



Defending America in the 21st Century

New Challenges, New Organizations,
and New Policies

Executive Summary of
Four CSIS Working Group Reports
on Homeland Defense

Frank Cilluffo, Joseph J. Collins, Arnaud de Borchgrave,
Daniel Gouré, Michael Horowitz

Center for Strategic and International Studies
Washington, D.C.

About CSIS

The Center for Strategic and International Studies (CSIS), established in 1962, is a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary.

CSIS is dedicated to policy impact. It seeks to inform and shape selected policy decisions in government and the private sector to meet the increasingly complex and difficult global challenges that leaders will confront in the next century. It achieves this mission in four ways: by generating strategic analysis that is anticipatory and interdisciplinary; by convening policymakers and other influential parties to assess key issues; by building structures for policy action; and by developing leaders.

CSIS does not take specific public policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

President and Chief Executive Officer: John J. Hamre
Senior Vice President and Director of Studies: Erik R. Peterson
Director of Publications: James R. Dunton

© 2000 by the Center for Strategic and International Studies.
All rights reserved.

Center for Strategic and International Studies
1800 K Street, N.W., Washington, D.C. 20006
Telephone: (202) 887-0200
Fax: (202) 775-3199
E-mail: books@csis.org
Web site: <http://www.csis.org/>

CSIS Working Group Reports on Homeland Defense

Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy
Frank J. Cilluffo, Sharon L. Cardash, Gordon N. Lederman

Cyber Threats and Information Security: Meeting the 21st Century Challenge
Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michèle M. Ledgerwood

Defense of the U.S. Homeland Against Strategic Attack
Daniel Gouré

Homeland Defense: A Strategic Approach
Joseph J. Collins, Michael Horowitz

Contents

Introduction to the Problem	1
Conclusions	9
Recommendations	11

Introduction to the Problem

The United States faces a series of serious threats to its homeland. These emerging challenges come from missile proliferation in rogue states; the potential use by terrorists of chemical, biological, radiological, and nuclear (CBRN) devices; and various threats to the nation's critical information and economic infrastructure. These threats, although low in probability, have potentially high consequences. Some of them, particularly those involving nuclear or biological weapons, have the potential to cause mass destruction.

Although they are not new, these threats are to a large degree novel. It will take unprecedented efforts by the military and civilian federal, state, and local officials, as well as elements of the private sector, to meet them. Adding to the complexity, neither the federal government nor the U.S. military will usually be the lead actor in meeting these threats. Today, the "first to fight" may well be a police officer, a firefighter, or an information security technician. New actors must become part of the national security equation.

To date, U.S. homeland defense efforts have been like the proverbial glass that is both half full and half empty. Over the past five years, U.S. efforts to address these new challenges have been prodigious yet inadequate. We have fallen well short of putting into place the resources and organizational structure necessary to meet the new threats. The most pressing needs today are for a revised plan for national missile defense (NMD) as well as major organizational changes that will allow comprehensive planning and better training to meet the terrorist and cyber threats. The United States cannot wait for these threats to emerge full grown before taking effective steps to deal with them. The report that follows assesses the nation's progress in meeting these threats to the U.S. homeland and makes recommendations to solve this complex set of problems.

Several recent major strategic assessments—including the Quadrennial Defense Review, the report of the National Defense Panel, and the reports of the U.S. Commission on National Security in the 21st Century—contain strong warnings about new threats to the American homeland. The U.S. Commission issued this stark prediction:

2 Defending America in the 21st Century

America will become increasingly vulnerable to hostile attack on our homeland, and our military superiority will not protect us. . . . States, terrorists, and other disaffected groups will acquire weapons of mass destruction, and some will use them. Americans will likely die on American soil, possibly in large numbers.¹

Other senior officials have arrived at the same conclusion. In fact, a highly placed official on the National Security Council (NSC) staff reported that President Bill Clinton believes that “within the next ten years, there was a 100 percent chance of a chemical or biological attack in our country.”²

To many, homeland defense appears to be a new requirement. But the perception of homeland defense as a new mission strips it of an important part of its context. Homeland defense—the defense of the United States’ territory, critical infrastructure, and population from direct attack by terrorists or foreign enemies operating on our soil—was, is, and will always be the most essential function of our government.

What is changing, however, is not only the level and type of threat, but also how the United States accomplishes homeland defense. Today, the shape of homeland defense has been influenced by three factors:

- the uniquely dominant power position of the United States,
- the technological development of certain states hostile to the United States, and
- the onset of the information age, which has empowered individuals and non-state actors.

First, after the end of the Cold War, the United States became the world’s sole superpower. Its technological prowess—especially in precision attack and information systems—is unmatched and unprecedented. For most competitors, the overriding lesson of recent operations is that successful challenges to the United States must be indirect or asymmetrical. For rogue states and some non-state actors, attacking the United States at home may even be easier than trying to attack a small element of U.S. forces at sea or in the field.

The second factor is the technological development of many nations that pose a potential threat to the United States. Many rogue states—a shorthand expression for about a half dozen states hostile to U.S. interests, including Iran, Iraq, and

¹ United States Commission on National Security/21st Century, *New World Coming: American Security in the 21st Century* (Arlington, Va.: The Commission, 1999), p. 141.

² Richard Clarke in an interview with Lesley Stahl on *60 Minutes*, CBS Television, October 22, 2000.

North Korea—are entering the latter stages of the industrial age and gaining the ability to develop chemical, biological, nuclear, and missile technology. At the same time, for both strategic and economic reasons, Russia, China, and North Korea have compounded the proliferation problem. Today, for most analysts, the focal point for national missile defense is protection from accidental attacks from great powers or small attacks from Iran, Iraq, or North Korea.

