Countering Bioterrorism: The Role of Science and Technology

Panel on Biological Issues, Committee on Science and Technology for Countering Terrorism, National Research Council

ISBN: 0-309-50350-7, 106 pages, 6 x 9, (2002)

COUNTERING BIOTERRORISM

THE ROLE OF SCIENCE AND TECHNOLOGY

Panel on Biological Issues

Committee on Science and Technology for Countering Terrorism

INSTITUTE OF MEDICINE
NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

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

THE NATIONAL ACADEMIES PRESS • 500 FIFTH STREET, N.W. • Washington, DC 20001

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 by institutional funds.

International Standard Book Number 0-309-08607-8

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; call (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

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 chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

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

Liaisons from the Parent Committee to the Panel

MARGARET A. HAMBURG, Nuclear Threat Initiative
P. ROY VAGELOS, Merck & Co., Inc. (retired)

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
ALDEN B. CHANG, Administrative Assistant, Board on Health Sciences Policy
JUDY ESTEP, Senior Program Assistant, Board on Health Promotion and Disease Prevention

Consultant

KATHI E. HANNA, Writer

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

Preface

The September 11, 2001, attacks galvanized the nation to strengthen its counterterrorism defenses. Immediately following the attacks, the presidents of the National Academy of Sciences, National Academy of Engineering, and Institute of Medicine wrote to President Bush offering the advice of the National Academies on how best to harness the country's science and technology capacity to meet critical security and antiterrorism needs.

In December 2001, the National Academies appointed a committee of 24 of the country's leading scientific, engineering, medical, and public policy experts to offer counsel on an integrated science and technology plan for combating terrorism. To supplement the knowledge of its members, the committee convened eight panels with expertise in specific topic areas, from the chemical and biological disciplines to the domains of energy, information technology, and transportation. Barry Bloom and Joshua Lederberg, both members of the main committee, co-chaired the Panel on Biological Issues, which comprised 22 experts 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 main committee's report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, was released on June 25, 2002. The committee recommends a strategy whereby the nation's scientific and engineering capacity can be strengthened and brought to bear in the fight against terrorism. *Making the Nation Safer* synthesizes the contributions of the eight expert

panels into chapters, each containing specific research and policy recommendations. The contribution of the Panel on Biological Issues (Chapter 3 of *Making the Nation Safer*) is reprinted in this report to provide a focused report on the scientific and technological measures needed to counter bioterrorism. The executive summary of the main committee's report is reprinted in Appendix A of this report.

The Panel on Biological Issues met three times over a 5-month period with extensive interactions by email and conference calls. The panel wishes to thank the following individuals who provided briefings to the panel: William Winkenwerder, Department of Defense; Kevin Tonat, Department of Health and Human Services; D.A. Henderson, Department of Health and Human Services; Anthony Fauci, National Institute of Allergy and Infectious Diseases; Kathryn Zoon, Food and Drug Administration; David Lipman, National Center for Biotechnology Information; Chuck Ludlum, Office of Senator Joseph Lieberman; and William Dallas Jones, California Office of Emergency Services.

The panel's contribution was reviewed as part of the main committee's report 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 its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process.

The full listing of the reviewers of the main committee's report is provided in that report. Several of those reviewers were selected because of their expertise relevant to the biological sciences and bioterrorism. Special appreciation is expressed to the following reviewers: Steven M. Block, Stanford University; Floyd E. Bloom, The Scripps Research Institute; Stanley Falkow, Stanford University; Thomas J. Kelly, Sloan-Kettering Institute; Harley W. Moon, Iowa State University; Lucy Shapiro, Stanford University; Harold E. Varmus, Memorial Sloan-Kettering Cancer Center. Although these individuals provided many constructive comments and suggestions, they were not asked to endorse findings and conclusions, nor did they see the final document before its release.

The review was overseen by R. Stephen Berry, James Franck Distinguished Service Professor Emeritus, University of Chicago, and Gerald P. Dinneen, Retired Vice President of Science and Technology, Honeywell Inc. Appointed by the National Research Council, they were responsible for making certain that an independent examination of the report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for content rests entirely with the authors and the institution.

