise can make. This list is offered simply as a demonstration that the research communities involved in these and similar efforts have critical contributions to make in laying the groundwork for improvements in homeland security. In order that research programs may increase the pace of discovery and the effectiveness of new counterterrorism technologies, relevant communities will require information about what kinds of new capabilities would be of most value to the nation and support for performing the necessary fundamental research.

The Need to Sustain the Nation's Scientific and Engineering Talent Base

Realizing S&T's potential for combating terrorism will require, among other things, sufficient numbers of talented men and women to pursue the necessary education and research. The *Science and Engineering Indicators 2002* report[10] documents a variety of factors that contribute to the declining U.S. ability to maintain a strong workforce in science and engineering. For example, the United States ranks 14th in the number of bachelor's degrees awarded in the natural sciences and engineering (normalized by the number of 24-year-olds in each country). In 1975, the United States was in the top three. This decline in the supply of scientists and engineers is reflected in a growing dependence on noncitizens to fill many spaces in American graduate schools; since 1980 the percentage of doctoral degrees in the natural sciences and engineering awarded to noncitizens has increased dramatically. Meanwhile, the number of such doctorates being granted in Europe and Asia is growing rapidly. While some noncitizens remain in the United States, some return to their countries of origin, and U.S. industry is experiencing a shortage of qualified technical workers in certain key areas. Companies have been moving their production facilities offshore for a number of years, and industry research and development centers have begun to follow. Such a shift not only may affect the nation's economic security but also may interfere with its ability to develop and produce critical technologies necessary for a long-term counterterrorism agenda.

Expanding the number of American scientists and engineers is particularly important in light of the current uncertainty about the status of foreign students. If efforts to limit the number of potential terrorists in the United States result in severe immigration restrictions, the recruiting of foreign-trained scientists and engineers for graduate-student and other research positions might slow to a trickle, and an even more severe shortage of scientists and engineers in this country can be expected.

In the 1950s, when militarily challenged by the Soviet Union, the United States enacted the National Defense Education Act (NDEA) to increase the availability of people trained in science, technology, foreign languages, and other key areas.[11] Today, our nation is again facing a complex threat and will again need to draw upon a cadre of scientists and engineers to defend itself. Thus it is time to provide additional incentives and new science and engineering educational programs.

---

[10]Available online at <http://www.nsf.gov/sbe/srs/seind02/start.htm>.

[11]The National Defense Education Act of 1958 was a direct result of the launch of Sputnik and the perceived increase in risk it implied for national security. NDEA provided support, from the late 1950s throughout the 1970s, for large numbers of students who became scientists and engineers. One result was that the number of Ph.D.'s awarded annually by U.S. colleges and universities rose from 8,600 in 1957 to 34,000 in 1973.

Recommendation 13.3: The committee is convinced that a human resource development program aimed at producing a sustained increase in baccalaureate and doctoral degrees granted in fields consistent with the government's long-term priorities for homeland security research is needed.

One factor that is affecting the supply of new scientists and engineers is the cost of education in this country—in some other countries, education is fully subsidized, while in the United States most students leave school with a considerable burden of debt. An effective human resource development program might use fellowships, forgivable loans, and opportunities for postdegree employment to allow talented students to embark on science and engineering careers unencumbered by heavy debt loads. This program should have clearly defined goals, expected outcomes, and accountability. One agency that might design and lead the program is NSF, and relevant fields would include all science and engineering disciplines and some areas of social sciences and humanities.[12]

This program, a call to young people by the government, would be consistent with the President's national initiative emphasizing public service. It has the potential to draw on talented young people from all sectors of society, including elements of the population that have not participated in these fields in the past.

Investing in Research in a Variety of Disciplines

Since the mid-1990s, physical sciences and engineering have mostly been funded at levels equal to the rate of inflation or only slightly above it.[13] The cumulative effect of years of relatively low investment is that the research base on which to build new science and technology initiatives of the kind discussed in this report is less than optimal. The current congressional embrace of the idea of providing significant increases to the NSF budget over the next few years is encouraging.[14] However, to do justice to the various counterterrorism programs

---

[12]In addition to providing human resources needed for S&T counterterrorism research and development, such a program could also increase the expertise available for other government counterterrorism activities (for example, the program could support students specializing in languages needed by intelligence communities).

[13]Board on Science, Technology, and Economic Policy, National Research Council, 2001, *Trends in Federal Support of Research and Graduate Education,* National Academy Press, Washington, D.C.; Committee on Science, Engineering, and Public Policy, 2001, *Observations on the President's Fiscal Year 2002 Federal Science and Technology Budget,* National Academy Press, Washington, D.C.; American Association for the Advancement of Science, 2001, *AAAS Report XXVI: Research and Development FY 2002,* Washington, D.C.; and American Association for the Advancement of Science, 2002, *Congressional Action on Research and Development in the FY 2002 Budget*, Washington, D.C.

[14]See "House Science Subcommittee Hearing on NSF Doubling Bill," FYI: The AIP Bulletin of Science Policy News, No. 60 (May 15, 2002). Available online at <http://www.aip.org/enews/fyi/2002/060.html>.

that are required, adequate and sustained support is urgently needed for the multiple agencies that provide fundamental knowledge on which emerging technologies will be based.

Balancing the Needs of National Security with the Requirements for Productive and Creative Research

An expanded concept of national security (i.e., the shift from confronting military forces overseas to protecting the homeland from terrorists), together with an expanded role for S&T in addressing ways to counter terrorism, raises some very difficult issues for the nation's research enterprise. They need to be resolved before the nation can realize the contributions of S&T described in this report.

In particular, because much of the research performed at universities will be essential for protecting the nation, there will be increasing pressure to keep critical knowledge out of the hands of people who might aid (or actually become) terrorists. In this environment, the federal government has already begun to express deep concerns about whether terrorists can take advantage of the open and international discussion of projects and results that characterizes university research. Scientists, on the other hand, worry that constraints on the free exchange of ideas may slow progress or even close down some fruitful areas of investigation altogether. This conflict between science and security is a difficult issue. More can be found on the topic in a recent Congressional Research Service report.[15]

This conflict always arises in wartime (including the Cold War), and universities and government have continually struggled to walk a fine line between protecting the nation's security while also retaining the ability to conduct the free and open exchanges necessary to make rapid and creative scientific progress. Successful resolution of this conflict depends on careful analysis of exactly what information must be protected and what constraints least impair the universities' effectiveness. Increased interaction between the government agencies responsible for security and the scientific community in universities and industry will enable the United States to come up with new and creative ways to defend itself and to outthink and outpace its enemies. The government should not place restrictions on research—such as limits on who performs research or who gets to share in the created knowledge—without first engaging in a thoughtful process that includes consultation with the universities and solid, case-by-case study of the risks vs. the benefits of open scientific investigation.[16]

---

[15]Knezo, Genevieve J. 2002. *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education,* Congressional Research Service, Washington, D.C., April 8. Available online at <http://www.fas.org/irp/crs/RL31354.pdf>.

[16]The government should also consider alternative research models to allow university researchers to perform research with national security implications. Faculty (and possibly students) could per-

Recommendation 13.4: OSTP, in collaboration with the OHS and other federal security authorities, should initiate immediately a dialogue between federal and state government and the research universities on the balance between protecting information vital to national security and the free and open way in which research is most efficiently and creatively accomplished. This dialogue should take place *before* enactment of major policy changes affecting universities as research and educational institutions.

Based on this interaction and on an understanding of the risks and rewards of conducting key scientific and technological research in an open environment, OSTP—in cooperation with OHS and other security agencies—should work out principles on which specific policies, both for government and the universities, can be based.

REFERENCES

Ad Hoc Faculty Committee on Access to and Disclosure of Scientific Information. 2002. *In the Public Interest*, Massachusetts Institute of Technology, Cambridge, Mass., June 12.

Knezo, Genevieve J. 2002. *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education,* Congressional Research Service, April 8. Available online at <http://www.fas.org/irp/crs/RL31354.pdf>.

Office of Management and Budget. 2001. *Annual Report to Congress on Combating Terrorism,* August. Available online at <http://www.whitehouse.gov/omb/legislative/nsd_annual_report 2001.pdf>.

National Science Board, National Science Foundation. 2002. *Science and Engineering Indicators—2002, Volume 1*, NSB-02-1, Arlington, Va., U.S. Government Printing Office, Washington, D.C. Available online at <http://www.nsf.gov/sbe/srs/seind02/start.htm>.

National Science Board, National Science Foundation. 2002. *Science and Engineering Indicators—2002, Volume 2*, NSB-02-2, Arlington, Va., U.S. Government Printing Office, Washington, D.C. Available online at <http://www.nsf.gov/sbe/srs/seind02/start.htm>.

U.S. Commission on National Security/21st Century (Hart-Rudman Commission, Phase III). 2001. *Road Map for National Security: Imperative for Change,* February 15.

---

form such work at affiliated institutions, such as private laboratories or hospitals (e.g., MIT faculty could work at Lincoln Laboratory or Draper Laboratory; see MIT report *In the Public Interest* [Ad Hoc Faculty Committee on Access to and Disclosure of Scientific Information, 2002], p. iv). Academic scientists could also form collaborations with researchers in national laboratories, not-for-profit institutions, or industrial laboratories in order to contribute to classified projects without involving students.

Bibliography

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission). 2000. *Second Annual Report to the President and the Congress,* December 15.

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission). 2001. *Third Annual Report to the President and the Congress,* December 15.

Boettcher, Mike, and Ingrid Arnesen. 2002. "Al Qaeda Documents Outline Serious Weapons Program," CNN, January 25. Available online at <http://www.cnn.com/2002/US/01/24/inv.al.qaeda.documents/index.html>.

Broad, William J. 2002. "U.S. Tightening Rules on Keeping Scientific Secrets," *N.Y. Times,* February 17.

Carter, Ashton B. 2001-02. "The Architecture of Government in the Face of Terrorism," *International Security,* Vol. 26, No. 2, Winter, pp. 5-23.

Carter, Ashton B., and William J. Perry. 1999. *Preventive Defense: A New Security Strategy for America*, Brookings Institution, Washington, D.C.

Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (Deutch Commission). 1999. *Combating Proliferation of Weapons of Mass Destruction,* July 14.

Commission on the Roles and Capabilities of the United States Intelligence Community (Brown Commission). 1996. *Preparing for the 21st Century—An Appraisal of U.S. Intelligence,* March.

Diamond, Jared. 2002. "Why We Must Feed the Hands That Could Bite Us," *Washington Post,* January 13.

Garwin, Richard L. 2001. "The Many Threats of Terror," *New York Review of Books,* October 2.

Garwin, Richard L. 2001. "The Many Threats of Terror: An Epilogue, *New York Review of Books,* December 22.

Garwin, Richard L., Ralph E. Gomory, and Matthew S. Meselson. 2002. "How to Fight Bioterrorism," *Washington Post,* May 14.

The Heritage Foundation Homeland Security Task Force. 2002. *Defending the American Homeland,* chaired by L. Paul Bremer III and Edwin Meese III, January. Available online at <http://www.heritage.org/homelanddefense/welcome.html>.

Holton, Gerald. 2002. "Reflections on Modern Terrorism," *Edge*. Revision, at certain points, of a paper with the same title, presented at the Conference on Terrorism, held at Stanford, California, 1976, and published in *TERRORISM: An International Journal*, Vol. 1, No. 3/4, 1978, pp. 265-276. Available online at <http://www.edge.org/3rd_culture/holton/holton_print.html>.

Homeland Security Council. 2001. *Homeland Security Presidential Directive–1, Subject: Organization and Operation of the Homeland Security Council,* October 29.

Homer-Dixon, Thomas. 2002. "The Rise of Complex Terrorism," *Foreign Policy: The Magazine of Global Politics, Economics, and Ideas*, January/February.

Huber, Peter, and Mark P. Mills. 2002. "How Technology Will Defeat Terrorism," *City Journal,* Winter, Vol. 12, No. 1. Available online at <http://www.city-journal.org/html/12_1_how_tech.html>.

Joint Task Force on Intelligence and Law Enforcement (Richards/Rindskopf Report). 1995. *Report to the Attorney General and the Director of Central Intelligence,* May.

Knezo, Genevieve J. 2001. *Federal Research and Development for Counter Terrorism: Organization, Funding, and Options,* November 26 (updated January 3, 2002), Order Code RL31202.

