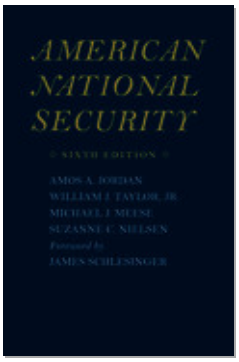
American National Security

Jordan, Amos A., Taylor, Jr., William J., Meese, Michael J., Nielsen, Suzanne C., Schlesinger, James



Published by Johns Hopkins University Press

6

Homeland Security

Protecting the U.S. homeland and its citizens against all manner of threats has been one of the foremost duties of government throughout the country's history; to this end, the Constitution empowers Congress to "raise and support Armies . . . provide and maintain a Navy," and "provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions."[1] The terrorist attacks of September 11, 2001, focused the nation on a dimension of the security challenge that had been receiving scant attention. The result was the most significant reorganization of the U.S. government since 1947, a reorganization that included the creation of a new Department of Homeland Security (DHS). In addition, the Department of Defense (DoD) formed a new combatant command to plan and implement the U.S. military's actions in securing the homeland, and Congress passed significant legislation designed to facilitate the prevention of future attacks.

These efforts have brought to light fundamental questions associated with providing homeland security in a liberal democracy with a federal system of government. Defining their respective roles and forging effective cooperation among the many organizations and federal, state, and local jurisdictions with a stake in some aspect of homeland security are predictably difficult. The process of making resource allocation choices on what to protect and how to protect it is fraught with political consequences. Important judgments on the desired balance between liberty and security underpin most major homeland security decisions, as demonstrated in debates over the limits of law enforcement authority and the proper role of the military in the homeland. This chapter outlines the development of U.S. homeland security efforts and explores many of these issues.[2]

Growth of the Homeland Security Bureaucracy

Prior to the terrorist attacks of 9/11, the term *homeland security* was rarely used. Protection of the U.S. homeland was accomplished by a variety of organizations at the federal, state, and local levels that performed law enforcement, national defense, counterespionage, border protection, health, and emergency management functions.[3] During most of the country's history, homeland security actions largely centered on defense of borders and coastlines against external attack. This theme continued through the Cold War, with emphasis on civil defense activities and preparation for the possibility of a nuclear strike.

During the 1990s, concern over terrorist attacks began to dominate the U.S. homeland security agenda. The 1993 bombing of the World Trade Center, which killed six and injured over one thousand, focused attention on the emerging threat posed by transnational Islamist terrorist groups, as did a string of attacks against the United States on foreign soil: the 1996 Khobar Towers bombing in Saudi Arabia, the 1998 bombings of the American embassies in Kenya and Tanzania, and the 2000 attack on the USS *Cole* in Yemen. In addition, the 1995 bombing of the Murrah Federal Building in Oklahoma City and the 1995 sarin gas attack on the Tokyo subway by Aum Shinrikyo provided deadly examples of domestic terrorism. Several natural disasters—most notably Hurricane Andrew in 1992—demonstrated potential problems in the nation's capability to respond to catastrophic events.

Against this backdrop and the growing realization that transnational terrorist networks and the proliferation of nuclear, biological, radiological, and chemical weapons technology posed a major threat to the U.S. homeland, various government and academic groups began to take a harder look at the country's ability to prevent and, if unsuccessful, mitigate the impact of terrorist attacks. Well before 9/11, reports by the U.S. Commission on National Security/21st Century (The Hart-Rudman Commission) and the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the Gilmore Commission) recommended improvements in information sharing on terrorist threats, increased efforts on national preparedness for attacks, clarification of national priorities and objectives through strategic planning, and significant organizational changes in the executive branch.[4]

The events of 9/11 crystallized much of this thinking, and the government quickly embarked on an enormous reorganization designed to deal more effectively with the threat of future attacks. The key elements of this effort included the creation of the DHS, an extensive reorganization of the intelligence community, and passage of legislation including the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, commonly referred to as the *Patriot Act*. The U.S. Northern Command, a new military combatant command focused on homeland security issues, was also established.

The Department of Homeland Security. President George W. Bush announced the creation of the Office of Homeland Security on September 20, 2001,

launching a whirlwind of action to put responsibility for most homeland security tasks under a single organizational umbrella. On November 25, 2002, the DHS was formally established by the Homeland Security Act. This new department subsumed the Office of Homeland Security and brought together all or part of twenty-two organizations, including the Transportation Security Administration, U.S. Customs and Border Protection, the Federal Emergency Management Agency (FEMA), the U.S. Secret Service, and the U.S. Coast Guard, with wide-ranging duties and charters. With over one hundred eighty thousand employees, the department became the third-largest in the U.S. government. The organization of DHS is depicted in Figure 6.1.