Andrew Pope, Jennifer Kuzma, and Cathy Liverman managed the panel's work. Kathi Hanna, a consultant to the committee, summarized the panel's deliberations into a draft of the report. Judy Estep worked on the details of this publication. Special thanks go to Alden Chang for his work in support of the main report.

Contents

Executive Summary

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.

INTELLIGENCE, DETECTION, SURVEILLANCE, AND DIAGNOSIS

Increased awareness in the science and technology (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.

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.

Recommendation 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.

Recommendation 2: Federal agencies should work cooperatively and in collaboration with industry to develop and evaluate rapid, sensitive, and specific early-detection technologies.

Recommendation 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.

Recommendation 4: Use knowledge of complex biological patterns and high-throughput laboratory automation to classify and diagnose infections in patients in primary care settings.

Recommendation 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.

PREVENTION, RESPONSE, AND RECOVERY

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

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 research 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 14: Develop methods and standards for decontamination. Develop standards for levels of decontamination and certification of products to ensure safety.

POLICY AND IMPLEMENTATION

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.

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 this report, are offered in that spirit.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation: 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 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.

CONCLUDING REMARKS

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 would be 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 report 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.

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.

1

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 REPORT

This report was published as Chapter 3 of the National Academies' report, *Making the National Safer: The Role of Science and Technology in Countering Terrorism* (see Appendix A, Executive Summary of the full report). It is published here as a stand-alone report to focus on measures to counter bioterrorism.

This report is organized into three chapters: (1) intelligence, surveillance,

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

detection, and diagnosis; (2) prevention, response, and recovery; and (3) policy and implementation followed by concluding remarks. Each chapter 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 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 report 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 report 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.

2

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 2.1).

Recommendation 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, espe-

BOX 2.1
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.

cially 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 16 and surrounding discussions). Cen-

tralized 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 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., com-

bining 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 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 training 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: 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 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 suc-

cessfully 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 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.

[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>.

3

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.

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 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]

[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>.

Recommendation 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, comprehensive, 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 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, particularly 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

[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>.

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 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; 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 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 equipment; 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 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 agri-

culture 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 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. 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 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 possible 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 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.

4

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 report, 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 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 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, however, it is currently difficult to find targeted funding sources and mechanisms.

Recommendation 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 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 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 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.

---

[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>

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.

5

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.

BOX 5.1
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>

The reader is referred to Box 5.1 for Web sites with additional information on bioterrorism.

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.

Appendix A

Executive Summary
Making the Nation Safer: The Role of Science and Technology in Countering Terrorism

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 13)

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.

Appendix B

Panel and Staff Biographies

Co-Chair

BARRY BLOOM, Ph.D., 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 M.A. from Harvard University, and his Ph.D. from the Rockefeller University. 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 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. Dr. Bloom is a member of the Institute of Medicine, the American Academy of Arts and Sciences, and the National Academy of Sciences.

Co-Chair

JOSHUA LEDERBERG, Ph.D., is a Sackler Foundation Scholar at the Rockefeller University, New York. His lifelong research, for which he received the Nobel Prize in 1958, has been in genetic structure and function in microorganisms. He has a keen interest in international health and was co-chair of the

previous Institute of Medicine study (1990–1992) on Emerging Infections. He has been a member of the National Academy of Sciences since 1957 and is a charter member of the Institute of Medicine. He is currently a member of other NRC panels, the National Research Council Committee on Biological Threats to Agricultural Plants and Animals, the National Academy of Science Committee on International Security and Arms Control, the Defense Science Board, and the Defense Threat Reduction Agency's Threat Reduction Advisory Committee.

RONALD ATLAS, Ph.D., is a professor of biology and graduate dean at the University of Louisville. He received a B.S. degree from the State University of New York at Stony Brook in 1968, an M.S. from Rutgers University in 1970, and a Ph.D. from Rutgers University in 1972. He then served for a year as a National Research Council Research Associate at the Jet Propulsion Laboratory. He is a member of the American Academy of Microbiology and was the recipient of the American Society for Microbiology award in Applied and Environmental Sciences.