Information technology and globalization constitute a third factor. The onset of the information age—marked by the development of the personal computer and the expansion of the Internet—has decreased the power of states and other mass hierarchical organizations and increased the capabilities of markets, individuals, small groups, and networks. Individuals and nongovernmental organizations (NGOs)—the logical, issue-oriented extension of empowered individuals—have become important subsidiary actors in international relations. Economic and even social relations have become subject to globalization, a force outside the control of even the most powerful states.³

These factors present a set of threats that are steadily becoming more serious. In an era of global communications and expanding trade and travel, states or small groups of terrorists—of foreign or domestic vintage—can directly attack the United States' homeland. The knowledge that empowers them to do this is often free to all on the Internet. The resulting attacks can be by conventional means (gun, knife, or bomb), or they can exploit the growing body of knowledge about CBRN (chemical, biological, radiological, or nuclear) weapons or information and the vulnerability of telecommunication systems.⁴ As noted above, a small number of states also represent a potential ballistic or cruise missile threat to the U.S. homeland.

The potential use of biological agents—anthrax, plague, mycotoxins, for example—is particularly troubling. Such agents may well become a more attractive option for a hostile state or terrorist bent on mass destruction. Ounce for ounce, the lethality of these agents is many times that of chemical agents or nuclear weapons. Pounds or possibly ounces of biological agent can do a job that would require tons of a chemical agent.

- In one study, 30 kilograms of anthrax spores applied in a densely populated area at maximum effectiveness created 500 times the number of deaths that could have been produced by 300 kilograms of deadly sarin nerve gas.

³ Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Anchor Books, 2000), pp. 29–72 ; and Thomas L. Friedman, “Parsing the Protests,” *New York Times*, April 14, 2000, p. A31.

⁴ This report will use CBRN for accuracy. It clearly denotes the classes of weapons under discussion. CBRN weapons do not always achieve mass destruction. The less precise term “weapons of mass destruction” (WMD) couples an ambiguous set of weapons with the effects that these weapons may or may not achieve. Moreover, conventional ordnance may well achieve mass destruction under certain circumstances.

4 Defending America in the 21st Century

- A 12.5 kiloton (thousand tons of TNT equivalent) nuclear device—close to the potency of the bomb dropped on Hiroshima—employed in the same area would likely have produced 20 percent fewer deaths than well-dispersed anthrax under relatively ideal climactic conditions.⁵
- Another study suggested that the lethality of 250 pounds of anthrax, spread efficiently over the Washington, D.C., metropolitan area, could cause up to 3 million deaths, significantly more than would likely result from a 1 megaton (a million tons of TNT equivalent) hydrogen bomb.⁶

While the effects of biological agents are subject to varying estimates, there is little doubt that biological weapons in the hands of state or non-state actors have the potential to create much greater destruction than any society can tolerate.

Many recent studies have pointed out the difficulties that terrorists would incur if they wanted to use biological agents. Several factors, however, make the use of biological agents by terrorists a substantial danger in the future. First, in the near term, non-state actors may be helped by rogue states, removing technological obstacles to the efficient use of any kind of CBRN weapons. Second, proliferation in the developing world or the insecurity of the Russian or Iraqi CBRN arsenal may provide a ready source of agent to terrorists. Third, future advances in genetics may make it easier to create more potent and more easily useable agents. Fourth, technological barriers to the effective dispersal of biological agents are disappearing, and knowledge of these advances will inevitably spread.⁷ Finally, our medical and public health systems do not have the capacity to handle a large-scale, CBRN terrorist attack. In the future, terrorists using biological weapons are likely to have a much greater capacity for mass destruction.

Enemies of the United States, opponents of its armed forces, or those in opposition to U.S.-based multinational corporations can also choose cyber crime, cyber vandalism or cyber attacks against U.S. public or private interests, turning our reliance on information systems into a strategic vulnerability.⁸ Cyber vulnerability is magnified by the fact that 95 percent of all U.S. military traffic moves over civilian telecommunications and computer systems. A terrorist can

⁵ Anthony Cordesman, *The Risks and Effects of Indirect, Covert, Terrorist, and Extremist Attacks with Weapons of Mass Destruction: Challenges for Defense and Response*, September 1, 2000, webu6102.ntx.net/homeland/reports/EffectsTerrWMD.pdf (accessed November 2000).

⁶ Tara O'Toole, "Biological Weapons: National Security Threat and Public Health Emergency," a presentation at CSIS, August 22, 2000.

⁷ Randall J. Larson and Ruth A. David, "Homeland Defense: Assumptions First, Strategy Second," *Strategic Review* (Fall 2000): 6–8.

⁸ Frank Cilluffo and Bruce Berkowitz, eds., *Cybercrime, Cyberterrorism, and Cyberwarfare: Averting an Electronic Waterloo* (Washington, D.C.: CSIS, 1998), pp. 1-72.

combat U.S. military forces, disrupt a military operation, or hurt the U.S. economy by hindering our vulnerable civilian telecommunications systems.

Some terrorists are already practicing: In 1999, there were more than 22,000 attacks against unclassified military computer systems, a threefold increase over the number reported in the previous year. A few experts believe that number to have reached a few hundred thousand per year.⁹ Some estimates suggest that only 10 percent of penetrations are detected.

The cyber threat in particular will present new organizational issues. As Richard Clarke, National Coordinator for Security, Counterterrorism, and Infrastructure Protection, told a CSIS audience:

There is a unique challenge here. For the first time in our history, the Armed Forces cannot defend us from the foreign threat. They cannot surround the power grid. . . . Therefore, we are asking the private sector to defend not only itself, but the country as well.¹⁰

In all, a challenging scenario might be a large-scale CBRN terrorist attack or series of attacks, backed up by an intensive cyber attack on the U.S. government and civil telecommunications infrastructure. Such an attack might be timed to coincide with a deployment of military forces to an overseas contingency. To meet such a multidimensional threat, federal, state, and local governments as well as the private sector must pay more attention to unconventional and transnational threats to the U.S. homeland. In the process, this nation will have to change the way it does much of the business of national defense.

The set of instruments that the United States must use to combat threats to our security will have to become much broader. In the past, the first line of defense might be a ship at sea, a fighter aircraft on patrol, or an infantryman walking point. Today, the “first to fight” may well be a police officer, a volunteer firefighter, a hazardous material technician, a nurse, or even an information security technician. Compounding the problem, there may be a significant period of time between the attack and its discovery. Cyber and CBRN terrorists may not leave a clear “return address,” making deterrence, attribution, and even retaliation after attacks on the U.S. homeland increasingly difficult. A delay in identifying such attacks could be very costly.