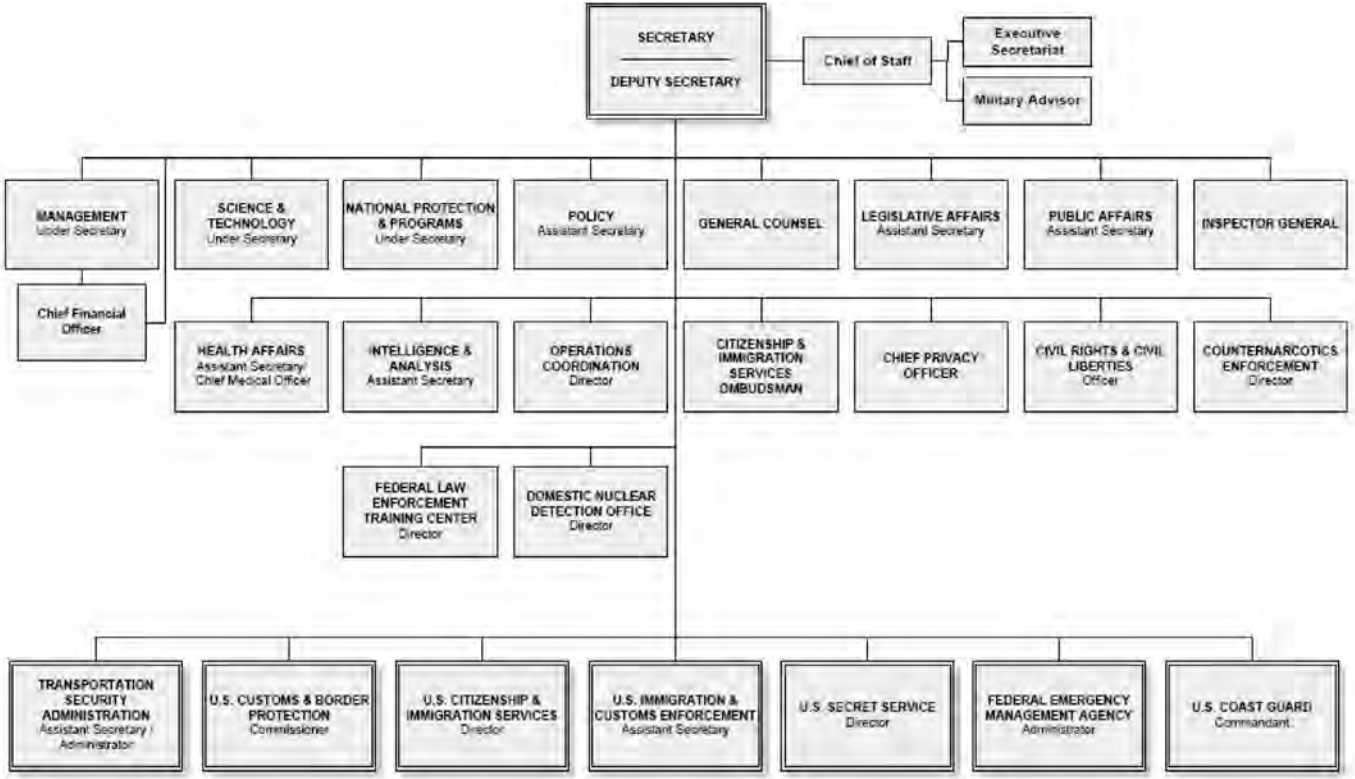
The department was assigned the broad mission to "prevent terrorist attacks within the United States, to reduce America's vulnerability to terrorism, and to minimize the damage and recover from attacks that may occur."[5] The Homeland Security Act also formally established the Homeland Security Council (HSC), an organization similar to the National Security Council (NSC), to advise the president on homeland security matters and to coordinate interagency policy development and implementation (for more on the HSC, see Chapter 10). Many states and local communities instituted similar organizational changes, with the same goal of improving unity of effort in securing the homeland.

Despite general consensus on the need for change, criticism of the Homeland Security Act reflected basic American tensions regarding the role and efficiency of federal government. Some argued that, in at least two key ways, the government may not have gone far enough in centralizing power. First, the Federal Bureau of Investigation (FBI), which leads law enforcement counterterrorism activities, was left in the Department of Justice, and other critical homeland security functions, such as intelligence gathering and analysis, also remained outside DHS control.[6] Second, the department's primary focus on terrorism, rather than an all-hazards approach to homeland security, could result in missed opportunities to create a more seamless system.