Knezo, Genevieve J. 2002. *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education,* Congressional Research Service, April 8. Available online at <http://www.fas.org/irp/crs/RL31354.pdf>.

Lewis, Bernard. 1990. "The Roots of Muslim Rage," *The Atlantic*, September.

Lewis, Bernard. 1993. *Islam and the West*, Oxford University Press, Inc., New York.

National Commission on Terrorism (Bremer Commission). 2000. *Countering the Changing Threat of International Terrorism,* September.

National Science Board, National Science Foundation. 2002. *Science and Engineering Indicators—2002, Volume 1*, NSB-02-1, Arlington, Va., U.S. Government Printing Office, Washington, D.C. Available online at <http://www.nsf.gov/sbe/srs/seind02/start.htm>.

National Science Board, National Science Foundation. 2002. *Science and Engineering Indicators—2002, Volume 2*, NSB-02-2, Arlington, Va., U.S. Government Printing Office, Washington, D.C. Available online at <http://www.nsf.gov/sbe/srs/seind02/start.htm>.

Nye, Joseph S. 2001. "How to Protect the Homeland," *New York Times,* September 25.

Office of Management and Budget. 2001. *Annual Report to Congress on Combating Terrorism,* August. Available online at <http://www.whitehouse.gov/omb/legislative/nsd_annual_report 2001.pdf>.

Office of Technology Assessment. 1991. *Technology Against Terrorism: The Federal Effort,* OTA-ISC-487, July. Available online at <http://www.wws.princeton.edu/~ota/disk1/1991/9139_n.html>.

O'Hanlon, Michael E., Peter R. Orszag, Ivo H. Daalder, I.M. Destler, David L. Gunter, Robert E. Litan, and James B. Steinberg. 2002. *Protecting the American Homeland: A Preliminary Analysis,* Brookings Institution Press, Washington, D.C., May.

The President's Commission on Critical Infrastructure Protection (Marsh Commission). 1997. *Critical Foundations,* October.

Ronfeldt, David, and John Arquila, eds. 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND, Santa Monica, Calif.

Singer, Maxine. 2002. "The Challenge to Science: How to Mobilize American Ingenuity," *The Age of Terror: America and the World Sfter September 11,* Strobe Talbott and Nauan Chanda, eds., Basic Books, New York.

U.S. Commission on National Security/21st Century (Hart-Rudman Commission, Phase III). 2001. *Road Map for National Security: Imperative for Change,* February 15.

U.S. Department of State. 2002. *Patterns of Global Terrorism 2001,* Counterterrorism Office, Washington, D.C., May 21. Available online at <www.state.gov/s/ct/rls/pgtrpt/2001/html>.

Appendixes

A

Committee and Staff Biographies

Lewis M. Branscomb is the emeritus Aetna Professor of Public Policy and Corporate Management and emeritus director of the Science, Technology, and Public Policy Program in the Center for Science and International Affairs at Harvard University's Kennedy School of Government. Dr. Branscomb, a member of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine, has a background in physics and public policy. He was a research physicist at the National Bureau of Standards (now the National Institute of Standards and Technology) and also served as its director. He was the founder and first director of the Joint Institute for Laboratory Astrophysics at the University of Colorado and an at-large director of the Associated Universities for Research in Astronomy. He served on the President's Science Advisory Committee (PSAC), where he chaired the PSAC committee on space science and technology during Project Apollo. Dr. Branscomb served as vice president and chief scientist of IBM Corporation until his retirement 1986. Dr. Branscomb is a former president of the American Physical Society and of Sigma Xi, the Scientific Research Society.

Richard D. Klausner is executive director of the global health programs at the Bill and Melinda Gates Foundation. Dr. Klausner, a member of the National Academy of Sciences and the Institute of Medicine, is well known for his contributions to multiple aspects of cell and molecular biology and is highly cited for work in biology and biomedical research. His work has been recognized with numerous honors and awards, including the Outstanding Investigator Award from the American Federation of Clinical Research and the William Damashek Prize for Major Discoveries in Hematology. From 1995 until 2001 he was director of

the National Cancer Institute. From 1984 until 1997 he was chief of the Cell Biology and Metabolism Branch of the National Institute of Child Health and Human Development. Dr. Klausner has served on numerous advisory committees, including as chair of an NRC project charged with writing standards for science education for the United States from kindergarten through 12th grade. Dr. Klausner is the past president of the American Society for Clinical Investigation. He is the author of over 280 scientific articles and several books.

John D. Baldeschwieler, is J. Stanley Johnson Professor and professor of chemistry, emeritus, at the California Institute of Technology. Dr. Baldeschwieler, a member of the National Academy of Sciences, joined the Caltech faculty (after several years at Harvard and Stanford universities) in 1973. His research has focused on molecular assemblies for use in the delivery of pharmaceuticals, for scientific instrumentation, and particularly for development of ion cyclotron resonance spectroscopy. He also pioneered the use of nuclear magnetic resonance and double resonance spectroscopy, nuclear Overhauser effects, and perturbed angular correlation spectroscopy in chemical systems. Dr. Baldeschwieler was a member of the President's Science Advisory Committee from 1969 to 1972, serving as vice chairman from 1970 to 1972. He served as deputy director of the Office of Science and Technology from 1971 to 1973. He is a fellow of the American Academy of Arts and Sciences and the American Philosophical Society. He was a founder of Vestar Inc., which merged with NeXagen Inc. to form NeXstar Pharmaceuticals. He also served as director of NeXstar until it was acquired by Gilead Sciences, Inc. Dr. Baldeschwieler was also a founder and director of Combion, Inc. He currently serves as a managing member of the Athenaeum Fund and is a director of Drug Royalty Corporation Inc., the Huntington Medical Research Institutes, Pasadena Entretec, and several privately held companies. He is a recipient of the National Medal of Science.

Barry R. Bloom is dean of the faculty and professor of immunology and infectious diseases at the Harvard School of Public Health. He received his B.A. degree and an honorary S.D. from Amherst College, his A.M. from Harvard University, and his Ph.D. from the Rockefeller University. Dr. Bloom served as a consultant to the White House on international health policy in 1977-1978. He is a member of the WHO Advisory Committee on Health Research and has chaired the WHO committees on leprosy research and tuberculosis research and the Scientific and Technical Advisory Committee of the UNDP/World Bank/WHO Special Programme for Research and Training in Tropical Diseases. Dr. Bloom chairs the WHO UNAIDS Vaccine Advisory Committee and serves on the National AIDS Vaccine Research Committee. He recently received a major grant from the Bill and Melinda Gates Foundation for an AIDS prevention initiative in Nigeria. He was a member of both the National Advisory Council of the National Institute for Allergy and Infectious Diseases at the National Institutes of Health (NIH) and the U.S. National Vaccine Advisory Committee. He was

elected president of the American Association of Immunologists in 1984 and served as president of the Federation of American Societies for Experimental Biology (FASEB) in 1985. He currently serves on the Scientific Advisory Board of the National Center for Infectious Diseases of the Centers for Disease Control and Prevention (CDC) and the National Advisory Board of the Fogarty International Center at the NIH. Dr. Bloom is chairman of the Board of Trustees of the International Vaccine Institute. He was co-chair of the Board on Global Health of the Institute of Medicine of the National Academy of Sciences. He received the first Bristol-Myers Squibb Award for Distinguished Research in Infectious Diseases, shared the Novartis Award in Immunology in 1998, and was the recipient of the Robert Koch Gold Medal for lifetime research in infectious diseases in 1999. Dr. Bloom is a member of the Institute of Medicine, the American Academy of Arts and Sciences, and the National Academy of Sciences.

L. Paul Bremer III is chairman of the crisis consulting practice of Marsh and McLennan Companies, Inc., the world's leading risk and insurance services firm. Prior to this position, Ambassador Bremer, an expert in terrorism, had a 23-year career in the U.S. diplomatic service. In 1999, Speaker of the House of Representatives Dennis Hastert appointed Ambassador Bremer as chairman of the National Commission on Terrorism. Earlier, he was ambassador-at-large for counter terrorism under President Ronald W. Reagan.

William F. Brinkman retired as vice president, research, at Bell Laboratories, Lucent Technologies, on September 30, 2001. In that position his responsibilities included the direction of all research to enable the advancement of the technology underlying Lucent Technologies' products. He received his B.S. and Ph.D. (physics) degrees from the University of Missouri in 1960 and 1965, respectively. He joined Bell Laboratories in 1966 after spending 1 year as an NSF postdoctoral fellow at Oxford University in 1965. In 1972 he became Head of the Infrared Physics and Electronics Research Department, and in 1974 became the director of the Chemical Physics Laboratory. He held the position of director of the Physical Research Laboratory from 1981 until moving to Sandia in 1984. He returned to Bell Laboratories in 1987 to become executive director of the Physics Research Division. In 1993 he became Physical Sciences Research Vice President, and in January 2000 became Vice President, Research. He has worked on theories of condensed matter, and his early work involved the theory of spin fluctuations in metals and other highly correlated Fermi liquids. This work resulted in a new approach to highly correlated liquids in terms of almost localized liquids and to a theory of the metal-insulator transition. The explanation of the superfluid phases of one of the isotopes of helium and many properties of these exotic states of matter was a major contribution in the mid-1970s. The theoretical explanation of the existence of electron-hole liquids in semiconductors was another contribution in that period. Subsequent theoretical work on liquid crystals and incommensurate systems brought additional important contri-

butions to the theoretical understanding of condensed matter. Dr. Brinkman is strongly interested in improving technology and the connection between research and products. He has also been heavily involved in transferring optical technology and helped create Lucent's rapidly expanding optoelectronics business. He has served on many advisory committees. He is a member of the National Academy of Sciences and the American Academy of Arts and Sciences. He was chair of the National Academy of Sciences Physics Survey and the Solid-State Sciences Committee. He served on the Council of the National Academy of Sciences and is president of the American Physical Society. Dr. Brinkman was the recipient of the 1994 George E. Pake Prize.

Ashton B. Carter is Ford Foundation Professor of Science and International Affairs at Harvard University's John F. Kennedy School of Government and co-director, with William J. Perry, of the Preventive Defense Project, a research collaboration of Stanford University and Harvard University's Kennedy School of Government. From 1993 to 1996, Dr. Carter served as Assistant Secretary of Defense for International Security Policy, where he was responsible for national security policy concerning the states of the former Soviet Union. He was twice awarded the Department of Defense Distinguished Service medal. Dr. Carter continues to serve the Department of Defense as an adviser to the Secretary of Defense and as a member of the Defense Science Board and DOD's Threat Reduction Advisory Committee. From 1998 to 2000, he served in an official capacity as senior advisor to the North Korea Policy Review. Before his government service, Carter was director of the Center for Science and International Affairs in the Kennedy School of Government at Harvard University and chairman of the editorial board of International Security. Dr. Carter received bachelor's degrees in physics and in medieval history from Yale University and a doctorate in theoretical physics from Oxford University, where he was a Rhodes Scholar. In addition to authoring numerous scientific publications and government studies, Dr. Carter is the author and editor of a number of books, including *Preventive Defense: A New Security Strategy for America* (with William J. Perry). Dr. Carter's current research focuses on the Preventive Defense Project, which designs and promotes security policies aimed at preventing the emergence of major new threats to the United States. He is a senior partner of Global Technology Partners, LLC, a chairman of the Advisory Board of MIT Lincoln Laboratories, and a member of the Draper Laboratory Corporation and of the board of directors of Mitretek Systems, Inc. Dr. Carter is a consultant to Goldman Sachs and the MITRE Corporation on international affairs and technology matters, a member of the Council on Foreign Relations, the Aspen Strategy Group, and the National Committee on U.S.-China Relations, and a fellow of the American Academy of Arts and Sciences.