RUTH BERKELMAN, M.D., is currently a professor of epidemiology and international health at the Rollins School of Public Health, Emory University. A former Assistant Surgeon General, she has served as a Senior Adviser to the Director, Centers for Disease Control and Prevention (CDC) and as deputy director of the National Center for Infectious Diseases. She led CDC's efforts to respond to the threat of emerging infectious diseases, and is currently a member of the American Society of Microbiology's Policy and Scientific Affairs Board. She has also been active with the Infectious Diseases Society of America, and the American Epidemiological Society. A graduate of Harvard Medical School, she is board certified in internal medicine and pediatrics. She serves on the Board of Trustees at Princeton University.

GAIL CASSELL, Ph.D., is Vice President of Infectious Disease Research, Drug Discovery Research & Clinical Investigation, Eli Lilly and Company, Lily Corporate Center. She has received a number of awards for her research in infectious diseases and is a recent past President of the American Society of Microbiology. She has been active in national and international policy deliberations, including those of NIH and the U.S.-Japan Cooperative Medical Science Program. She was also a member of the International Science and Technology Center Science Advisory Committee and a member of the steering committee of the U.S.-Japan Cooperative Medical Science Program. She is the recent chair of the Board of Scientific Counselors of the National Center for Infectious Diseases of the Centers for Disease Control and Prevention (CDC) and a past member of the NIAID, NIH Advisory Council, and the NIH Director's Advisory Committee.

THOMAS CECH, Ph.D., is President of the Howard Hughes Medical Institute. He is also a Distinguished Professor at the University of Colorado, Boulder. He received his B.A. degree in chemistry from Grinnell College and his Ph.D. degree in chemistry from the University of California, Berkeley. His postdoctoral work in biology was conducted at the Massachusetts Institute of Technology. He is a member of the National Academy of Science and of the Institute of Medicine. Among the many honors he has received are the Lasker Award, the National Medal of Science, and the 1989 Nobel Prize in chemistry.

DAVID FRANZ, D.V.M., Ph.D., is currently Vice President of Chemical & Biological Defense Division at Southern Research Institute. He has served in the U.S. Army Medical Research and Materiel Command for 23 of his 27 years on active duty. Dr. Franz has served as both Deputy Commander and then Commander of the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) and as Deputy Commander of the U.S. Army Medical Research and Materiel Command. Dr. Franz served as Chief Inspector on three United Nations Special Commission biological warfare inspection missions to Iraq, and as technical advisor on long-term monitoring. He also served as a member of the first two US/UK teams that visited Russia in support of the Trilateral Joint Statement on Biological Weapons, and as a member of the Trilateral Experts' Committee for biological weapons negotiations. Dr. Franz was Technical Editor for the Textbook of Military Medicine on Chemical and Biological Defense released in 1997. He has been an invited speaker at many nationally and internationally recognized organizations. Dr. Franz currently serves on the National Research Council's Committee on Biological Threats to Agricultural Plants and Animals. Dr. Franz holds a D.V.M. from Kansas State University and a Ph.D. in Physiology from Baylor College of Medicine.

CLAIRE FRASER, Ph.D., is the President of the Institute for Genomic Research. She served previously as the Director of the Department of Microbial Genomics and Vice-President for Research. As leader of the teams that sequenced the genomes of several microbial organisms, Dr. Fraser has helped initiate the era of comparative genomics. Her research interests include whole genome sequence analysis of microbial genomes and the use of genomic-based approaches to elucidate differences in gene expression. She earned her B.S. from Rensselear Polytechnic Institute and her Ph.D. from The State University of New York at Buffalo.

DAVID GALAS, Ph.D., is Vice President, Chief Academic Officer, and Norris Professor of Applied Life Science at Keck Graduate Institute of Applied Life Sciences (KGI), Claremont, California. Before coming to help found and develop KGI, a new research and educational institution in the applied life sciences, Dr.

Galas served as president and chief scientific officer of Seattle-based Chiroscience R&D Inc., a genomics and drug discovery company. This company was formed through the acquisition of Darwin Molecular Corporation, which Dr. Galas helped start in 1993, and he served as vice president of research and development. He received his Ph.D. in physics from the University of California, Davis-Livermore. He received his undergraduate degree in physics from the University of California, Berkeley. He has also held positions at the University of Geneva, Switzerland, and the University of California's Lawrence Livermore Laboratory.