⁹ Jim Wolf, “Hacking of Pentagon Computers Persists; Pace Undiminished This Year, Complicating Security Efforts,” *Washington Post*, August 23, 2000, p. A23; and comments by Richard Clarke at a lecture for MIT Alumni Association, October 10, 2000.

¹⁰ Richard Clarke, “Homeland Defense: Proceedings of the April 5 Senior Advisory Group Meeting and Participants List,” 2000, webu6102.ntx.net/homeland/reports/sag040500.html (accessed November 2000).

6 Defending America in the 21st Century

The United States must view homeland defense as a partnership among federal, state, local, and private-sector organizations. It must reorganize vertically—federal, state, and local—as well as horizontally within the executive branch. While these threats are legitimate national security problems, they are not—except for national missile defense—primarily the domain of the Pentagon or even the federal government. State and local officials will primarily be in charge. Federal officials will usually find themselves in support of state and local officials. New Jersey governor Christine Todd Whitman, reminded a Capitol Hill audience that state governors were the commander in chief in their states:

As is true so often . . . it comes back to the governors to manage the fallout, literally or figuratively, of any kind of terrorist attack. . . . We are the ones along with our mayors and our local government officials, who actually must deal with people. It is fine to deal with the theory, and we want to be part of that process, but ultimately, we are the ones who are responsible for dealing with the people.¹¹

Legal authority to act in nontraditional areas of homeland defense presents another dilemma. In routine operations, the president and the secretary of defense (the “National Command Authority”) have sufficient legal authority to use the armed forces at home. For example, *posse comitatus*, the law that prohibits most military personnel from engaging in law enforcement, is sufficiently flexible to permit exceptions for riots, civil disturbances, and even support for counternarcotics programs.

There are, however, more complex, unresolved legal issues concerning homeland defense. Because meeting contemporary threats may involve extensive information gathering at home, homeland defense tasks will be especially sensitive to a nation that jealously guards its civil rights. The specter of massive federal involvement in terrorist incidents has been the subject of a few major motion pictures but no significant political debate.¹² In one of his valedictory speeches, Secretary of Defense William Cohen highlighted the sensitivity of homeland defense issues:

I believe that we as a democratic society have yet to come to grips with the tension that exists between our constitutional protection of the right to privacy [and] the demand that we made . . . to protect us.¹³

The issue of legal authority during mass destruction incidents in urban areas is especially problematic. In the case of such an unlikely but not impossible scenario, it is not even clear what the legal questions are, never mind the answers. Expanding homeland defense roles for the Department of Defense (DOD) may

¹¹ Governor Christine Whitman, as recorded in “Homeland Defense: Proceedings of the April 5th Senior Advisory Group Meeting,” 2000, webu6102.ntx.net/homeland/reports/sag040500.html (accessed November 2000).

¹² A recent movie, *Seige*, for example, highlighted the difficulties of seeking military solutions to urban terrorism and highlighted concerns for civil rights in domestic terrorist incidents.

¹³ Secretary of Defense William S. Cohen in a speech delivered at CSIS, October 2, 2000.

make sense; it will also set off alarms. Policy architects will have to balance individual rights with the need to protect society under difficult and potentially unique circumstances.

In summary, homeland defense can be viewed as the defense of the most vital of all of the nation's traditional interests. It also comprises a new set of priority defense activities to meet novel threats that have in common the potential for direct impact on the United States. These threats have appeared in the form of missile proliferation in hostile states, the emergence of CBRN terrorism, and a variety of threats to the nation's critical information and economic infrastructure. Each of these threats is in many ways unique. New national strategies will have to deal with a wide range of both new and old challenges.

These new threats in their worst forms are low-probability but high-impact threats. All of them carry a high element of unpredictability about them. Indeed, the threat of mass destruction inherent in a missile attack or CBRN terrorism—especially in the mid- to long-term future—is such that either one, if it occurred, could literally change the course of U.S. history. The effects of either of these attacks on contemporary foreign and domestic policy would be profound.

Clearly, the United States must do whatever is possible to prevent or deter these threats. The nation must also continue to refine its ability to deal with them if they do occur. The more unprepared we are, the more we encourage attacks on the homeland. The more prepared we are, the higher the likelihood that we can prevent, deter, or effectively cope with the effects of an attack.

The following material—digested from four CSIS working group reports posted on www.csis.org—suggests that in the latter half of the 1990s the nation made significant progress on many issues of homeland defense, but still must dramatically improve policy, programs, and organization for homeland defense against diverse threats. Memories of the repeated failures, for example, to develop and test successfully the United States' controversial national missile defense system remain fresh. Equally salient are the unresolved missile defense issues that concern U.S. allies, as well as China and Russia. At the same time, vigorous efforts to improve the United States' ability to deal with CBRN terrorist threats or threats to its critical infrastructure remain incoherent and inadequate. As one group of experts noted after a simulation of a relatively unsophisticated, single-point, bioterrorist attack: "...the systems and resources now in place would be hard-pressed to successfully manage a bio-weapons attack such as that portrayed in [one scenario of the federal government's] 'TOPOFF' exercise."¹⁴

¹⁴ Thomas Inglesby, Rita Grossman, and Tara O'Toole, "A Plague on Your City: Observations from TOPOFF," *Biodefense Quarterly* 2, no. 2 (September 2000): 9. TOPOFF is the code name for a Defense Department nationwide counterterrorism exercise.

8 Defending America in the 21st Century

While the Office of Management and Budget (OMB) has improved the transparency of the budget process, there is only limited coordination, little long-term planning, inadequate programmatic development, and a near total lack of net assessments. Annual budgets are in search of long-term programs, which, in turn, are in search of the national plans that would give them objectives and priorities. We have only begun to understand all that we are doing and not doing for homeland defense. We do not have adequate threat estimates, technical assessments, or net assessments to guide our policymakers.