Charles B. Curtis is the president and chief operating officer of the Nuclear Threat Initiative. Previously, Mr. Curtis served as the executive vice president

and chief operating officer of the United Nations Foundation. Before joining UNF, Mr. Curtis was a partner in Hogan and Hartson, a Washington-based law firm with both domestic and international offices. Mr. Curtis served as Under Secretary and, later, Deputy Secretary of Energy from February 1994 to May 1997. He was the chief operating officer of the Department and, among other duties, had direct programmatic responsibility for all its energy, science, technology and national security programs. Mr. Curtis is a lawyer with over 15 years of practice experience and more than 18 years in government service. He was a founding partner of the Washington law firm Van Ness Feldman. Mr. Curtis has held positions on the staff of the U.S. House of Representatives, the U.S. Treasury, the Securities and Exchange Commission, and the Federal Energy Regulatory Commission, which he chaired from 1977 to 1981. He is a current member of the Council on Foreign Relations.

Mortimer L. Downey III, former U.S. Deputy Secretary of Transportation, is a principal consultant with PB-Consult, the management consulting subsidiary of Parsons Brinckerhoff. As deputy secretary from 1993 to 2001, Mr. Downey was the U.S. Department of Transportation's chief operating officer. He also served on the President's Management Council, as Chairman of the National Science and Technology Council's Committee on Transportation Research and Development, and as a member of the board of directors of Amtrak. Previously, Mr. Downey was executive director and chief financial officer of New York's Metropolitan Transportation Authority, the nation's largest independent public authority. He is well known for developing innovative solutions to complex public policy issues and has championed a systemwide approach to transportation decision making. Mr. Downey serves as the chairman of the board of directors of the National Academy of Public Administration and as a board member of the Eno Transportation Foundation. He received the Frank Turner Lifetime Achievement Award from the Transportation Research Board, the Lifetime Achievement Award from the American Public Transportation Association, and the Leadership Award from ITS America.

Richard L. Garwin is the Phillip D. Reed Senior Fellow for Science and Technology at the Council on Foreign Relations, New York, and an emeritus fellow at IBM's T.J. Watson Research Center. Dr. Garwin is a member of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. His expertise in experimental and computational physics includes contributions to nuclear weapons design, instruments and electronics for nuclear and low-temperature physics, computer elements and systems, superconducting devices, communications systems, behavior of solid helium, and detection of gravitational radiation. He was a member of the President's Science Advisory Committee from 1962 to 1965 and 1969 to 1972 and of the Defense Science Board from 1966 to 1969. He currently consults for the Los Alamos National Laboratory, Sandia National Laboratories, and the Council on Foreign Relations

and is an active member of the JASONs. In 1998, he was a member of the nine-person Commission to Assess the Ballistic Missile Threat to the United States (Rumsfeld Commission). He has written extensively on nuclear weapons-related issues over the course of several decades, particularly on the question of maintaining the nuclear stockpile under a comprehensive test ban regime. Until August 2001, he chaired the State Department's Arms Control and Nonproliferation Advisory Board. He is a fellow of the American Physical Society and the American Academy of Arts and Sciences and a member of the American Philosophical Society.

Paul H. Gilbert is senior vice president, principal professional associate, and principal project manager of Parsons Brinckerhoff Quade and Douglas, Inc., senior vice president of Parsons Brinckerhoff International Inc., and recently retired as director of Parsons Brinckerhoff, Inc. and of Parsons Brinckerhoff International, Inc., and as chairman of Parsons Brinckerhoff Quade and Douglas, Inc. A member of the National Academy of Engineering, his expertise is in project management of design and construction of large complex facilities. Mr. Gilbert was the project director of the PB/MK team for design, construction management, and construction of the conventional facilities of the Department of Energy's superconducting super collider. He has served as principal-in-charge for major engineering projects such as the Stanford Linear Accelerator Positron-Electron Project, the Basalt Waste Isolation Project at Hanford, the Nuclear Power Plants in Mined Caverns Study, the Downtown Seattle Transit Project, the Long Beach Naval Fuel Pier, and the Boston and San Francisco Effluent Outfall Tunnels. He is the author of Parsons Brinckerhoff's *Project Management Manual* and has also published various technical papers and articles. Mr. Gilbert is a member of a variety of professional organizations, including the American Society of Civil Engineers, The Moles, Project Management Institute, and Society of American Military Engineers. He has won numerous awards in civil engineering and construction management, including American Society of Civil Engineers fellow, the Rickey Medal, and the Construction Management Award.

M.R.C. Greenwood is chancellor of the University of California, Santa Cruz, a position she has held since July 1, 1996. In addition to her position as chancellor, Dr. Greenwood also holds a UC Santa Cruz appointment as professor of biology. A member of the Institute of Medicine, her research interests are in developmental cell biology, genetics, physiology, nutrition, and science and higher education policy issues. Her work over the past 25 years has focused on the genetic causes of obesity. Prior to her UC Santa Cruz appointments, Chancellor Greenwood served as dean of graduate studies, vice provost for academic outreach, and professor of biology and internal medicine at the University of California, Davis. Previously, Dr. Greenwood taught at Vassar College, where she was the John Guy Vassar Professor of Natural Sciences, chair of the Department of Biology, and director of the Undergraduate Research Summer Institute. From November

1993 to May 1995, Dr. Greenwood held an appointment as associate director for science at the Office of Science and Technology Policy in the Executive Office of the President of the United States. Dr. Greenwood is a fellow of the American Association for the Advancement of Science and of the California Academy of Sciences. She has been honored by numerous organizations for her contributions to science and science policy. She was (1998) president of the American Association for the Advancement of Science and served as AAAS's board chair in 1999. She is a Presidential appointee, U.S. Senate-confirmed member of the National Science Board. She also served as a member of the board of directors of the National Association of State Universities and Land-Grant Colleges (NASULGC) and serves on the Science Advisory Board of the National Oceanic and Atmospheric Administration (NOAA). She is an ex officio member of the board of directors of the Tech Museum of Innovation in California and serves on the board of directors of the California Healthcare Institute. In March 2000, Dr. Greenwood was appointed to Governor Davis's Council on Bioscience. She also serves on the board of directors of the Silicon Valley Manufacturing Group.

Margaret A. Hamburg, M.D., is vice president for biological programs, Nuclear Threat Initiative, whose mission is to strengthen global security by reducing the risk of use and preventing the spread of nuclear and other weapons of mass destruction. Before her current position, she was the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services. Prior to that, Dr. Hamburg served for almost 6 years as the Commissioner of Health for the City of New York, and one of her many accomplishments included the creation of the first public health bioterrorism preparedness program in the nation. She completed her internship and residency in internal medicine at the New York Hospital/Cornell University Medical Center and is certified by the American Board of Internal Medicine. Dr. Hamburg is a graduate of Harvard College and Harvard Medical School. She currently serves on the Harvard University Board of Overseers. She is a member of the Institute of Medicine, the New York Academy of Medicine, the Council on Foreign Relations, and is a fellow of the American Association of the Advancement of Science.

William Happer is a professor in the Department of Physics at Princeton University. Dr. Happer, a member of the National Academy of Sciences, specializes in modern optics, optical and radiofrequency spectroscopy of atoms and molecules, and spin-polarized atoms and nuclei. In 1964, Dr. Happer was a research associate at the Columbia University Radiation Laboratory and also served as a physics professor. He was codirector of the Columbia Radiation Laboratory from 1971 to 1976 and director from 1976 to 1979. Dr. Happer was awarded the Class of 1909 Professorship of Physics at Princeton in 1988. In 1991, he was appointed director of energy research in the Department of Energy, where he oversaw a basic research portfolio that included much of the federal funding for high-energy and nuclear physics, materials science, magnetic confinement fu-

sion, environmental science, the Human Genome Project, and other areas. In 1993 he was reappointed professor of physics at Princeton University and was named Eugene Higgens Professor of Physics and chair of the University Research Board in 1995. Throughout his career, Dr. Happer has served as a scientific consultant to numerous firms, charitable organizations, and government agencies. He was a founder of Magnetic Imaging Technologies, Inc. (now part of Nycomed Amersham), a startup company focused on the development of magnetic resonance imaging with laser-polarized helium-3 and xenon-129. He has published over 160 scientific papers. He is a fellow of the American Physical Society and the American Association for the Advancement of Science; he is also a member of the American Academy of Arts and Sciences and the American Philosophical Society. Dr. Happer was awarded an Alfred P. Sloan Fellowship in 1966, an Alexander von Humboldt Award in 1976, the 1997 Broida Prize, and the 1999 Davisson-Germer Prize of the American Physical Society.

John L. Hennessy is president of Stanford University. Dr. Hennessy, a member of the National Academy of Engineering, received his master's and doctoral degrees in computer science from the State University of New York at Stony Brook in 1975 and 1977, respectively. In the fall of 1977 he joined Stanford as assistant professor of electrical engineering, rising to associate professor in 1983 and full professor in 1986. Professor Hennessy initiated the MIPS project at Stanford in 1981 (MIPS is a high-performance Reduced Instruction Set Computer (RISC)), built in VLSI. MIPS is one of the first three experimental RISC architectures. In addition to his role in the basic research, Dr. Hennessy played a key role in transferring this technology to industry. During a sabbatical leave from Stanford in 1984 to 1985, he cofounded MIPS Computer Systems (now called MIPS Technologies, Inc.), which specializes in the production of chips based on these concepts. He also led the Stanford DASH (Distributed Architecture for Shared Memory) multiprocessor project. DASH was the first scalable shared-memory multiprocessor with hardware-supported cache coherence. Most recently, he has been involved in FLASH (FLexible Architecture for Shared Memory), which is designed to support different communication and coherency approaches in large-scale, shared-memory multiprocessors.

Joshua Lederberg is Sackler Foundation Scholar at the Rockefeller University. Dr. Lederberg, a member of the National Academy of Sciences and the Institute of Medicine, has an extensive background in biological and physical sciences, including bacteriology, biochemistry, biophysics, epidemiology, genetics, microbiology, molecular biology, toxicology, and virology. He is a leading geneticist and microbiologist who received the Nobel Prize in 1958 for his work in genetic structure and function in microorganisms (he was also awarded the U.S. National Medal of Science in 1989). Prior to serving as president of the Rockefeller University from 1978 to 1990, Dr. Lederberg served on the faculty at the University of Wisconsin and at the Stanford School of Medicine. He has served on

numerous scientific boards and advisory committees, including the WHO's Advisory Health Research Council, the President's Cancer Panel, and the Congress Technology Assessment Advisory Council.

Thomas C. Schelling is Distinguished University Professor and professor of economics, emeritus, of Harvard University. A member of the National Academy of Sciences and the Institute of Medicine, Dr. Schelling's research interests have included military strategy and arms control, energy and environmental policy, climate change, nuclear proliferation, organized crime, foreign aid and international trade, conflict and bargaining theory, racial segregation and integration, the military draft, tobacco and drugs policy, and ethical issues in policy and in business. He spent the years 1948 to 1953 in Europe and Washington with the Marshall Plan and related programs, joined Yale University in 1953, Harvard University in 1958, and came to Maryland in 1990. He is a distinguished fellow of the American Economic Association and was its president in 1991. In 1993, he received the National Academy of Sciences award for Behavioral Research Relevant to the Prevention of Nuclear War.

Maxine F. Singer is the president of the Carnegie Institution of Washington and scientist emeritus at the National Cancer Institute, National Institutes of Health in Bethesda, Maryland. Prior to coming to Carnegie in 1988, she was chief of the Laboratory of Biochemistry, Division of Cancer Biology and Diagnosis at the National Cancer Institute, where she conducted research in biological chemistry and molecular genetics. At the Carnegie Institution, Dr. Singer oversees operations and research of five renowned scientific research laboratories. She also has instituted a community outreach and education program that brings leading scientific speakers to the community and trains local science teachers. Dr. Singer is a member of various advisory panels to scientific societies, the government, and academia. Currently she chairs the National Academies' Committee on Science, Engineering and Public Policy and serves on the NASA Astrobiology Institute Scientific Advisory Board. Dr. Maxine Singer is a member of the National Academy of Sciences and the Institute of Medicine.

Neil J. Smelser served as the director of the Center for Advanced Study in the Behavorial Sciences, Stanford, California, from 1994 to August 2001. His research interests are sociological theory, economic sociology, collective behavior, sociology of education, social change, and comparative methods. From 1958 to 1994 he was on the faculty of the Sociology Department of the University of California, Berkeley, serving as university professor since 1971. He is a member of the American Academy of Arts and Sciences, the American Philosophical Society, and the National Academy of Sciences.