CDR SHAUN JONES, M.D., USN, currently advises senior advanced technology and concepts groups throughout the national security community. Prior to the current assignment, he completed a distinguished 6-year term at the Defense Advanced Research Projects Agency (DARPA). DARPA is the primary research and development arm of the Office of the Secretary of Defense and is widely known for many of the revolutionary technological advancements to include those enabling Internet and Stealth technology. Dr. Jones is an internationally recognized expert in the diverse disciplines of advanced medical and surgical technologies and biological warfare defense and is a regularly invited consultant to a variety of DoD strategic panels. His extensive military operational experience includes Naval Undersea and Surface Warfare, as well as Special Operations. At the request of the national security community, Dr. Jones now leads a select effort studying the impact of biomedical technology on the future of national security. Dr. Jones is currently an active duty Captain (sel) in the United States Navy and an Assistant Professor of Surgery at the Uniformed Services University of the Health Sciences. He earned his medical degree at the Uniformed Services University of the Health Sciences. He completed a residency in Otorhinolaryngology-Head and Neck Surgery at the National Naval Medical Center and was a resident research fellow in the Divisions of Cytokine Biology and Monoclonal Antibodies, Center for Biologics Evaluation and Research of the Food and Drug Administration (FDA).

ROBERT LAMB, Ph.D., Sc.D., is an Investigator of the Howard Hughes Medical Institute and also John Evans Professor of Molecular and Cellular Biology at Northwestern University and a Professor of Microbiology-Immunology at Northwestern University Medical School. He received his undergraduate degree reading Biochemistry at the University of Birmingham, England, and his Ph.D. and Sc.D. from the University of Cambridge. Dr. Lamb came to the United States in 1974 to do postdoctoral work with Purnell Choppin at the Rockefeller University, where he later became a faculty member. In 1983, Dr. Lamb joined the faculty at Northwestern University. Dr. Lamb is an expert on the replication of influenza virus and paramyxo viruses and his interests include the mechanism of assembly of the viruses, the mechanisms of entry of these viruses into cells and the interactions of these viruses with the host cell. Dr. Lamb is an Associate Editor of the

standard textbook *Fields Virology* and serves as Editor-in-Chief of *Virology*. Dr. Lamb has been awarded two consecutive merit awards from the National Institutes of Health for his work on influenza virus, and the Wallace Row Award for Excellence in virologic research from the National Institute of Allergy and Infectious Diseases. Dr. Lamb is a Fellow of the American Academy of Microbiology and a Fellow of the American Association for the Advancement of Sciences. For 2001–2002, Dr. Lamb is President of the American Society of Virology.

SIMON LEVIN, Ph.D., is the George M. Moffett Professor of Biology in the Department of Ecology and Evolutionary Biology, and Associate Faculty Member in the Program in Applied and Computational Mathematics at Princeton University, where he was also the Founding Director of the Princeton Environmental Institute. He is also an Affiliated Faculty Member of the Princeton Environmental Institute and a Faculty Fellow of the Princeton Society of Fellows in Liberal Arts. He retains an Adjunct Professorship at Cornell University, where previously he was the Charles A. Alexander Professor of Biological Sciences, Chair of the Section of Ecology and Systematics, Director of the Ecosystems Research Center, and Director of the Center for Environmental Research. Professor Levin has also served as President of the Ecological Society of America and of the Society for Mathematical Biology. He is an elected member of the National Academy of Sciences and a Fellow of the American Academy of Arts and Sciences and the American Association for the Advancement of Science. He was the founding Editor of the journal *Ecological Applications*, and has edited numerous journals and book series, including the *Journal of Mathematical Biology* and the *SIAM Journal of Applied Mathematics*. His recent book, *Fragile Dominion*, develops an understanding of ecosystems and the biosphere as complex adaptive systems, and lays out lessons for managing our environment. He also edited the five-volume Encyclopedia of Biodiversity.