The four working group reports of this project tell us that, compared to the U.S. posture five years ago, there has been measurable progress in missile defense, the protection of critical infrastructure, and defense against CBRN terrorism. To get to where we need to be, however, much work needs to be done. Not only are programmatic and policy fixes in order, but many aspects of U.S. homeland defense policy need to be reconsidered, and others need a plan to tie them together. This kind of defense planning is hard enough to do when it entails coordinating the responsibilities of five disciplined, uniformed military services. It is far more complex when it involves wide interagency cooperation on the federal level and also includes state, local, and private actors. We must do more for homeland defense, but, more importantly, we must do it better.

Conclusions

Among the most important findings of the four working group reports on homeland defense are the following:

- There is a priority need to reevaluate our national missile defense goals, programs, and testing program.
- The most obvious need in the area of homeland defense is a national plan and a comprehensive, multiyear program. To develop and enforce such a plan, however, will require major organizational changes in the federal government and new organizations to spur state-federal and state-state dialog.
- The homeland defense effort must fit into the U.S. system of laws and concept of federalism. At the same time, given the possibility of mass destruction and mass disruption, we need to explore areas where new legal authorities may be necessary.
- It will be increasingly important to assess where policies and programs for homeland defense fit in terms of national priorities. Conceptually, homeland defense tasks are related to but do not replace current tasks for deterrence, engagement, presence, and power projection. A failure in any of those tasks may well increase risks to the homeland. Likewise, a failure to build appropriate homeland defense capabilities might encourage an attack that could jeopardize a deployment for an overseas operation.
- U.S. homeland defense efforts have been reactive, disjointed, and focused on post facto consequence management. In addition to the critically important issues of crisis and consequence management, we must see homeland defense in terms of preventing, deterring, disrupting, and attributing attacks on the homeland.
- The U.S. intelligence apparatus is geared primarily to assess major foreign threats in the form of overt attacks on the United States and its allies. While there have been significant improvements in intelligence work on terrorist issues, the United States must continue to redirect efforts at gaining, processing, and analyzing intelligence across the full spectrum of terrorist and cyber threat actions from early planning through execution to attribution of the event.
- In a similar vein, we need to sharpen our knowledge of the effects of the evolving cyber threat and CBRN weapons. The United States urgently requires

10 Defending America in the 21st Century

a net technical assessment that looks not only at threats but also at U.S. capabilities to meet them.

- There is a critical need to train more people to prepare for and deal with cyber security and homeland defense issues.
- There is a critical need in the field of cyber security for the government to improve cooperation with the private sector, create incentives for the private sector to better protect its own systems, and improve its own credibility by improving its internal operations.

Recommendations

The recommendations that follow are those of the four separately constituted reports prepared by the working groups. The recommendations have been modified slightly for this comprehensive executive summary. For detailed discussion and explanation of each recommendation, the reader is referred to the report in question.

Missile Defense

The next administration must develop a new plan for missile defense. The threat assessment needs recalibration, and current missile defense plans may not make sense in terms of the technological possibilities. Future air and cruise missile defenses must also be taken into account. Moreover, the next administration will also have to improve coordination with U.S. allies, come to some final agreement (or disagreement) with Russia over the Anti-Ballistic Missile (ABM) Treaty, and link national missile defense to an overall approach to arms control and efforts to reshape strategic offensive forces. Much useful research and development has taken place during the past decade. Now we must develop an architecture that reflects new strategic requirements and encompasses the threat, the infrastructure, and the technology.

President Clinton's decision to postpone NMD deployment provides the opportunity to reevaluate the path to national missile defense and the criteria for future systems. The next administration will undoubtedly conduct a review of programs and options. In light of program delays, there will be time, probably several years, before a decision on NMD will be required if a deployment is to take place as soon as a defense is judged feasible.

The decision on program direction should be based on a return to first principle: a clearly stated administration goal that the United States should deploy as soon as possible an effective NMD. An initial deployment, however, need not, indeed it probably cannot, provide the same level of effectiveness as a robust system. Any system must have sufficient growth potential to address new missions. The planned NMD architecture should allow for capabilities beyond those associated with an initial deployment, capabilities that will enable it to be effective against not only a near-term North Korean threat but also advanced threats posed by North Korea and simple or complex threats from other nations.

12 Defending America in the 21st Century

To develop and demonstrate an effective NMD capability at the earliest possible date, the next administration should:

- Consider an initial NMD deployment, as soon as practical, at Grand Forks, North Dakota. Such a deployment would serve as a test-bed for the planned system, allow for testing of the integrated command, control, and communications (C3), and permit crew training.
- Restructure the NMD test and evaluation program. More tests and more realistic testing of the system are required.
- Address the countermeasures (CM) issue through a program to develop and test representative CMs.
- Ensure the successful development and deployment of the Space-Based Infrared System (SBIRS). Space-based surveillance will be required both as an alternative to land-based radar and as a means of defeating some countermeasures.

A program that can meet the requirement of effective defense against initial threats with growth potential will require, at a minimum, the following elements:

- Multiple sites for ground-based interceptors (three to five)
- An interceptor inventory in the several hundreds
- Freedom to deploy sensors
- Freedom to test and develop advanced defenses (e.g., directed energy)
- Freedom to deploy theater defenses (abandonment of demarcation)

The next administration should consider additional measures to refine the set of potential options for responding to an emerging ballistic missile threat. These include the following:

- Evaluate options for enhancing an initial NMD system by the deployment of additional defensive layers (e.g., boost-phase, naval NMD, point defenses). Such an evaluation should not be permitted to delay efforts to deploy a land-based national missile defense.
- Improve intelligence collection and analysis of states possessing or acquiring ballistic missiles. Traditional assessments of proliferants' capabilities, intentions, and behaviors are inadequate. In addition, there is little understanding of potential adversaries' military plans regarding ballistic missiles and weapons of mass destruction (WMD).
- Develop a new strategy for addressing the ABM Treaty that recognizes the limits the treaty imposes on development of missile defenses. Effective

nationwide defense against anticipated threats is not possible within the ABM Treaty. Modest amendments to the treaty will not permit the development or deployment of the robust system needed if a sophisticated threat emerges. The choices are to modify “early and often,” pursue a “Big Bang” revision, or, if Moscow refuses to negotiate changes to the ABM Treaty, withdrawal.