Philip M. Smith is co-chair of the Advisory Board, California Institute for Telecommunications and Information Technology, and is a partner in McGeary and Smith, consultants on science and technology policy. He has been involved in

developing national and international science and technology policy and programs since the 1950s. Dr. Smith was the executive director of the National Research Council for 13 years and has held senior positions in the White House Office of Science and Technology Policy, the Office of Management and Budget, and the National Science Foundation. He was a member of the NRC Committee on Science, Technology and Health Aspects of the Foreign Policy Agenda of the United States, is a member of several current advisory committees for the National Academies and the American Association for the Advancement of Science, was an advisor to the Committee for Economic Development, and is a director at Aurora Flight Sciences, Inc.

P. Roy Vagelos is retired chairman and CEO of Merck and Company, Inc., having served as chief executive officer for 9 years, from 1985 to 1994. He was first elected to the board of directors in 1984 and served as its chairman from 1986 to 1994. He was previously executive vice president of the worldwide health products company and before that president of its research division. Earlier, he served as chairman of the Department of Biological Chemistry of the School of Medicine at Washington University in St. Louis and as founding director of the university's Division of Biology and Biomedical Sciences. He had previously held senior positions in cellular physiology and biochemistry at the National Heart Institute. Dr. Vagelos is a member of the National Academy of Sciences, the Institute of Medicine, the American Academy of Arts and Sciences, and the American Philosophical Society. He received his M.D. degree from Columbia University in 1954. In 1995, he received the National Academy of Science Award for Chemistry in Service to Society.

Vincent Vitto is the president and CEO of Charles Stark Draper Laboratory, Inc., which specializes in guidance, navigation and control, and autonomy and microelectronics. His areas of expertise are communications and surveillance technologies. As assistant director of the Lincoln Laboratory of the Massachusetts Institute of Technology (MIT), he was responsible for programs in surface surveillance and communications. Prior to that position, Mr. Vitto was head of the Communications Division, which included work on technology and system concept development of military satellite communications systems. Mr. Vitto has been a member of many government advisory boards and panels; he currently is vice chair of the Defense Science Board and chair of NRC's Naval Studies Board.

George M. Whitesides is Mallinckrodt Professor of Chemistry at Harvard University. Professor Whitesides, a member of the National Academy of Sciences, has a background in biological and physical sciences, including materials science, organic chemistry, and biochemistry. He is a leading chemist who received the U.S. National Medal of Science in 1998. His research interests include surface chemistry, materials science, self-assembly, capillary electrophoresis,

organic solid state, molecular virology, directed ligand discovery, and protein chemistry. He has served on numerous scientific boards and advisory committees including, most recently, a biological warfare defense study for the Department of Defense.

R. James Woolsey is a partner at the law firm of Shea & Gardner in Washington, D.C. He returned to the firm in January 1995 after serving 2 years as director of Central Intelligence. He has practiced there for 21 years, on four occasions, since 1973. Mr. Woolsey's law practice has been in the fields of civil litigation, alternative dispute resolution, and corporate transactions; increasingly his practice has been international. He served recently as counsel for major U.S. and overseas corporations in both commercial arbitrations and the negotiation of joint ventures and other agreements. He serves regularly as a neutral (both as an arbitrator and a mediator) in commercial disputes between major companies. Mr. Woolsey is presently a member of the board of directors or board of managers of Linsang Partners, LLC; BC International Corporation; Fibersense Technology Corporation; Invicta Networks, Inc.; DIANA, LLC; and Agorics, Inc. He is also a member of the board of governors of the Philadelphia Stock Exchange. He has served in the past as a member of the boards of Sun HealthCare Group, Inc.; USF&G; Yurie Systems, Inc.; Martin Marietta; British Aerospace, Inc.; Fairchild Industries; Titan Corporation; and DynCorp. Besides serving as director of Central Intelligence, Mr. Woolsey has served in the U.S. government as ambassador to the Negotiation on Conventional Armed Forces in Europe (CFE), Vienna, 1989-1991; Under Secretary of the Navy, 1977-1979; and General Counsel to the U.S. Senate Committee on Armed Services, 1970-1973. He was also appointed by the President as delegate at large to the U.S.-Soviet Strategic Arms Reduction Talks (START) and Nuclear and Space Arms Talks (NST), and served in that capacity on a part-time basis in Geneva, 1983-1986. During military service in the U.S. Army he served as an adviser on the U.S. delegation to the Strategic Arms Limitation Talks (SALT I), Helsinki and Vienna, 1969 to 1970. Mr. Woolsey has been a director or trustee of numerous civic organizations, including the Smithsonian Institution, where he was chairman of the Executive Committee of the Board of Regents, the Goldwater Scholarship Foundation, The Aerospace Corporation, and Stanford University. He has been a member of the National Commission on Terrorism, 1999-2000; the Commission to Assess the Ballistic Missile Threat to the U.S. (Rumsfeld Commission), 1998; the President's Commission on Federal Ethics Law Reform, 1989; the President's Blue Ribbon Commission on Defense Management (Packard Commission), 1985-1986; and the President's Commission on Strategic Forces (Scowcroft Commission), 1983. He is currently a trustee of the Center for Strategic and International Studies and chairman of the Advisory Committee of the Clean Fuels Foundation.

Staff

Ronald D. Taylor has been the director of the Naval Studies Board of the National Research Council since 1995. He joined the National Research Council in 1990 as a program officer with the Board on Physics and Astronomy and in 1994 became associate director of the Naval Studies Board. During his tenure at the National Research Council, Dr. Taylor has overseen the initiation and production of more than 40 studies focused on the application of science and technology to problems of national interest. Many of these studies address national security and national defense issues. From 1984 to 1990, Dr. Taylor was a research staff scientist with Berkeley Research Associates, working on-site at the Naval Research Laboratory on projects related to the development and application of charged particle beams. Prior to 1984, Dr. Taylor held both teaching and research positions in several academic institutions, including assistant professor of physics at Villanova University, research associate in chemistry at the University of Toronto, and instructor of physics at Embry-Riddle Aeronautical University. Dr. Taylor holds a Ph.D. and an M.S. in physics from the College of William and Mary and a B.A. in physics from Johns Hopkins University. In addition to science policy, Dr. Taylor's scientific and technical expertise is in the areas of atomic and molecular collision theory, chemical dynamics, and atomic processes in plasmas. He has authored or coauthored nearly 30 professional scientific papers or technical reports and given more than two dozen contributed or invited papers at scientific meetings.

Elizabeth L. Grossman has been a program officer at the National Research Council since March of 1997. Past reports she has worked on include *Black and Smokeless Powders: Technologies for Finding Bombs and the Bomb Makers*, a study that examined the problems related to preventing the use of pipe bombs in the United States, and *Future Biotechnology on the International Space Station*, an examination of the plans for cellular biology and protein crystal growth research on the space station. Her regular position is with the Board on Assessment of NIST Programs, which produces an annual report evaluating the broad array of research programs at the National Institute of Standards and Technology. She holds a B.A. in physics and mathematics from Swarthmore College and a Ph.D. in computational physics from the University of Chicago.

B

Panel Members and Staff

PANEL ON BIOLOGICAL ISSUES

Barry R. Bloom, *Co-chair*, Harvard School of Public Health
Joshua Lederberg, *Co-chair*, Sackler Foundation at the Rockefeller University
Ronald Atlas, University of Louisville
Ruth Berkelman, Emory University
Gail Cassell, Lilly Research Laboratories, Eli Lilly and Company
Thomas R. Cech, Howard Hughes Medical Institute
David Franz, Southern Research Institute
Claire Fraser, Institute for Genomic Research
David Galas, Keck Graduate Institute of Applied Life Sciences
CDR Shaun Jones, U.S. Navy
Robert A. Lamb, Howard Hughes Medical Institute/Northwestern University
Simon Levin, Princeton University
John Mekalanos, Harvard Medical School
Tom Monath, Acambis, Inc.
Randall Murch, Federal Bureau of Investigation
Edward D. Penhoet, University of California, Berkeley
David Relman, Stanford University
Peter Rosen, University of California, San Diego
Luis Sequeira, University of Wisconsin
Jeffery Taubenberger, Armed Forces Institute of Pathology
Dean Wilkening, Stanford University
Catherine Woteki, Iowa State University

Staff

Andrew M. Pope, Director, Board on Health Sciences Policy
Cathy T. Liverman, Senior Program Officer, Board on Health Promotion and Disease Prevention
Jennifer Kuzma, Senior Program Officer, Board on Life Sciences
Kathi E. Hanna, Consultant
Alden B. Chang, Administrative Assistant, Board on Health Sciences Policy

PANEL ON CHEMICAL ISSUES

John D. Baldeschwieler, *Chair*, California Institute of Technology
Lynn F. Schneemeyer, *Vice Chair*, Lucent Technologies (formerly)
Will D. Carpenter, Monsanto (retired)
Rolf Deininger, University of Michigan
Crispin Eley, Gilead Sciences
David Fontaine, ChevronTexaco
Victoria F. Haynes, Research Triangle Institute
Alexander MacLachlan, DuPont (retired)
Norman Singer, Ideas Workshop, Inc.
Timothy M. Swager, Massachusetts Institute of Technology
Charles Zukoski, University of Illinois

Staff

Chris Elfring, Director, Polar Research Board
Chadwick A. Tolman, Program Officer, Board on Environmental Studies and Toxicology
Gregory H. Symmes, Associate Executive Director, Division on Earth and Life Studies
Bryan P. Shipley, Senior Project Assistant, Board on Environmental Studies and Toxicology

PANEL ON NUCLEAR AND RADIOLOGICAL ISSUES

William Happer, *Chair*, Princeton University
Harold M. Agnew, Los Alamos Scientific Laboratory (retired)
Michael R. Anastasio, Lawrence Livermore National Laboratory
Robert J. Budnitz, Future Resources Associates, Inc.
Richard L. Garwin, Council on Foreign Relations
Roger L. Hagengruber, Sandia National Laboratories
Glenn F. Knoll, University of Michigan

George W. Ullrich, Office of the Deputy Under Secretary of Defense for Science and Technology

Staff

Kevin D. Crowley, Director, Board on Radioactive Waste Management
Micah D. Lowenthal, Program Officer, Board on Radioactive Waste Management
Darla J. Thompson, Senior Project Assistant/Research Assistant, Board on Radioactive Waste Management

PANEL ON INFORMATION TECHNOLOGY

John L. Hennessy, *Co-chair*, Stanford University
David Patterson, *Co-chair*, University of California, Berkeley
Steven Bellovin, AT&T Research
W. Earl Boebert, Sandia National Laboratories
David Borth, Motorola Laboratories
William F. Brinkman, Bell Laboratories/Lucent Technologies (retired)
John M. Cioffi, Stanford University
W. Bruce Croft, University of Massachusetts, Amherst
William P. Crowell, Cylink
Jeffrey M. Jaffee, Lucent Technologies
Butler W. Lampson, Microsoft Corporation
Edward D. Lazowska, University of Washington
David E. Liddle, U.S. Venture Partners
Tom Mitchell, Carnegie Mellon University
Donald A. Norman, Nielsen Norman Group
Jeannette M. Wing, Carnegie Mellon University

Staff

Herbert S. Lin, Senior Scientist, Computer Science and Telecommunications Board
Steven E. Woo, Program Officer, Computer Science and Telecommunications Board
David Drake, Senior Project Assistant, Computer Science and Telecommunications Board

PANEL ON TRANSPORTATION

Mortimer L. Downey, *Chair*, PB-Consult
H. Norman Abramson, Southwest Research Institute

Lisa M. Bendixen, Arthur D. Little, Inc.
Anthony J. Broderick, Federal Aviation Administration (retired)
Noel K. Cunningham, Port of Los Angeles
John J. Fearnsides, George Mason University
CDR Stephen E. Flynn, U.S. Coast Guard
Francis B. Francois, American Association of State Highway and Transportation Officials (retired)
Ernest R. Frazier, Sr., National Railroad Passenger Corporation
Robert E. Gallamore, Northwestern University
Henry L. Hungerbeeler, Missouri Department of Transportation
Brian M. Jenkins, RAND
Daniel Murray, ATA Foundation
Edmond L. Soliday, United Airlines (retired)
Richard A. White, Washington Metropolitan Area Transit Authority
James A. Wilding, Metropolitan Washington Airports Authority