JOHN MEKALANOS, Ph.D., is the Adele H. Lehman Professor of Microbiology and Molecular Genetics at Harvard Medical School. He received his B.A. and Ph.D. in Microbiology from the University of California, Los Angeles. Amongst various awards during his career, Dr. Mekalanos has been the recipient of the Harvard University Ledlie Prize, and was elected to the National Academy of Sciences in 1998.

TOM MONATH, M.D., is Vice President of Research and Medical Affairs at Acambis, Inc. He has been engaged in programs of WHO and the National Vaccines Advisory Committee. He was formerly director of the Division of Vector-Borne Infectious Diseases, CDC, and Chief of Virology, USAMRIID. His research has included work on arboviruses, viral hemorrhagic fevers, bubonic plague, and other zoonotic diseases. He has served on various committees dealing with biological weapons (BW) issues.

RANDALL MURCH, Ph.D., is the Deputy Assistant Director, Laboratory Division, Federal Bureau of Investigation. He earned a Bachelor of Science degree in biology from the University of Puget Sound, Tacoma, Washington, in 1974. He earned a Master of Science Degree in Botanical Sciences from the University of Hawaii, Honolulu, in 1976. He completed a Doctor of Philosophy degree in Plant Pathology at the University of Illinois, Champaign-Urbana, in 1979. He is a member of the American Association for the Advancement of Science, American Academy of Forensic Sciences, and the American Society of Crime Laboratory Directors. Dr. Murch regularly works with the Departments of Defense, Energy, Agriculture, and Health and Human Services to plan and develop the nation's response to, and resolution of, biological, chemical, and nuclear terrorism. Dr. Murch has a diverse array of investigative, operational, forensic, applied science and engineering, management, and program development assignments and experiences throughout his 22-year FBI career. Further, he served in the Defense Threat Reduction Agency as the director of its advanced studies group. There, he led the design and execution of many intellectually aggressive studies on new approaches to reduce the threat of weapons of mass destruction. He currently serves as the head of the FBI's national program for applied engineering and technical operation support.

EDWARD PENHOET, Ph.D., is dean of the School of Public Health at the University of California, Berkeley. Prior to his appointment as dean in 1998, Dr. Penhoet was president and chief executive officer of Chiron Corporation in Emeryville, California. He also taught at the University of California, Berkeley, from 1971 to 1998. Dr. Penhoet received his Ph.D. in biochemistry from the University of Washington in 1968 and was a National Institutes of Health postdoctoral fellow at the University of California, San Diego. Dr. Penhoet is active in state and national service organizations including the California Healthcare Institute and the California Governor's Biotechnology Council. He is a member of the Institute of Medicine.

DAVID RELMAN, M.D., is Associate Professor of Medicine and of Microbiology and Immunology at Stanford University. He received his B.S. in biology from the Massachusetts Institute of Technology and his M.D. from Harvard Medical School. Dr. Relman also serves as a Staff Physician at the Veterans Administration Palo Alto Health Care System. Among the many awards and honors he has received are the Senior Scholar Award in Global Infectious Disease from the Ellison Medical Foundation, and the Squibb Award from the Infectious Diseases Society of America. Dr. Relman is a member of the Blue Ribbon Panel on Bioterrorism, NIAID, NIH.

PETER ROSEN, M.D., is a Professor of Clinical Medicine and Surgery and Director of Education in the Department of Emergency Medicine at the Univer-

sity of California, San Diego. He is editor-in-chief of the *Journal of Emergency Medicine* and a consulting editor to *Emergindex Microindex*. Dr. Rosen is a fellow in the American College of Surgeons, a senior board member and consultant with the American Board of Emergency Medicine, and a member of the Institute of Medicine. He has been awarded the Burroughs Wellcome Education Award, and an award for Outstanding Contribution to Emergency Medicine. Dr. Rosen received his undergraduate degree from the University of Chicago and his M.D. from Washington University Medical School.