- Provide significant additional funding, on the order of several billion dollars annually, to ensure that the proposed program can be achieved.

Organization to Meet CBRN and Cyber Threats

A national plan for these aspects of homeland defense must encompass federal-, state-, and local-level responsibilities. This plan must include threat assessments, objectives, key concepts, and means. It would cover all details of the nation’s defense against terrorists, as well as plans for critical infrastructure protection. Missile defense is more of a classical defense responsibility, but the U.S. homeland defense plan would also include provisions for consequence management against a foreign missile strike on the territory of the United States.

Today, such an overarching plan is not possible because no one has the authority to write one and make it stick. Today, the nation has up to \$12 billion of federal budget authority, in search of long-term programs, which, in turn, are in search of coordinated and prioritized objectives. Recent suggestions about super coordinators or new deputy attorneys general ignore the complexity of this problem. The United States cannot rely on super coordinators or subcabinet officers to build new federal-state bridges or to ride herd on cabinet departments.

We recommend that the president make the vice president responsible for most aspects of homeland defense. In performing this function, the vice president would be assisted by an "Emergency Planning Staff," or EPS, drawn from a reinforced national coordinator's staff and selected Department of Justice organizations. The National Coordinator for Security, Critical Infrastructure and Counterterrorism would retain the current title and would become the principal deputy to the vice president for homeland defense issues. He or she would also continue to be a member of the NSC staff. The national coordinator would also become the chief of the Emergency Planning staff. The head of the Federal Emergency Management Agency (FEMA) would report through the national coordinator to the vice president. Both of these positions would be confirmable by the United States Senate.

Among his or her principal responsibilities, the vice president would chair a new National Emergency Planning Council that would include representatives from all departments, agencies, states, and territories. This council would be the senior body for federal and state coordination on matters relating to critical infrastructure protection or response to terrorist incidents. Private-sector organizations would be invited to participate on issues related to critical

infrastructure protection. The council would meet twice yearly, once at the principal level (vice president, governors, CEOs), once at the subordinate level. The national coordinator would be the vice chair of the council.

Under this reorganization, there would be no changes to the principal State Department, Justice Department, and FEMA responsibilities for crisis management and consequence management. Federal Bureau of Investigation and CIA counterterrorist coordination efforts would remain unchanged. Neither the national coordinator nor the vice president would supervise ongoing counterterrorism or counterintelligence operations. The National Infrastructure Protection Center (NIPC) would remain under the auspices of the FBI, and the Critical Infrastructure Assurance Office (CIAO) would remain at the Department of Commerce.

Some consolidation of offices and/or functions would take place to support new EPS in the Office of the Vice President. The National Defense Preparedness Office (NDPO), a Department of Justice clearinghouse for domestic preparedness, would be transferred to FEMA. Selected divisions of the Office of State and Local Domestic Preparedness Support, currently in the Office of Justice Programs, would also become a part of FEMA or the Emergency Planning Staff. The EPS and FEMA would also absorb responsibility for running training programs under the Nunn-Lugar-Domenici Act that were recently been transferred from the Defense Department to the Justice Department.

At the same time, the president and Congress should augment FEMA with personnel as well as administrative and logistical support to play a lead role in domestic CBRN preparedness. FEMA is already well integrated into state- and local-level activity, and it makes little sense to take away training for consequence management from the very organization that has been assigned that function.

The Pentagon must also realign offices so that it has one coherent system for civil support to natural disasters and to terrorism, as opposed to the two distinct systems that it has today. The Directorate of Military Support (DOMS) should no longer work for the Secretary of the Army, but instead be aligned with the Joint Staff and Joint Task Force Civil Support. In the next administration, the Assistant to the Secretary of Defense for Civil Support should become a confirmable Assistant or Deputy Under Secretary of Defense. When confirmed, this official needs to ensure that lines of responsibility within the Office of the Secretary of Defense are clarified and that any overlap in the functions of the Assistant Secretary of Defense for Reserve Affairs and the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict is corrected.

To foster more effective oversight, a bipartisan congressional task force should study ways to improve and simplify the oversight of selected homeland defense tasks. The objective would be for each legislative body to have only one authorization and one appropriations committee for cyber threats, CBRN

terrorism, and critical infrastructure protection. The leadership of the House and the Senate should also appoint a minority and majority staff specialist in each of the appropriations and authorization committees to follow all counterterrorism programs. These staffers can educate members who are voting on a specific agency's counterterrorism program about how that program or policy fits into the overall U.S. counterterrorism effort.

Planning for CBRN and Cyber Threats

Among the key, recurring tasks for the vice president, the national coordinator, and the Emergency Planning Staff would be the following:

- Develop an Annual Preparedness Report, to include evaluations of the nation's ability to prevent, deter, and respond to attacks on the homeland.
- Coordinate or otherwise participate in the development of threat assessments, technical assessments, and net assessments relating to homeland defense.
- Coordinate the development of future programs in each related federal department or agency and institute coherent and effective annual budgetary reviews.
- Coordinate national plans for critical infrastructure protection and domestic terrorism response.
- Supervise all aspects of emergency planning and policy development for the federal government.

The vice president, the national coordinator, and the EPS should also accomplish the following projects on a priority basis.

As soon as practical, the vice president and the national coordinator, in conjunction with OMB, should assess the budgetary programs of federal agencies for homeland defense. The objective here, as noted above, would be to create annual budgets that clearly support long-term programs that, in turn, support the major objectives outlined in the national plans.

Early on, the vice president and the national coordinator need to assess the United States' present and future needs against its ongoing research efforts and make detailed recommendations to the president and the Congress. While the CSIS working groups on homeland defense have not made a detailed assessment of R&D needs, many experts believe that the federal government should foster an acceleration of research in immunology and genetics with the objective of putting improvements in immune responses ahead of the ability to create new and more

deadly biological agents.¹ A net technical assessment is needed on this set of options, as well as on others that include an analysis of potential deployment costs and requirements, countermeasures, and relative costs and benefits.