Staff

Thomas R. Menzies, Jr., Senior Program Officer, Transportation Research Board

PANEL ON ENERGY FACILITIES, CITIES, AND FIXED INFRASTRUCTURE

Paul H. Gilbert, *Chair*, Parsons Brinckerhoff Quade and Douglas, Inc.
Edward V. Badolato, Contingency Management Services, Inc.
Gregory B. Baecher, University of Maryland
Benjamin S. Cooper, Association of Oil Pipe Lines
Jeremy Isenberg, Weidlinger Associates, Inc.
Lawrence T. Papay, Science Applications International, Corporation
Michael P. Ramage, ExxonMobil (retired)
Lawrence Spielvogel, Consulting Engineer
Joan B. Woodard, Sandia National Laboratories
John J. Wise, *Liaison from Board on Energy and Environmental Systems,* Mobil Research and Engineering Company (retired)

Staff

James J. Zucchetto, Director, Board on Energy and Environmental Systems
Alan T. Crane, Senior Program Officer, Board on Energy and Environmental Systems
Panola D. Golson, Senior Project Assistant, Board on Energy and Environmental Systems

PANEL ON BEHAVIORAL, SOCIAL, AND INSTITUTIONAL ISSUES

Neil J. Smelser, *Chair*, University of California, Berkeley (emeritus)
Robert McCormick Adams, University of California, San Diego
Lisa Anderson, Columbia University
Nazli Choucri, Massachusetts Institute of Technology
Eugene Hammel, University of California, Berkeley (emeritus)
Arie Kruglanski, University of Maryland
Ira Lapidus, University of California, Berkeley (emeritus)
Timothy McDaniel, University of California, San Diego
Phyllis Oakley, U.S. Department of State (retired)
Thomas C. Schelling, University of Maryland

Staff

M. Faith Mitchell, Deputy Director, Division of Behavioral and Social Sciences and Education
Janet E. Garton, Program Associate, Board on Behavioral, Cognitive, and Sensory Sciences and Education
Benjamin Woolsey, Project Assistant, Center for Social and Economic Studies

PANEL ON SYSTEMS ANALYSIS AND SYSTEMS ENGINEERING

Vincent Vitto, *Chair,* Charles S. Draper Laboratory, Inc.
David F. Andersen, State University of New York at Albany
Robert F. Brammer, TASC, Northrop Grumman Corporation
Ashton B. Carter, Harvard University
Paul K. Davis, RAND
Yacov Y. Haimes, University of Virginia
Daniel E. Hastings, Massachusetts Institute of Technology
M. Elisabeth Paté-Cornell, Stanford University
William B. Rouse, Georgia Institute of Technology
Andrew P. Sage, George Mason University
Robert J. Thomas, Cornell University
Samuel G. Varnado, Sandia National Laboratories
George M. Whitesides, Harvard University

Staff

Charles F. Draper, Senior Program Officer, Naval Studies Board
Sidney G. Reed, Consultant, Naval Studies Board
Mary G. Gordon, Information Officer, Naval Studies Board
Susan G. Campbell, Administrative Assistant, Naval Studies Board
Ian M. Cameron, Project Assistant, Naval Studies Board

C

Panel Activities

PANEL ON BIOLOGICAL ISSUES

Co-chaired by STCT committee members Barry Bloom and Joshua Lederberg, the Biological Panel consisted of 22 members with expertise in medicine, public health, microbiology, cellular biology, virology, drug and vaccine development, health policy, laboratory analysis, plant pathology, zoonotic disease, food-borne disease, molecular biology, genomics, emergency medical response systems, infectious disease, bioterrorism, bioforensics, statistics, and epidemiological modeling.

The panel convened three times and communicated by e-mail and conference calls over a 3-month period. During its meetings, the panel received briefings on research and development activities within the U.S. Department of Defense as well as at the Department of Health and Human Services. The panel greatly appreciates the briefings it received from the following individuals: William Winkenwerder, Department of Defense; Kevin Tonat, Department of Health and Human Services, Office of Emergency Preparedness; Anthony Fauci, National Institute of Allergy and Infectious Diseases; Kathryn Zoon, Center for Biologics Evaluation and Review, Food and Drug Administration; David Lipman, National Center for Biotechnology Information, National Library of Medicine; Chuck Ludlum, Office of Senator Joseph Lieberman; and William Dallas Jones, California Office of Emergency Services.

PANEL ON CHEMICAL ISSUES

Chaired by STCT committee member John D. Baldeschwieler and co-chaired by Lynn Schneemeyer, the Chemical Panel consisted of 11 members with exper-

tise in the areas of chemistry, chemical engineering, sensors, chemical weapons, industrial chemistry, dispersion modeling, pharmaceutical manufacturing, food safety, and water supply. In addition, William F. Brinkman, a member of the STCT committee, provided helpful input.

The panel met twice, in January and February, and then communicated by a series of conference calls and e-mail exchanges. The first meeting was held at Irvine in conjunction with the Workshop on National Security and Homeland Defense hosted by the NRC Board on Chemical Science and Technology. At the workshop the panel heard military, industrial, and civilian perspectives on security by David R. Franz (Southern Research Institute), Scott D. Cunningham (DuPont), and Richard L. Garwin (IBM). At the second meeting, in Washington, D.C., the panel heard a presentation by David Kontny, the Canine and Explosives Program manager at the FAA. The panel was also supplied with numerous publications to serve as background and to inform its work.

PANEL ON NUCLEAR AND RADIOLOGICAL ISSUES

Chaired by STCT committee member William Happer, the Nuclear and Radiological Panel consisted of eight members with expertise in nuclear weapons design, capabilities, and use; nuclear weapons and materials protection, control, and accounting; nuclear material detectors and sensors; conventional weapons capabilities; and reactor safety. The panel met four times and communicated by e-mail and conference calls over a 3-month period. During its meetings, the panel received briefings from representatives of several agencies and organizations, including the Central Intelligence Agency, Department of Defense, Department of Energy and its national laboratories, Federal Aviation Administration, Nuclear Regulatory Commission, Office of Science and Technology Policy, Nuclear Energy Institute, and NAC International. More details on speakers and topics are provided in the classified annex to this report.

PANEL ON INFORMATION TECHNOLOGY

Co-chaired by John L. Hennessy (STCT committee member) and David Patterson, the Information Technology Panel consisted of 16 members with expertise in computer, information, Internet, and network security; computer and systems architecture; computer systems innovation, including interactive systems; national security and intelligence; telecommunications, including wireline and wireless; data mining, fusion, and information management; machine learning and artificial intelligence; automated reasoning tools; information processing technologies; information retrieval; networked, distributed, and high-performance systems; software; and human factors. The panel met three times over 2 months and communicated by e-mail and conference calls during the project. During its meetings, the panel heard from experts in cybersecurity and national security and

intelligence, including (panel member) Bill Crowell, president and chief executive officer of Cylink, and John Hamre, president and chief executive officer of the Center for Strategic and International Studies.

PANEL ON TRANSPORTATION

Chaired by STCT committee member Mortimer L. Downey, the Transportation Panel consisted of 16 members with expertise in transportation operations and administration; research and technology; and safety, security, and law enforcement. The panel convened twice and communicated by e-mail and conference calls over a 3-month period. During its meetings, the panel received briefings on the security-related R&D activities of most of the modal agencies within the U.S. Department of Transportation. Thanks are due to Steven Ditmeyer, Federal Railroad Administration; James O'Steen and Frits Wybenga, Research and Special Programs Administration; David Price and Michael Trentacoste, Federal Highway Administration; Douglas McKelvey, Federal Motor Carrier Safety Administration; Lyle Malotky, Federal Aviation Administration; William Siegel, Federal Transit Administration; Captain James Evans, U.S. Coast Guard; and Richard John and Michael Dinning of the Volpe National Transportation Systems Center. Thomas Day, vice president for engineering, U.S. Postal Service, also made valuable contributions to the panel's considerations.

The panel also met with other experts outside government. Joseph Del Balzo, JDA Aviation Technology Solutions, discussed technological possibilities for computerized prescreening of passenger traffic to enhance aviation security. Thomas Hartwick discussed the state of sensor and screening technologies and systems for improving aviation security. Raja Parasuraman, Catholic University, and Victor Riley, Honeywell Corporation, discussed the role of human factors in the design, development, and deployment of security technologies and systems. The panel extends its gratitude to all four for their valuable contributions.

In addition, the panel wishes to thank Stephen McHale, Deputy Under Secretary for Transportation Security, and Paul Busick, Acting Associate Administrator for Civil Aviation Security. Both briefed the panel on the status of the newly created Transportation Security Administration and welcomed panel member ideas and comments.

PANEL ON ENERGY FACILITIES, CITIES, AND FIXED INFRASTRUCTURE

Chaired by STCT committee member Paul H. Gilbert, the Energy Facilities, Cities, and Fixed Infrastructure Panel consisted of nine members with experience in the electricity, oil, and gas sectors, and in buildings and other structures, water systems, and in vulnerability to attacks. The panel worked intensively, meeting

three times in 3 months and communicating frequently by phone and e-mail. The panel drew on information provided by a number of briefings and from a variety of other sources as well as on the panel members' own expertise; the panel's contribution was crucial in the preparation of two chapters, "Energy Systems" and "Cities and Fixed Infrastructure."

Briefings to the panel were made by Massoud Amin, Electric Power Research Institute; Harvey M. Bernstein, Civil Engineering Research Foundation; Laurence W. Brown, Edison Electric Institute; Lynn Costantini, North American Electric Reliability Council; Debra DeHaney, U.S. Conference of Mayors; Stephen Gehl, Electric Power Research Institute; Bobby R. Gillham, Conoco, Inc.; Miriam Heller, National Science Foundation; Larry Kezele, North American Electric Reliability Council; Fred Mower, University of Maryland; Sam Varnado, U.S. Department of Energy; and Joe Vipperman, American Electric Power Company, Inc.

PANEL ON BEHAVIORAL, SOCIAL, AND INSTITUTIONAL ISSUES

Chaired by STCT committee member Neil Smelser, the Behavioral, Social, and Institutional Panel consisted of 10 members and included scholars from the disciplines of anthropology, demography, economics, history, political science, psychology and sociology. Special areas of expertise of the panel members included the history of Muslim societies, the contemporary Middle East, the politics of the state, revolutionary social movements, deterrence and game theory, the cognitive structure of beliefs, disaster studies, the politics of diplomacy and peace-keeping, and social change. The panel met twice in Washington, D.C., read a variety of materials in the exploding literature on terrorism, and between the meetings exchanged materials and ideas by e-mail.

PANEL ON SYSTEMS ANALYSIS AND SYSTEMS ENGINEERING

Chaired by STCT committee member Vincent Vitto, the Systems Analysis and Systems Engineering Panel consisted of 13 members with areas of expertise in agent-based modeling, ergonomics and human factors, infrastructure modeling and interdependencies, modeling and simulation, operations research, risk modeling, systems analysis, systems dynamics, systems management, systems engineering, and threat analysis. The panel convened three times over a 2-month period and communicated by e-mail. During its meetings, the panel received briefings on systems analysis and systems engineering initiatives within the federal government, including the Department of Defense. Special thanks are due to Frank Dixon, Joint Program Office for Special Technology Countermeasures; Michael Evenson, Defense Threat Reduction Agency; and Miriam Heller, National Science Foundation.

In addition, panel members provided the panel as a whole with briefings on

the following topics: analytic architecture for capabilities-based planning, mission system analysis, and transformation; centrality of the state variable in modeling and its implications for critical infrastructure protection against terrorism; complexity of modeling the interconnectedness and interdependencies of critical infrastructures, as well as interdependencies of the military infrastructures (defense infrastructure sectors) and the civilian infrastructures; decision support as a function of modeling approach; human security consortium initiative; interdependencies between the markets being designed for electric power systems and their impact on the engineering (and vice versa), as well as the idea of hidden failures and cascading events; modeling the interface of social science and engineering; national infrastructure simulation and the analysis center initiative; overarching model for threat assessment; role of governance and nature of decision making; symptoms of governance and decision-making problems; system of systems and federation of systems characterizations; and trade-offs associated with who can decide who decides.