LUIS SEQUEIRA, Ph.D., is the J.C. Walker Professor Emeritus in the Departments of Bacteriology and Plant Pathology, University of Wisconsin. He attended Harvard University, where he was awarded bachelor's (1949), master's (1950), and Ph.D. (1952) degrees in biology. Following graduation, he spent a year as a fellow at Harvard University and Instituto Biologico in Sao Paulo, Brazil. Dr. Sequeira was director of the Office of International Programs of the American Phytopathology Society; a member of the Scientific Advisory Committee of the Banana Improvement Program of the World Bank; and a member of the Board of Visitors of the Organization for Tropical Studies. He has served as editor-in-chief of *Phytopathology, Molecular Plant-Microbe Interactions*, associate editor of *Plant Physiology* and is on editorial boards of several other publications. He is a former president of the American Phytopathological Society and former chairman of the Agricultural Sciences Section of the National Academy of Sciences. Dr. Sequeira received the Distinguished Achievement Award from the Phytopathological Society of Colombia in 1981, the E. C. Stakman Award from the University of Minnesota in 1992, and the Award of Distinction from the American Phytopathological Society in 1994. He is a member of the National Academy of Sciences (member of the Council, 1999-2000) and the American Academy of Microbiology. Dr. Sequeira is currently a member of the National Science Board.

JEFFERY TAUBENBERGER M.D., Ph.D., serves as Chief of the Division of Molecular Pathology at the Armed Forces Institute of Pathology in Washington, D.C., a position he has held since 1994. He received his M.D. and Ph.D. degrees from the Medical College of Virginia and did a residency in Anatomic Pathology at the National Cancer Institute. His clinical activities involve diagnostic molecular genetic pathology. He is board certified in Anatomic Pathology and Molecular Genetic Pathology. His clinical interests are chiefly in the development and implementation of molecular diagnostic assays for neoplasia and infectious diseases. His research interests include 1) influenza virus biology and surveillance, including characterization of the 1918 influenza virus that killed 40 million people; 2) biology and surveillance of other virus diseases including marine mammal morbilliviruses; 3) genetic changes in breast cancer; and 4) functional genomics of lymphocyte differentiation.

DEAN WILKENING, Ph.D., is director of the Science Program at Stanford University's Center for International Security and Cooperation since 1995. After receiving his Ph.D. in physics from Harvard University in 1982, he spent two years studying defense policy on a Ford Foundation fellowship at the Center for Science and International Affairs, Kennedy School of Government, Harvard University. In 1983 he joined the staff of the RAND Corporation, where he held several management positions as a senior researcher in the Engineering and Applied Sciences and International Policy departments. In addition, from 1985–1994 Dr. Wilkening taught courses on nuclear weapons policy at the University of California, Los Angeles. His major research interests include nuclear strategy, ballistic missile defense, chemical and biological weapons proliferation, and arms control. His most recent work involves an analysis of national and theater ballistic missile defense.

CATHERINE WOTEKI, PH.D., R.D., is Dean of the College of Agriculture at Iowa Sate University. Previously, she served as a professor of human nutrition and food science at the University of Nebraska and a senior research scientist at the University of Maryland, the Under Secretary for Food Safety for the U.S. Department of Agriculture, the Acting Under Secretary for Research, Education, and Economics, the Deputy to the Associate Director of Science of the Office of Science and Technology Policy, and from 1990 to 1994, she was Director of the Food and Nutrition Board, Institute of Medicine, National Academy of Sciences. She received her undergraduate degree from Mary Washington College in Fredericksburg, Virginia, and pursued graduate studies in human nutrition at Virginia Polytechnic Institute and State University, Blacksburg, Virginia, and received a Ph.D. in human nutrition. Dr. Woteki received the Elijah White Award from the National Center for Health Statistics, the Special Recognition Award from the U.S. Public Health Service, and the Staff Achievement Award from the Institute of Medicine. She is a member of the Institute of Medicine.

LIAISONS FROM THE COMMITTEE TO THE PANEL

MARGARET 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 this, Dr. Hamburg served for almost six 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 Ameri-

can 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 for the Advancement of Science.

P. ROY VAGELOS, M.D., is retired Chairman and CEO of Merck and Company, Inc., having served as chief executive officer for nine 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.