The vice president and his new staff should develop a new and comprehensive series of exercises, simulations, and evaluations. The purpose of these activities will be to identify and improve the readiness of the government to carry out potential tasks and coordinate an effective response to all incidents, especially those that involve CBRN weapons or that might otherwise create mass destruction. At the same time, these exercises should be specifically designed to identify and help to resolve conflicts of legal authority and potential civil rights issues.

In conjunction with this series of exercises, the federal government must develop ways (see below) to improve the lessons-learned process so as to ensure that learning from exercises takes place and that the resulting knowledge receives the widest possible dissemination.

As soon as practical, the president should also direct the vice president and the director of Central Intelligence (DCI) to assess the country's ability to gain, process, analyze, and disseminate intelligence on cyber and terrorism issues. CBRN counterterrorism poses unique challenges to the U.S. intelligence community. Terrorist groups are difficult to penetrate and less susceptible to technological collection techniques. Continuing to widen the circle of intelligence consumers to include Health and Human Services (HHS) and selected state and local officials will be an important task. It is clear also that FBI and CIA guidelines about recruiting terrorists as informants must be simplified to make it easier to recruit terrorists to provide information.² Several specific steps to strengthen the intelligence community need urgent examination and may require important changes to intelligence programs and budgets:

- Invest in all source intelligence capabilities. Multidisciplinary intelligence collection is crucial to provide indications and warning of a possible attack as well as insights into the cultures and mindsets of terrorist organizations, and to identify key vulnerabilities that can be exploited and leveraged to disrupt terrorist activities before they occur. To date, signal intelligence (SIGINT) has provided decisionmakers with the lion's share of operational counterterrorism intelligence. National technical means cannot be allowed to atrophy further. While a robust technical intelligence capability is crucial, our human intelligence capability must also be enhanced. This is especially needed against

¹ Conversation between Joseph Collins of CSIS and Dr. Tara O'Toole of the Johns Hopkins Center for Civilian Biodefense Studies, Washington, D.C., August 22, 2000.

² This issue was first publicized in L. Paul Bremer III, et al., *Countering the Changing Threat of International Terrorism: Report of the National Commission on Terrorism* (Washington, D.C., July 13, 2000), pp. 7-10.

terrorists, who operate in small groups with less technical paraphernalia to monitor and who are less vulnerable to satellite reconnaissance.

- Invest in intelligence analytical capabilities. The intelligence community, including the FBI, must invest in expertise—linguists, CBRN experts, and regional experts—to buttress its analytical ability to track terrorists considering using CBRN weapons. Moreover, the intelligence community must think creatively in structuring its analytic capabilities to track the CBRN terrorist threat.
- Tighten coordination among the nonproliferation, counterproliferation and counterterrorism communities. Rotational assignments at the analyst level would in part serve this end.
- Tap the scientific and biomedical research communities. Develop networking relationships with the scientific and biomedical research communities, whose knowledge of emerging capabilities and of other information gleaned from the open scientific literature, international scientific collaborations, and conferences could prove invaluable to the intelligence community—particularly with respect to the bioterrorism threat. Indeed, some of the most critical intelligence related to bioterrorism may be derived through the ongoing and open-source practice of international public health and surveillance activities, such as those run by the World Health Organization.
- Invest in detection and attribution capabilities. A credible retaliatory capability, essential for effective deterrence, depends on a strong attribution capability to identify the perpetrators and their supporters. These capabilities include laboratory facilities, other equipment, and the personnel necessary for CBRN attribution.
- Strengthen the U.S. warning capability. Facilitate rapid communications for conveying information concerning warning and preemptive attack. Conduct a lessons-learned study of U.S. government warning across the entire intelligence cycle (collection, processing, analysis, and dissemination).
- Carry out a "Net Assessment of Intelligence Capabilities to Deal with Asymmetric and Terrorist Attacks." Develop a comprehensive net assessment of current and projected U.S. intelligence capabilities to deal with the problems of warning, detection, defense, targeting, and damage assessment, with a supporting net technical assessment of the capabilities to use national technical means and the current and future capabilities of key organizations like the National Security Agency and the National Reconnaissance Office, and the role of human intelligence.
- Develop "Annual Net Threat Assessments of the Foreign and Domestic Threat of CBRN Attacks and Terrorism." Provide federal planners with the basis for assessing the emerging risk of such attacks and develop an integrated analysis structure for planning U.S. programs and response.

The vice president and the EPS should join with the Defense and State Departments to review the United States' arms control posture to see if a more effective enforcement regime could put teeth into the prohibitions on the development of biological weapons. Even though its verification procedures will have serious limits, the Biological Weapons Convention is useful because it strengthens the international norm against development of biological weapons and creates an impediment to nations bent on acquiring biological warfare capabilities.

Finally, the vice president and the EPS should study other ways to build up the nation's prevention and deterrent capabilities against terrorists and cyber attack. For example, a well-conceived, effective, and well-publicized exercise program that demonstrates U.S. capability to deal with attacks could help to deter hostile states or terrorists from choosing biological or chemical weapons or attacking our critical infrastructure.

Similarly, the vice president and the national coordinator should support the continuation of the Nunn-Lugar Threat Reduction Act. In the future, to help prevent threats to the West, Nunn-Lugar needs to redouble its efforts to assist the Russian government to destroy chemical stocks and related equipment.

CBRN Terrorism and Other Homeland Defense Training

An inadequate number of people in the United States are trained for cyber security and to combat CBRN terrorism.

In the cyber area, in 1999 only 10 U.S. citizens received the highest academic degrees in computer security. Majoring in other aspects of computer science or related disciplines carries much greater financial rewards. Clearly, the federal government will have to establish incentives for people to move into this field and stay in government service. In this regard, CSIS applauds the appropriation in FY2001 of \$11 million of scholarship money, administered by the National Science Foundation, for students who will serve in government cyber security positions.

In the area of CBRN terrorism, the focus should be on training emergency responders, emergency room personnel, and public health officials. Only about 3 percent of the total number of emergency responders have been trained in the past five years. To assist in training at their level, emergency responders need a single doctrinal focal point for manuals and training programs for civilian CBRN terrorism responders.