D

Acronyms and Abbreviations

3G	third generation
AFOSR	Air Force Office of Scientific Research
APHIS	Animal and Plant Health Inspection Service
API	American Petroleum Institute
ARO	Army Research Office
ARPA	Advanced Research Projects Agency
ASCE	American Society of Civil Engineers
ASHRAE	American Society of Heating, Refrigeration, and Air Conditioning Engineers
ASTM	American Society for Testing and Materials
ATF	Bureau of Alcohol, Tobacco, and Firearms
ATP	Advanced Technology Program (at NIST)
BW	biological warfare
CBACI	Chemical and Biological Arms Control Institute
CBIRF	Chemical, Biological Incident Response Force
CBO	Congressional Budget Office
CBRNE	chemical, biological, radiological, nuclear, and explosive
CDC	(United States) Centers for Disease Control and Prevention
CFD	computational fluid dynamics
CFR	Code of Federal Regulations
CHIPS	Clearing House Interbank Payments System
CIA	Central Intelligence Agency

C3I	command, control, communications, and information
CRS	Congressional Research Service
CSTB	Computer Science and Telecommunications Board
C-TPAT	Customs-Trade Partnership Against Terrorism
CW	chemical weapons
DARPA	Defense Advanced Research Projects Agency
DDOS	distributed denial-of-service (attack)
DI	deionized
DNA	deoxyribonucleic acid
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DSL	digital subscriber line
DTRA	Defense Threat Reduction Agency
EHV	extra high voltage
EIA	Energy Information Administration
EMP	electromagnetic pulse
EOC	emergency operations center
EOP	Executive Office of the President
EPA	Environmental Protection Agency
EPRI	Electric Power Research Institute
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FFRDC	federally funded research and development center
FOIA	Freedom of Information Act
GIS	geographic information system
GN&C	guidance, navigation, and control
GNP	gross national product
GOCO	government-owned, contractor-operated
GTI	Gas Technology Institute
HACCP	Hazard Analysis and Critical Control Point (an FDA program)
HE	high explosives

HEPA	high-efficiency particulate air (filter)
HEU	highly enriched uranium
HHS	Department of Health and Human Services
HSC	Homeland Security Council
HVAC	heating, ventilation, and air-conditioning
IAEA	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronics Engineers
IMS	ion mobility spectrometer
IND	investigational new drug
IND	improvised nuclear device
IOM	Institute of Medicine
IPP	independent power producers
IRS	Internal Revenue Service
ISO	independent system operator
IT	information technology
IU	intelligent information unit
IW	information warfare
LAN	local area network
LD_{50}	lethal dose at which 50 percent of the exposed subjects die
LDC	local distribution company
LNG	liquefied natural gas
m^2/g	square meters per gram
MANET	mobile ad hoc network
MIT	Massachusetts Institute of Technology
MPC&A	material protection, control, and accounting
MWS	multisensor warning systems
^{14}N	the most common isotope of nitrogen
NARUC	National Association of Regulatory Utility Commissioners
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NDEA	National Defense Education Act
NDMS	National Disaster Medical System
NEHRP	National Earthquake Hazards Reduction Program
NEI	Nuclear Energy Institute
NFPA	National Fire Protection Association
NIAID	National Institute of Allergy and Infectious Diseases
NIH	National Institutes of Health
NIOSH	National Institute for Occupational Safety and Health
NIST	National Institute of Standards and Technology

NNSA	National Nuclear Security Administration
NPC	National Petroleum Council
NPP	nuclear power plant
NQR	nuclear quadrupole resonance
NRC	National Research Council
NSF	National Science Foundation
NSTC	National Science and Technology Council
OHS	Office of Homeland Security
OMB	Office of Management and Budget
ONR	Office of Naval Research
OPCW	Organization for the Prohibition of Chemical Weapons
OSTP	Office of Science and Technology Policy
PAL	permissive action link
PCAST	President's Committee of Advisors on Science and Technology
PCCIP	President's Commission on Critical Infrastructure Protection
PCR	polymerase chain reaction
PDD62	Presidential Decision Directive No. 62
PDD63	Presidential Decision Directive No. 63
picogram	a trillionth (10^{-12}) of a gram
PETN	pentaerythritol tetranitrate, a high explosive
PPE	personal protective equipment
PRA	probabilistic risk assessment
Pu	plutonium
QA	quality analysis
QC	quality control
R&D	research and development
RAM-D	reliability, availability, maintainability, and durability
RDD	radiological dispersal device
RDT&E	research, development, test, and evaluation
RDX	1,3,5-trinitro-1,3,5-triazacyclohexane, a high explosive
RF	radio frequency
RTO	regional transmission operator
S&T	science and technology
SBIR	Small Business Innovation Research
SCADA	supervisory control and data acquisition
SEC	Securities and Exchange Commission
SNM	special nuclear material
SWIFT	Society for Worldwide Interbank Financial Telecommunication

TIC	toxic industrial chemical
TMR	tactical mobile robotics
TNT	2,4,6-trinitrotoluene, a high explosive
TSA	Transportation Security Administration
USCOM	U.S. Conference of Mayors
USDA	U.S. Department of Agriculture
USNRC	U.S. Nuclear Regulatory Commission
VX	O-ethyl, S[2-(diisopropyl amino) ethyl]methylphosphonothiolate, a nerve agent
WHO	World Health Organization
WMD	weapons of mass destruction
WWI	World War I
WWII	World War II
XML	extensible markup language
Y2K	year 2000

Index

A

Advanced Concept Technology Demonstration program in DARPA, 117
Advanced Research Projects Agency (ARPA), 352
Advanced Technology Program (ATP) in NIST, 117, 359
Aerospace Corporation, 345
Afghanistan campaign, 28–29
Agricultural systems. *See* Human and agricultural health systems; Food distribution systems
Aircraft as weapons, 6, 42, 47, 50, 60, 91, 210, 253, 256, 259–260
Air Force Office of Scientific Research (AFOSR), 352
Air Force Research Laboratory (AFRL), 352
Al Qaeda, 26, 28
American Medical Association, 103
American Red Cross, 94, 280
American Society for Microbiology, 68
American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE), 258
American Water Works Association, 250
Ammonium nitrate, 122
Animal and Plant Health Inspection Service (APHIS) in USDA, 77–78, 93
Animal models, 81, 88, 101, 131, 355
Annual Report to Congress on Combating Terrorism, 347, 350, 358n
Anthrax, 65–66, 72, 76, 85, 102, 254, 258, 358
Anthrax attacks, 7, 25, 27, 62, 66, 94–95, 109, 118, 270, 275, 285
Antibiotics, 81–82, 85–87, 88, 99–100, 102
Antitrust regulations, 102, 184, 204, 360, 362–363
Army Corps of Engineers, 252
Army Research Laboratory (ARL), 352
Army Research Office (ARO), 352
Attribution, 28, 113, 146–147, 230–231, 323–324
  bioforensics (microbial forensics), 8, 70, 82–84,
  of nuclear and radiological attacks, 5–6, 59–60
Aum Shinrikyo attack, 111
Authentication, 149–151, 156–157, 329, 361
Aviation and Transportation Security Act, 211, 231
Aviation security, 52, 114, 142, 166, 211, 212, 215, 219–221, 226, 231, 319–320

B

Bayh-Dole Act, 359
Behavioral and social issues. *See* Response of people to terrorism; Human factors

Bin Laden, Osama, 295
Biometrics, 217, 226, 320, 329–330, 361
Bioterrorism, 7-8, 32, 65-67, 84-85, 104, 315-316. *See also* Human and agricultural health systems
BLASTEX software, 255–256
Bomb Data Registry (FBI), 253, 257
Border Patrol, 213n
Bremer Commission, 336–337
Buildings, major and monumental, 252–258. *See also* Cities and fixed infrastructure
Bureau of Alcohol, Tobacco, and Firearms (ATF), 121, 253, 257
Bureau of Reclamation, 252
Bush, George W., 1, 211, 281, 339

C

Catastrophic terrorism, 26–27
Centers for Disease Control and Prevention (CDC), 67–68, 75–77, 79–81, 85, 90, 101–102, 276, 354
Central Intelligence Agency (CIA), 318
Chemical agents. *See also* Toxic chemicals and explosive materials
  approximate toxicity of selected chemical agents, 110
  explosives, 49, 60, 112–113, 247, 257, 263
  explosives detection, 114, 206, 228, 361
  industrial chemicals, 111–112, 121–122, 128, 205, 211, 248
  military chemical weapons, 109–111
  sensors of, 113–117, 321
  treatment of injuries that result from, 129–131
Chemical/Biological Incident Response Force (CBIRF), 129
Chemical Weapons Convention, 110–111
Cities and fixed infrastructure, 16–17, 31, 35, 238–266
  electrical supply interruptions, 252
  emergency operations centers, 239–245
  information technology systems and communications, 252
  major and monumental buildings, 252–258
  stadiums and other places for large public gatherings, 258–261
  transportation and distribution systems, 252
  underground facilities, including tunnels, 262–265
  water supply and wastewater systems, 245–252
Civil liberties. *See* Privacy and civil liberties
Coding issues. *See* Computer code
Cold War, 5, 29, 59, 283, 338, 370
Collaboration, cross-agency, 331–332, 338–339, 350
Command, control, communications, and information (C3I) systems, 11, 146, 148, 158–166. *See also* Communications for first responders
  ad hoc interoperability, 159–160
  communications during an emergency, 160–163, 165–166
Commercial value for counterterrorism technologies and dual-use strategies, 23, 33, 132, 334, 360–362
  in the bioterrorism area, 67–68, 97, 131
  information technology, 149, 361
  sensors, 117, 132, 361
  transportation systems, 220–223, 232, 361
Commission on Aviation Safety and Security in the White House, 219n, 221n, 227n
Committee on Science and Technology for Countering Terrorism, 3, 183n
Communication with the public, 17, 62, 93–94, 162–163, 275–276
Communications for first responders, 2, 11, 137, 144, 146, 158–166, 172, 174, 230, 241, 243, 245, 258, 277
Complex and interdependent systems, 18–19, 31, 35, 287–312. *See also* Systems analysis and systems engineering
  counterterrorism threat modeling, 294–300
  implications for education, 309–310
  infrastructure modeling, 300–305
  modeling challenges for counterterrorism, 305–309
  systems approach to counterterrorism, 288–290
  systems management issues, 290–294
Computer code, improving, 154–155, 367
Computer Emergency Response Team, 145
Congress, 339–340, 342, 345–350, 354, 363
Congressional Budget Office (CBO), 350
Congressional Research Service (CRS), 350, 370
CONWEP software, 255–256

Cooperation between federal, state, and local governments, 22, 38, 92, 127–128, 145, 232, 241–243, 252, 277–278, 333–334, 357–359. *See also* Cross-agency collaboration
Critical Infrastructure Information Security Act, 363n
Cross-agency collaboration, 331–332, 338–339, 350
Crosscutting challenges and technologies, 19–20, 33, 35, 313–334
  autonomous mobile robotic technologies, 325–327. S*ee also* Robotic technologies
  biometrics, 329–330, 361
  controlling access to physical and information systems, 329–330. S*ee also* Authentication
  coordination of crosscutting technologies, 331–332, 338
  human and organizational factors, 330–331, 336. *See also* Human factors
  integrated data management, 317–320. *See also* Data mining; Information fusion
  SCADA systems, 327–328. *See also* Supervisory control and data acquisition systems
  sensors and sensor networks, 320–325. *See also* Sensors and sensor networks
  systems analysis and modeling, 315–317. *See also* Systems analysis and systems engineering; Modeling and simulation
Cultural memory, normalization and, 284–286
Customs inspections, 56, 216, 319. *See also* U.S. Customs Service
Customs-Trade Partnership Against Terrorism (C-TPAT), 219n, 319
Cyberattacks, 136–144. *See also* Information technology
Cybersecurity, 10–12, 147–157, 361, 367. *See also* Information technology
  for energy systems, 182, 187–188, 190, 203–204, 208. *See also* Supervisory control and data acquisition systems