NATIONAL ACADEMIES STAFF

ANDREW POPE, Ph.D., is Director of the Board on Health Sciences Policy at the Institute of Medicine. With expertise in physiology and biochemistry, his primary interests focus on environmental and occupational influences on human health. Dr. Pope's previous research activities focused on the neuroendocrine and reproductive effects of various environmental substances on food-producing animals. During his tenure at the National Academy of Sciences and since 1989 at the Institute of Medicine, Dr. Pope has directed numerous reports; topics that include injury control, disability prevention, biologic markers, neurotoxicology, indoor allergens, and the enhancement of environmental and occupational health content in medical and nursing school curricula. Most recently, Dr. Pope has directed studies on NIH priority-setting processes, fluid resuscitation practices in combat casualties, and organ procurement and transplantation.

KATHI E. HANNA, M.S., Ph.D., is a science and health policy consultant, writer, and editor specializing in biomedical research policy and bioethics. She has served as Research Director and Senior Editorial Consultant to the National Bioethics Advisory Commission and as Senior Advisor to the President's Advisory Committee on Gulf War Veterans Illnesses. In the 1980s and early 1990s Dr. Hanna was a Senior Analyst at the now defunct congressional Office of Technology Assessment, contributing to numerous science policy studies requested by

committees of the House and Senate on science education, research funding, biotechnology, women's health, human genetics, bioethics, and reproductive technologies. In the past decade, she has served as an analyst and editorial consultant to the Howard Hughes Medical Institute, the National Institutes of Health, the Institute of Medicine, and several charitable foundations. Before coming to Washington, she was the Genetics Coordinator at Children's Memorial Hospital in Chicago, where she directed clinical counseling and coordinated an international research program investigating prenatal diagnosis of cystic fibrosis. Dr. Hanna received her A.B. in Biology from Lafayette College, M.S. in Human Genetics from Sarah Lawrence College, and a Ph.D. from the School of Business and Public Management, George Washington University.

JENNIFER KUZMA, Ph.D., is a Senior Program Officer, Program Director, and Study Director, Board on Life Sciences. Dr. Kuzma joined the NRC in January 1999. She served as study director for the NRC report, *Genetically Modified Pest-Protected Plants (2000)*, and currently serves as program director for the standing Committee on Agricultural Biotechnology, Health and the Environment and study director for the Committee on Biological Threats to Agricultural Plants and Animals and the Committee on Indicators for Waterborne Pathogens. She obtained her Ph.D. in Biochemistry from the University of Colorado at Boulder where she worked on the purification and cloning of a newly discovered plant enzyme which catalyzes the formation of the gaseous molecule, isoprene. During this time, she also discovered that bacteria produce isoprene and holds a patent for optimizing this production as a biogenic isoprene source for rubber synthesis. Following her graduate work, she was a Research Fellow at the Rockefeller University where she was part of a team that identified a novel signal transduction intermediate, cyclic ADP-ribose, as a trigger for plant responses to cold, drought, and salinity. Her career in science policy began in 1997 when she was awarded an American Association for the Advancement of Science (AAAS) Risk Assessment Science Policy Fellowship. During her fellowship at the USDA, she worked on several risk assessment projects concerning biological hazards in the food supply, such as BSE and *E. coli* 0157:H7. Dr. Kuzma has a strong interest in risk assessment for the use of genetically engineered organisms in food or the environment.

CATHY T. LIVERMAN, M.L.S., is a Senior Program Officer at the Institute of Medicine. In 10 years at IOM, she has worked on projects addressing a number of topics including veterans' health, drug abuse, and injury prevention. She is currently the study director for an IOM study reviewing the literature on the health effects of exposure to pesticides and solvents. Her background is in medical library science with previous jobs at the National Agricultural Library and the

Naval War College Library. She received her B.A. from Wake Forest University and her M.L.S. from the University of Maryland.

ALDEN CHANG is the Administrative Assistant for the Board on Health Sciences Policy. He earned a B.A. in international affairs with a minor in Russian language and literature from the Elliot School of International Affairs, The George Washington University, Washington, DC.

JUDY ESTEP is a Senior Program Assistant at the Institute of Medicine. She has been with the National Academy of Sciences since 1987 and has provided administrative support for over 30 published reports.