To move toward these goals in the near term, the federal government should examine such options as the following:

- Fund the Justice Department’s Center for Domestic Preparedness (CDP) at Anniston, Alabama, to allow it to achieve full capacity of 10,000 trainees per year. Also, continue to fund the U.S. Public Health Service’s Noble Training Facility at the same location. Both of these new institutions are special national assets and should be carefully nurtured and protected.
- Encourage departments who use the CDP to assign all of their graduates to training roles within the local departments.
- Continue to coordinate with the U.S. Army Chemical School at Fort Leonard Wood, Missouri, to share training techniques and lessons learned on dealing with chemical and biological devices and defense operations.³
- Continue at a minimum the same level of interagency effort at mobile training after the Domestic Preparedness Program goes under Justice Department control in FY2001.
- State Department-sponsored training of host nation personnel is chronically underfunded and should be drastically increased. In other areas, the president and secretary of state should do whatever is necessary to assure full funding for protection of United States embassies and installations overseas.
- As a separate entity, fully fund the National Defense Preparedness Office clearinghouse for information on WMD preparedness planning and policy.

In the long term, the federal government should:

- Continue to reassess equipment and training needs across the country.
- Determine the steady state number of people that will have to be trained to deal with terrorism and weapons of mass destruction.
- As initial needs are met, gradually abolish mobile training teams and replace them to the greatest extent possible with multilevel institutional training at full capacity CDPs or other fixed training institutions. The focus of this institutional training should be to train local trainers and officials.
- Develop a WMD “training and doctrine center” in Anniston, Alabama, or some other suitable facility. This center could also become the hub of the cyber attack and CBRN terrorism lessons-learned process. Also, organize a series of conferences, as well as a private Internet site, to facilitate the sharing

³ CSIS questioned whether there was excess capacity at the USA Chemical School at Fort Leonard Wood that could be used to train first responders. An extensive estimate was conducted on-site and Army experts determined that there was very little excess capacity there. See correspondence from the USA Chemical School to CSIS, dated October 4, 2000.

of ideas and lessons-learned among emergency responders throughout the United States.

- Study the need and feasibility of establishing a second CDP-type of live agent training facility, probably in the western United States, to allow a greater number of responders to be trained expeditiously in a toxic agent environment.
- Foster greater organizational collaboration between the health sector and emergency management officials. Such collaboration is critical for survival at the local level during an epidemic. FEMA and HHS should develop an equivalent national preparedness program together to foster such collaboration. Linkage at the county and city level is critical and will not happen until FEMA and HHS are well-connected by a common doctrine guiding bioterrorism preparedness and response at the top level.

Medical Training and Preparedness

In a similar vein, we need to continue to improve the ability of U.S. hospitals, public health services, and health care providers to deal with mass casualties and the effects of chemical and biological weapons. This will entail the examination of the most cost-effective approach to equipment and drug stockpiling. All of this will be especially difficult in an environment where a third of all civilian hospitals are already losing money. The federal government will have to continue to leverage the public health and Veterans Administration (VA) medical systems to help local hospitals adapt to the threat. The core capacity for public health and medical care needs to be greatly enhanced with respect to detection and treatment of infectious disease. The biomedical and public health communities should be working in greater partnership with each other and should be integrated more effectively into the larger national security community. Once again, the federal government needs to determine the most cost-effective program to achieve the following:

- Capitalize the public health structure. Core functions of public health (e.g., disease surveillance and laboratory capability) will form the foundation of detection, investigation, and response for bioterrorist threats. Development of these core functions requires investing in communications facilities, administrative support, and surge personnel capabilities so that public health offices are capable of leading the effort to contain and eradicate epidemics. Run exercises to test capabilities and determine what is cost-effective.
- Direct FEMA and CDC to develop the national response capacity for the rapid assessment of a bioterrorist emergency occurring anywhere in the United States. These agencies will need to develop a Biological Emergency Support Team (BEST) that can rapidly assess and set priorities following the consequences of a bioterrorist event. This will ensure that FEMA can rapidly galvanize other federal departments around a common assessment and set of

response priorities during a national emergency. Furthermore, this arrangement links state and local infectious disease control agencies through CDC to the disaster management skills of FEMA.

- Expand the provisions on biological terrorism in the Terrorism Annex of the Federal Response Plan. The current U.S. plan for an organized response must be updated to include preparedness for a biological attack, which presents a host of unique and complicated challenges and requires reexamining lead agency roles and missions. The National Disaster Medical System (NDMS), which is composed of FEMA, the Defense Department, HHS, and the VA, has no strategy to rapidly augment medical resources at the state and local levels in the event of a biological attack. The NDMS has never been resourced properly, nor has it been properly focused on the issue of bioterrorism response. The NDMS needs to be funded adequately, and FEMA should be designated the lead federal agency to coordinate the NDMS's activities.
- Increase physicians' awareness of the symptoms of biological weapons. Physicians are the tripwire for recognizing a biological attack and must be trained to spot symptoms of exotic diseases and rapidly report unusual manifestations or clusters of disease to the appropriate public health authorities. HHS should work with pertinent infectious disease professional societies and medical specialists to further this goal.
- Develop a national bioterrorism surveillance capacity. Surveillance is the touchstone of public health and organizes the other capacities within the public health sector. A national bioterrorism surveillance system should allow public health and emergency managers to monitor the general health status of their populations, track outbreaks, monitor health service utilization, and serve as an alerting vehicle for a bioterrorist attack. There should be linkage between public health and clinical medicine, hospitals and health departments, local health officers, and local, state, and federal health authorities. This capacity does not exist at this time; an emergency mobilization toward this end is urgently needed.
- Develop suitable diagnostic capabilities and systems. Develop rapid and more reliable diagnostic capabilities, build regional diagnostic centers, and upgrade hospital diagnostic laboratories. Create a "library" of strains of diseases that is linked—in real time and via a safe intranet—to public health and medical systems worldwide. Rapid and "gold standard" diagnostic capabilities are critical to catching a biological attack in time to prevent massive casualties. Expand CDC's national bioterrorism laboratory response network and laboratory standardization efforts under way with the states. Full implementation of this multidepartment effort (the Defense, Energy, and Agriculture Departments as well as the FBI) will come close to full coverage of the entire nation. CDC's rapid response and technology transfer laboratory activities in support of this network should be dramatically expanded. The development of standardized assays and public health laboratory detection should be a priority.