D

Data integration. *See* Data mining; Information fusion; Standards for data integration and database interoperability
Data management. *See* Data mining; Information fusion
Data mining, 2, 117, 167–168, 170–171, 217, 225–226, 318–320. *See also* Information fusion
Decision-making support, 80, 128–129, 162, 165, 230, 251, 291–293, 296–298, 316, 343–346
Decontamination, 2
  of chemical agents, 9–10, 115, 118–120, 130
  of human and agricultural systems, 8, 78, 94–96
  of IT systems, 153–154
  of radiological material, 51, 58–59
  robotics for, 120, 230, 326
  of water supplies, 9, 125–126
Defense Advanced Research Projects Agency (DARPA), 11, 116, 120, 168, 287, 309, 325–326, 338, 352–353, 355
Defense Modeling and Simulation Office in DOD, 287, 302
Defense Threat Reduction Agency (DTRA), 5–6, 57, 60, 63, 93, 129, 309, 316, 353
Denial-of-service attacks, 137, 149n, 153
Department of Commerce (DOC), 122, 348–349, 350
Department of Defense (DOD), 52–53, 57, 63, 68, 76, 80, 90, 92, 96, 145, 194, 230, 242, 287, 331, 350, 353–355
Department of Energy (DOE), 11–13, 45n, 52–54, 57, 63–64, 68, 90, 116, 188, 190–195, 207, 313, 320, 331, 338, 348–350, 352, 355, 358n
Department of Health and Human Services (HHS), 8, 75, 91–92, 94, 96, 102, 355, 358n
Department of Homeland Security, 21–22, 68, 339, 342, 345, 349
Department of the Interior, 138
Department of Justice (DOJ), 242, 245, 250
Department of State, 26n, 52, 54, 193, 255
Department of Transportation (DOT), 14–15, 122, 200, 213n, 232, 265, 351, 358
Detection, 28, 166, 228–229, 314, 330. *See also* Sensors and sensor networks
  use of information technology in detecting attacks, 146–147, 149–151, 166, 187, 207
Deutch Commission Report, 349n

Dirty bombs. *See* Radiological dispersion devices
Distributed denial-of-service (DDOS) attacks, 137, 149n, 153
DNA (deoxyribonucleic acid), 74, 83, 87, 98, 322
Domain Name System (DNS), 138
Dual-use strategies. *See* Commercial value for counterterrorism technologies

E

Economic aspects of recovery, 282–284
Electric power, 180–195
  extra-high-voltage transformers, replacements for, 188–189
  intelligent, adaptive power grid, 192–193, 366–367
  implementation of existing technology for mitigating vulnerabilities, 183–188
  interruptions in, 252
  interdependence with other systems, 301–302
  recovery from outages, 185–186, 191–192
  representative vulnerabilities, 180–183
  research and development priorities and strategies, 188–195
Electric Power Research Institute (EPRI), 12, 60, 187, 190–195, 198
Electromagnetic pulse (EMP) attacks, 182, 190
Emergency medical response, 90–93, 129–131, 240–241
Emergency operations centers (EOCs), 16–17, 239–245
  communications and information technology, 144, 158–159
  recommended requirements list, 241
  vulnerability of EOC sites and facilities, 241–242, 243
Emergency response. *See* First responders
Energy systems, 12–13, 31, 34, 177–209
  cybersecurity, 182, 187–188, 190, 203–204, 208. *See also* Supervisory control and data acquisition systems
  electric power, 180–195
  oil and natural gas, 196–208
Environmental Protection Agency (EPA), 9, 68, 90, 96, 112, 121, 126–128, 213n, 248, 250, 252, 287, 358n, 360
Executive Office of the President (EOP), 347–349
Exercises, 28n, 36, 59, 127–128, 130, 159, 344, 354. *See also* Training
Explosives, 49, 60, 112–113, 247, 257, 263
  detection of, 114, 206, 228, 361
Extra-high-voltage (EHV) transformers, 13, 188–189

F

Federal Aviation Administration (FAA), 14, 52, 211, 213n, 220, 226n, 229, 303
Federal Bureau of Investigation (FBI), 58, 93, 121, 127, 318, 355
Federal Communications Commission (FCC), 245
Federal Emergency Management Agency (FEMA), 17–18, 59, 62, 92, 121, 127, 129–130, 233, 241–244, 276, 350, 354, 357, 358n
Federal Energy Regulatory Commission (FERC), 185–187, 194
Federal government's program of science and technology for countering terrorism, 21–22, 35, 335–356
  Congressional capabilities for supporting, 349–350
  current situation, 338–339
  essential partners in, 22–24, 35, 357–371. *See also* Industry in partnership with government; States and cities in partnership with government; Universities in partnership with government
  need for analytical capabilities to support decisions about, 343–346
  need for coordination, 338–348
  role of the federal agencies, 350–355
  roles of OHS, OSTP, and OMB, 340–348
Federal Highway Administration, 14, 235n
Federally funded research and development centers (FFRDCs), 345. *See also* Homeland Security Institute
Federal Radiological Emergency Response Plan, 5, 58–59
Federal Response Plan, 94
Filters, 2, 10, 89–90, 118–120, 126, 247, 254–255, 258, 260, 361
Financial systems, 108, 135, 139, 287

First responders, 33, 127–129, 145–146, 158–166, 241–245, 276–278, 354, 357. *See also* Communications for first responders
Food and Drug Administration (FDA), 8–9, 88, 100–101, 123–125
Food distribution systems, 77–79, 93, 122–124, 133–134, 354, 361. *See also* Human and agricultural health systems
Foot-and-mouth disease (FMD), 77, 85, 95
Forensics. *See* Attribution
Freedom of Information Act (FOIA), 184, 204
Funding and costs, 37–38, 186–187, 284, 347–348, 357, 359

G

Gas systems. *See* Natural gas systems
General Accounting Office (GAO), 66, 340n
General principals and strategies for using science and technology to counter terrorism, 4, 33
Gilmore Commission, 294, 336, 343
Global Emerging Infectious Diseases program in DOD, 75
Global Public Health Information Network, 75
Government-owned, contractor-operated (GOCO) facilities, 100
Guidance, navigation, and control (GN&C) systems, 326–327

H

Hart/Rudman Commission, 336–337, 347n, 349n, 363n
Hazard Analysis and Critical Control Point (HACCP) technology in FDA, 9, 123
Hazardous chemicals. *See* Toxic chemicals and explosive materials
HAZMAT (hazardous materials) teams, 127–128
Health Effects Institute, 360
Health systems. *See* Human and agricultural health systems
Heating, ventilation, and air-conditioning (HVAC) systems, 16, 89, 254–255, 257, 259, 261
High-efficiency particulate air (HEPA) filters, 89, 118, 258
Highly enriched uranium (HEU), 39–40, 49–50, 55, 57, 322–323
Homeland Security Council (HSC), 342, 346, 348
Homeland Security Institute, 21, 236, 242, 244, 293, 314, 344–346
Human and agricultural health systems, 7–8, 31, 34, 65–106, 365. *See also* Food distribution systems
  antimicrobials and antivirals, 85–87. *See also* Antibiotics
  bioterrorism and biological threats, 7–8, 32, 65–67, 84–85, 104, 315–316
  communicating risks and responses to the public, 93–94
  decontamination protocols, 94–96. *See also* Decontamination
  defining whether infectious agents and diseases are bioterrorist threats, 84–85
  human resources needed, 80, 96–97
  identification of biological agents in the environment, 71–73
  Internet resources on bioterrorism, 104
  involving the S&T and public health communities in intelligence and prevention, 69–71
  microbial forensics and analysis of trace evidence, 82–84
  personal protective equipment, 89–90. *See also* Protective equipment for individuals
  regulatory reform for drug development, 100–102
  response and recovery, 79–80, 90–93
  standards and standardization, 97–98. *See also* Standards
  surveillance and diagnosis of infection and disease, 73–79. *See also* Surveillance
  treatment protocols, 94, 129–131
  understanding the effects of biological weapons, 80–82
  vaccine development, 87–89, 98–100. *See also* Vaccines
Human factors, 15, 33, 147, 157, 224, 226, 234, 314, 330–331, 366
Human resources, 80, 96–97, 174, 368–369
HVAC (heating, ventilation, and air conditioning). *See* Ventilation systems

I

Immediate applications for existing technologies, 2

Immigration and Naturalization Service (INS), 213n, 233, 350
Improvised nuclear devices (INDs), 39, 49, 51–52, 55, 57, 322
  fabricated from stolen or diverted special nuclear material, 40–41, 44–45
Indemnification. *See* Liability and indemnification
Independent system operators (ISOs) of electric power systems, 185, 188, 195
Individual rights. *See* Privacy and civil liberties
Industrial chemicals, 111–112, 121–122, 128, 205, 211, 248
Industry in partnership with government, 359–364
  antitrust exemptions, 362–363
  commercial value for counterterrorism technologies, 360–362. *See also* Commercial value for counterterrorism technologies and dual-use strategies
  government procurement and acquisition rules, 363–364
  indemnification, 362
Infectious Diseases Society of America, 68
Influenza, 65, 76, 84, 94
Information fusion, 11–12, 136, 146–149, 166–170, 173, 318, 366. *See also* Data mining; Standards for data integration and database interoperability
Information technology (IT), 10–12, 31, 34, 135–176, 355, 367. *See also* Cybersecurity; Cyberattacks
  defensive strategy in protecting, 150
  implementation, 172–175
  information and network security, 147–157
  information fusion, 166–170. *See also* Information fusion
  IT and C3I for emergency response, 158–166. *See also* Communications for first responders
  long-term recommendations, 146–170
  planning for the future, 171
  privacy and confidentiality, 170–171
  research in, 146–170
  short-term recommendations, 144–146
  taxonomy of priorities, 148–149
  threats associated with IT infrastructure, 136–144
Infrastructure modeling, 300–305, 315–317, 338–339, 344
  infrastructure interdependencies, 13, 19, 300, 303, 315–317, 338–339
  energy systems, 184–185, 191, 194, 206–207
Institute for Defense Analyses, 345
Intelligence gathering, 20, 29, 52, 70–71, 136, 148, 157, 166, 169, 267, 294, 299, 318, 325, 366
Intelligent information units (IUs), attaching to railcars, 264–265
Interagency Task Force on Antimicrobial Resistance, 86
Interdependent systems. *See* Complex and interdependent systems
International Atomic Energy Agency (IAEA), 52, 54
International Civil Aviation Organization, 233
International Maritime Organization, 233
International Organization for Standardization, 303
Internet, 135, 137–143, 146, 150, 161, 164, 171, 203, 302
Investigational new drug (IND) status, 100, 102

J

Joint Services Chemical and Biological Defense Program, 353

L

LD_{50} (lethal dose at which 50 percent of the exposed subjects die), 81, 126
Liability and indemnification, 88, 99, 101–102, 184, 204, 249, 360, 362
Liquefied natural gas (LNG) facilities, 196, 200–201
Local distribution companies (LDCs) for natural gas distribution, 198–200

M

Marsh Commission, 336–337
Materials Protection, Control, and Accounting (MPC&A) program in Russia, 53–54
McCarthyism, 282
Media, the, 62, 275–276
Medical Research Institute of Infectious Diseases, U.S. Army, 353
Metadata, 19, 303–305. *See also* Standards for data integration and database interoperability

Metropolitan Medical Response System, 91–92
Microbial forensics. *See* Attribution
MITRE Corporation, 345
Modeling and simulation, 19–20, 287–288, 305–309, 315–318, 366. *See also* Infrastructure modeling; Risk modeling and risk assessment
of disease spread, 75, 79–81, 315–316, 322
for exercises, training, and decision making, 17, 21, 80, 92, 95, 242–244, 251, 316, 344
of specific systems, 129, 251, 255, 257, 273, 285, 315, 328
Monumental buildings, 252–258
Murrah Federal Building attack, 112, 122, 253, 259, 271

