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

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

Executive Summary

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

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

Context and Contents of the Report

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

As terrorists seek to exploit these vulnerabilities, it is fitting that we harness the nation's exceptional scientific and technological capabilities to counter terrorist threats.

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

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.

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.

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 source*s. 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 (in-

telligence), 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 post event 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 information 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 interoperability, 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 post event 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 gov-

ernment, 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 de-

ployment 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 necessarily 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 non-governmental 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 work-force. 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 counterterrorism 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.

Endnotes

1. From the President's June 6, 2002, address to the nation. The text of this speech is available online at www.whitehouse.gov/news/releases/2002/06/200206068.html.
2. The [italicized] 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
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