- Stockpile antibiotics, vaccines, and other related pharmaceuticals and materiel. Currently, CDC is developing a fledgling stockpile of pharmaceuticals for civilian use. DOD also has major stockpile activities in progress. These efforts must be more fully supported and extended to match evolving needs and emerging technologies. At the same time, because of the administrative complexities and financial costs (in the billions of dollars) associated with developing a national pharmaceutical stockpile of vaccines, drugs, and equipment, a standing board (which reports to the president) composed of scientists, stockpile managers, federal government representatives, and private-sector pharmaceutical administrators should ensure that the bioterrorism threat to civilian populations lines up with the national R&D efforts and the requirements of the pharmaceutical stockpile.
- Develop a comprehensive plan for assuring surge capacity for health care. Through both regional and national planning efforts, identify all existing assets and how they would be mobilized to address mass casualty care. In addition, develop working strategies for rapid expansion of care as needed, including potential mobilization of field hospitals or establishment of auxiliary care facilities (e.g., in school gymnasiums, armories, or hotels). This would also need to include strategies for rapid mobilization of critical equipment needs (e.g., ventilators or respiratory isolation capacity) on a regional basis.
- Increase R&D for new vaccines, antidotes, and medicines. Harness the power of the U.S. academic and business communities to research and develop better understanding of basic pathogens and immunology; new antidotes/vaccines, especially for unknown/“designer” toxins; ways to lengthen the shelf life of existing antidotes/vaccines; and improved biological detection capability (for both human and environmental samples). Provide incentives, utilize contracts, and adopt an "In-Q-Tel" style format with universities and companies. Strengthen applied R&D programs and ensure that R&D is not concentrated solely on military needs.
- Develop an integrated plan for biomedical research capabilities of the Departments of Defense and Health and Human Services. Ensure that applied research receives adequate focus as compared to long-term bench research projects.
- Legislate emergency supplemental funding authority (akin to FEMA natural disaster supplementals) for CBRN response activities reimbursement.
- Engage the pharmaceutical industry and the private sector as a whole. Explore new funding strategies to “incentivize” broader participation of the private sector, including ways to encourage greater engagement of hospitals/medical care providers in preparedness planning and capability building, and ways to more fully engage the pharmaceutical industry in developing and supplying new diagnostics, antibiotics, antivirals, and vaccines.
- Prepare a communications and information strategy. Information concerning medicine and diseases should be developed, in various languages, before the

event so as to be readily available. Public health and other governmental personnel who will engage in media relations during a biological attack should train for the role and should build trust with the media.

- Identify and remedy legal ambiguities or inadequate authority. An interagency task force, with state and local representation, should immediately begin efforts to identify legal issues raised by a CBRN threat or attack and work to resolve those issues, whether through proposing new laws or simply clarifying the application of existing laws and authorities.

Special Recommendations on Cyber Issues

As has been noted, to create improved cyber security, the government must improve cooperation with the private sector, create incentives for the private sector to better protect its own systems, and improve its own credibility by improving its internal operations.

Government can improve cooperation with the private sector in many ways. Options that deserve high priority consideration include the following:

- Conduct information-sharing on vulnerabilities and warnings of ongoing attacks or threats; share information on hacker modus operandi and on solutions and defenses to established threats and attacks.
- Continue to facilitate discussions within industry sectors, interaction with information sharing and analysis centers (ISACs), and assistance in collecting, "sanitizing," and disseminating pertinent warnings of threats and attacks.
- Build on the successful elements of the National Information Protection Center (NIPC) model while learning from its mistakes (most notably, its failure to reciprocate information sharing, and its tendency to demand private-sector action using national security language rather than business concerns).
- Establish a single point of national coordination for cyber concerns and alerts, specifically, the creation of both an office for a cyber "commander" (or "national CIO") and a "cyber-911" virtual center that would issue warnings, provide security-related information, and coordinate multiple-agency responses in emergencies. Unlike NIPC, this new virtual center would not be housed within the Department of Justice, but rather within an organization less restricted by its own information-protection and law-enforcement mission.

Government also can provide specific incentives to the private sector to better protect its own systems. Suggested approaches include the following:

- Collaborate in collecting and sharing risk-data information, and acting as the catalyst for the establishment of industrywide standards for information security in different business sectors.

24 Defending America in the 21st Century

- Grant relief from specific provisions of antitrust laws to companies that share information specifically related to vulnerabilities or threats.
- Establish liability limits against disruption of service for companies using security "best practices."
- Establish clear corporate liability for disruptions to consumers (i.e., limit consumer liability in ways similar to the Electronic Fund Transfer Act).
- Provide extraordinary liability relief to the private sector in the case of cyber warfare, similar to the indemnification authorities set up in case of destruction of commercial assets through conventional warfare.
- Provide specific awards or credits for information leading to hacker arrests.
- Enact intermediate regulatory steps (both domestic and international) governing shared systems.

Government can also increase its credibility with the private sector by taking certain internal measures:

- Generate an agreement across agencies on a clear definition of the problem and a clear breakdown of responsibilities (e.g., warning vs. defense vs. prosecution).
- Improve internal security practices, including strengthening the requirements for system upgrades and timely anti-virus software upgrades, tightening personal security requirements, and instituting personal accountability for the handling of sensitive government data.
- Improve information-sharing processes and incentives within and between agencies.
- At the agency level, establish policies that focus not only on remediation but also on reconstitution and continuity of operations.
- Work toward altering the incentive structure in the law enforcement and intelligence communities so that prevention becomes as important as prosecution.
- Vastly improve education and training not only of security professionals, but of all government employees handling sensitive data on government information systems.
- Provide direct financial incentives to universities to develop information security curricula, and to integrate information security not only into their current information science programs, but into their humanities and public policy courses as well.
- Finally, work toward more comprehensive legislation for international collaboration on both the prevention and prosecution of cyber crimes and cyber aggressions.