N

National Aeronautics and Space Administration (NASA), 287, 331, 333, 352, 355
National Association of Regulatory Utility Commissioners (NARUC), 186–187, 195
National Defense Education Act (NDEA), 368
National Disaster Medical System (NDMS), 92
National Fire Protection Association (NFPA), 16, 257–258, 358
National Guard, 127–128, 145, 280
National Infrastructure Simulation and Analysis Center, 191, 193, 207
National Institute of Allergy and Infectious Diseases (NIAID), 68, 76, 97
National Institute of Standards and Technology (NIST), 11, 16, 98, 120, 126, 145, 257–258, 260, 344, 348, 350, 352
National Institutes of Health (NIH), 68, 76, 80–81, 97–98, 131, 234, 244, 350, 352
National Medical Response Teams for Weapons of Mass Destruction, 91
National Nuclear Security Administration (NNSA), 57, 62–64, 348
National Science and Technology Council (NSTC), 22, 332, 342, 347
National Science Foundation (NSF), 11, 18, 116, 120, 168, 234, 304, 308–309, 331, 333, 338, 350, 352, 355, 369
National Security Agency (NSA), 242, 318
Natural gas systems, 196–201, 204–208
implementation of existing technologies for mitigating vulnerabilities, 204–205
liquefied natural gas, 200–201
physical vulnerabilities of the natural gas infrastructure, 197
pipelines, 198–200
research and development priorities and strategies, 205–208
Naval Research Laboratory (NRL), 352
Nerve agents, 108–111, 115, 129, 131
Network security, 147–157, 172–173
authentication, detection, and identification, 149–151
containment, 152–153
principles of defensive strategy, 150
recovery, 153–154
research issues, 154–157
Normalization and cultural memory, 284–286
North American Electric Reliability Council, 195
Nuclear and radiological threats, 4, 5–6, 31, 34, 39–64
homeland security challenges, 49–51
improvised nuclear devices (INDs), 40–41, 44–45, 49–50, 51–57
nuclear and radiological threat matrix, 39–49
nuclear power plants (NPPs), 6, 41–44, 46, 50–51, 60, 182
nuclear weapons and weapons components, 39–40, 42–43, 49–50, 51–57
radiological dispersion devices, 48, 49, 51, 58, 61–62
reducing vulnerabilities, 51–62
Nuclear Energy Institute (NEI), 42
Nuclear Posture Review, 53
Nuclear quadrupole resonance (NQR) spectrometry, 114
Nuclear Regulatory Commission. *See* U.S. Nuclear Regulatory Commission

O

Office of Emergency Preparedness, 92
Office of Homeland Security (OHS), 17, 21–22, 62–64, 94, 121, 145, 186, 188–189, 195, 211, 241–242, 245, 250, 258, 265, 290, 293–294, 319, 339–347, 350, 354, 358n, 360, 371
Office of Management and Budget (OMB), 145, 332, 340–343, 347–350, 358n
Office of Naval Research (ONR), 326, 352

Office of Science and Technology Policy (OSTP), 22, 242, 340–342, 344, 346–350, 359, 363, 371. *See also* President's Science Advisor
Oil and refined products, 201–208
  command, control, and communications, 203
  implementation of existing technologies for mitigating vulnerabilities, 204–205
  oil system vulnerabilities, 202
  pumping stations for crude oil and refined products, 203
  refineries, 201–202
  research and development priorities and strategies, 205–208
Oklahoma City attack, 112, 122, 253, 259, 271
Organization for the Prohibition of Chemical Weapons (OPCW), 110

P

Panic and fear, 61, 143, 259, 261, 274-275
Pathogens, 2, 84–85, 365. *See also* Human and agricultural health systems
Pentagon attack, 25, 255, 283
Political aspects of recovery from a terrorist event, 281–282
President's Commission on Critical Infrastructure Protection (PCCIP), 141, 193, 242, 337, 355
President's Council of Advisors on Science and Technology (PCAST), 342, 346, 363
President's Science Advisor, 62–64, 337, 341n, 347n
Prioritization, 3, 33, 36, 293, 294, 299, 314, 335, 337, 339, 343–346
  of counterterrorism efforts for transportation systems, 224
  of factors in security of energy systems, 183
  by individual social units (cities, etc.), 271
  of nuclear counterterrorism activities, 63–64
  a taxonomy of priorities for IT research, 148–149
Privacy and civil liberties, 15, 18, 29, 170–171, 175, 183, 226, 276, 281, 320, 329, 330–331, 361
Probabilistic risk assessment (PRA) approach, 257
Project Air Force, 345
Protective equipment for individuals, including first responders, 2, 22, 59, 89–90, 98, 120, 127–128, 276, 354,
Public health systems, 31, 66–67, 74–77, 90–93, 94, 102–103, 320. *See also* Human and agricultural health systems

Q

Quality analysis/quality control (QA/QC) programs, 123

R

Radiological dispersion devices (RDDs), 48, 49, 51, 58, 61–62. *See also* Nuclear and radiological threats
RAND Corporation, 345
"Reachback" capabilities, 129
Recovery, 28. *See also* Decontamination
  economic aspects of, 282–284
  from a catastrophic energy system shutdown, 186, 205
  in network security, 153–154
  political aspects of, 281–282
  sensors and sensor networks in, 323
  of transportation services, 230
Regional transmission operators (RTOs), 185, 188, 195
Regulations and rules, possible adjustments to, 359–364
  antitrust regulations, 102, 184, 204, 360, 362–363
  for information technology products, 145, 173
  pharmaceutical-related, 100–102, 124–125, 131, 362–363
  for specific systems, 122, 186, 227
  tightening of nuclear and radiological regulations, 52, 61
Response of people to terrorism, 17–18, 31, 35, 267–286
  anticipation and preparedness, 271–272
  goals of different types of terrorist attacks, 268
  institutional, group, and political vulnerability, 268–270
  long-term recovery processes, 281–286
  occurrence of attack, 274–279

short-term recovery processes, 279–280
universality of human responses, 270–271
warnings, 273, 277, 280
Response to terrorism, phases of, 27–28
Ridge, Tom, 277, 319, 341n, 342, 358n
Risk modeling and risk assessment, 95, 250, 257, 290, 294–300, 306–308, 317
Robotic technologies, 20, 72, 95, 120–121, 164, 206, 230, 244, 314, 325–327, 333, 367
Russian nuclear materials and weapons, 5, 40–41, 42–45, 49–50, 52–54

S

Sandia National Laboratories, 42, 60
Sarin gas attack in Japan, 111, 118
SCADA systems. *See* Supervisory control and data acquisition systems
Sensors and sensor networks, 2, 314, 320–325, 338, 350, 361, 365. *See also* Detection
deployment of, 19, 55–57, 117, 225, 323–325, 365
for detecting and characterizing biological and chemical agents and explosives, 7, 9, 71–73, 77, 98, 113–117, 228–230, 250–251, 260–261, 321–322, 324, 361
for detecting nuclear and radiological materials, 51, 55–57, 322–323, 354, 361
for first responders, 16, 163, 244
intrusion detection and monitoring, 189, 206–207
standards for and testing of, 10, 98, 117, 324–325
for water systems, 126, 250–251
September 11 attacks, 7, 16, 20, 25, 58, 60, 64, 102, 121, 161, 211, 219–220, 224, 231, 235, 253, 260, 271, 279, 282, 285, 288, 335
Shipping containers, 2, 14, 216–218, 361
Simulation. *See* Modeling and simulation
Small Business Innovation Research (SBIR) programs, 117, 359
Smallpox, 65, 84–86, 101
Special nuclear material (SNM), 39–41, 49–50
detection and interdiction of, 55–57, 322
need to inventory, 54
Spokespersons. *See* Trusted spokespersons
Stadiums and other places for large public gatherings, 258–261
Standards, 21, 22, 337, 339, 344, 348, 358, 359–360, 364
for biological detection and diagnosis, 7, 71–72, 76, 97–98
for buildings, 2, 16, 255–258
for communications for first responders, 2, 158–159, 245
for data integration and database interoperability, 19, 20, 303–305, 314, 320
for decontamination, 2, 10, 96
for emergency response protocols and equipment, 8, 22, 89, 120, 241, 244
for energy systems' control systems, 187, 204, 328
for filters, 2, 10, 89–90, 258
for sensors, 10, 325
for transportation systems and related equipment, 217, 232–233, 235
States and cities in partnership with government, 357–359. *See also* Cooperation between federal, state, and local governments
Stolen nuclear weapons and improvised nuclear devices. *See also* Nuclear and radiological threats
detection and interdiction, 55–57
protection, control, and accounting for, 52–55
Strategic research and planning for the Transportation Security Administration, 231–235
Supervisory control and data acquisition (SCADA) systems, 13, 19–20, 33, 122, 135, 139–141, 178, 194, 208, 327–328
attacks on, 139–140, 199
strengthening, 187, 190, 314, 361
vulnerabilities of, 141, 152, 203, 293
Surgeon General, 62, 276
Surveillance, 2, 27
biological, 7, 68, 73–79, 97–98, 321–322, 354
physical, 13, 120–121, 189, 207, 222, 263, 323, 325–326, 331
Systems analysis and systems engineering, 19, 31, 36, 233, 287, 293–294, 308–310, 314–317, 344, 351, 366. *See also* Complex and interdependent systems
Systems expertise for the OHS, 293–294, 343–346
Systems management issues, 290–294

T

Technical Support Working Group, 359
Telecommunications, 138–139, 143, 150, 302, 316, 361
Terrorism defined, 26–27n. *See also* Catastrophic terrorism
Threats associated with IT infrastructure, 136–144. *See also* Cyberattacks
  disproportionate impacts, 141–142
  IT attack as an amplifier of a physical attack, 137
  likelihood and impact, 142–144
  possibilities for attack using IT, 137–140
  security vulnerabilities of SCADA systems, 141. *See also* Supervisory control and data acquisition systems
Toxic chemicals and explosive materials, 8–10, 31, 34, 107–134. *See also* Chemical agents; Industrial chemicals
  chemicals as weapons, 108–113
  mitigating vulnerabilities, 113–127
  responding to attacks, 127–131
Training, 79, 103, 130, 272, 316. *See also* Exercises
  for first responders, 62, 127–128, 242–244, 300, 354
Transportation Security Administration (TSA) in DOT, 14–15, 211, 231–235, 319, 350–351, 354
Transportation systems, 13–15, 31, 35, 210–237
  aviation systems. *See* Aircraft as weapons; Aviation security
  common characteristics of, 212–214
  considerations for security strategies for, 214–223
  disruption of, 139, 196, 279, 315
  human factors, 15, 224, 226, 229, 232, 234
  industrial chemicals, transport of, 112, 121–122
  layered security systems, 214–220
  managing research and development activities, 224, 233–235, 351, 354, 358
  railcar and container contents, 263–265
  research and technology needs, 223–231
  shipping container threat scenario and security strategy, 216–218, 361
  strategic research and planning advice for the TSA, 231–235
Trusted spokespersons, 2, 6, 17, 62, 276
Tunnels. *See* Underground facilities
Tylenol-poisoning incident, 124

U

Unabomber case, 271
Underground facilities, including tunnels, 113, 230, 262–265
Undersecretary for Technology in Department of Homeland Security, 22, 342–343, 346
Underwriters Laboratories, 16
Universities in partnership with government, 364–371
  balancing security needs with the requirements for research, 370–371
  critical long-term research needs, 365–367
  investing in research in a variety of disciplines, 332–333, 369–370
  sustaining the nation's scientific and engineering talent base, 368–369
Urgent research opportunities, 2
U.S. Army, 45n, 114, 188
U.S. Bureau of Reclamation, 246
U.S. Coast Guard, 96, 121, 233, 343, 350
U.S. Conference of Mayors (USCOM), 238–239, 262, 265, 358
U.S. Customs Service, 213n, 216, 219, 233, 319, 350
U.S. Department of Agriculture (USDA), 68, 76–79, 93, 96, 128, 213n, 354
U.S. Nuclear Regulatory Commission (USNRC), 6, 41–42, 44n, 47–48, 50, 54, 60, 63, 182
U.S. Postal Service, 109, 214
USS *Cole* incident, 271

V

Vaccines, 8, 80–82, 85–89, 97, 98–101, 355, 362–363
Ventilation systems, 2, 10, 16, 89–90, 113, 119, 230, 243, 254–255, 257–258, 260–261, 263–264, 361
Veterans Administration (VA), 92
Volpe National Transportation Systems Center in DOT, 15, 233

W

Warnings, effectiveness of, 17, 162–163, 273, 277, 280
Water supply and wastewater systems, 125–127, 245–252

Weapons of mass destruction (WMD), 1, 31, 63, 91, 93–94, 128, 321. *See also* Bioterrorism; Chemical agents; Nuclear and radiological threats; Catastrophic terrorism
West Nile virus outbreak, 66
World Customs Organization, 233
World Health Organization (WHO), 75
World Organisation for Animal Health, 77
World Trade Center (WTC) attacks, 16, 25, 236, 241, 253–254, 258, 271, 283, 285, 323
World Wide Web, 141