Others felt that the reorganization stretched too far, claiming that the wide variety of organizations brought together under the department created the potential for abuse of power and produced too big a management challenge. As an example of the latter, some critics of FEMA's poor response to the devastation caused by Hurricane Katrina in 2005 argued that the agency had not received adequate funding and attention since its inclusion in the department. In any case, the initial years of the DHS's operations were marked by the type of bureaucratic infighting, budget debates, and inefficiencies that would be expected to accompany any governmental reorganization this extensive. The ultimate effectiveness of the department remains to be seen.

Other Organizational and Policy Changes. Reform of the intelligence community, geared toward enhancing information sharing and effectiveness in identifying and countering threats to the homeland, also took place as a result of 9/11. Signed in December 2004, the Intelligence Reform and Terrorism Prevention Act established the position of the Director of National Intelligence (DNI) to serve as

FIG. 6.1 Department of Homeland Security



Source: www.dhs.gov/xlibrary/assets/DHS_OrgChart.pdf

the president's principal advisor on intelligence matters and as the head of the U.S. intelligence community. Previously, the director of central intelligence had served in this capacity; the act essentially established an additional bureaucratic layer at the top of the intelligence structure to provide stronger centralized direction.

The Office of the DNI includes the National Counter-Terrorism Center, formally launched in December 2004 and chartered to serve as a focal point for integrating, analyzing, and disseminating terrorist-related intelligence from all U.S. sources. This integrating and information-sharing function is seen as particularly critical for counterterrorism intelligence, which may hinge on finding links between disparate bits of information from an array of sources, such as local law enforcement officers, electronic surveillance, and military forces operating abroad. Critics of intelligence reform have generally argued that the DNI has not been given adequate authority to force a truly integrated national intelligence effort; most notably, DoD intelligence organizations, which include the Defense Intelligence Agency and National Security Agency and spend approximately 80% of the country's intelligence budget, continue to operate largely outside the control of the DNI. A further discussion of the intelligence community and the role of intelligence in the national security process can be found in Chapter 7.

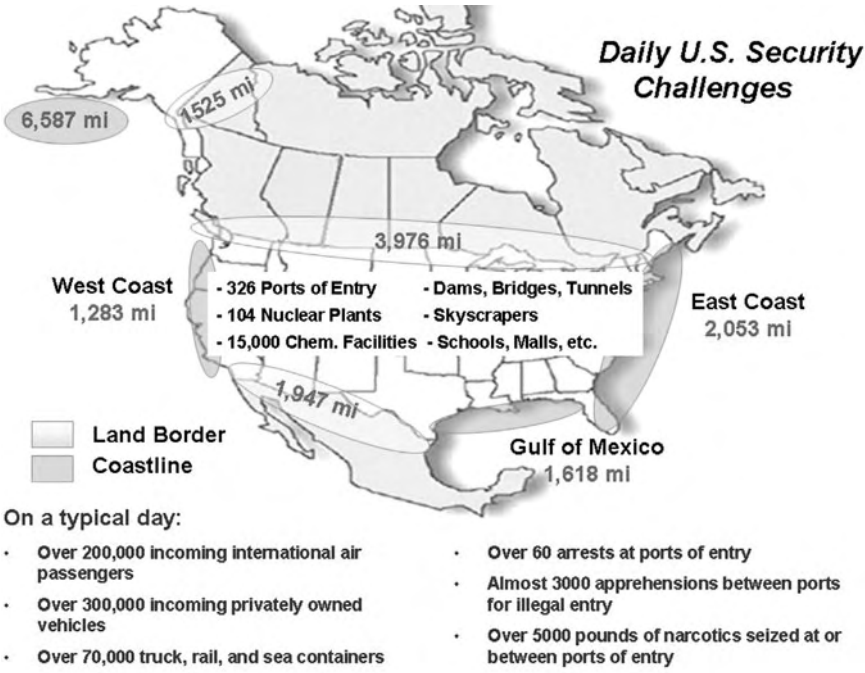
Passed during the same post-9/11 timeframe as several other major congressional initiatives and reauthorized in 2006, the Patriot Act quickly became the most publicized and debated piece of homeland security legislation. The Patriot Act expanded government authority to fight terrorism by easing some restrictions on foreign intelligence gathering in the United States, facilitating information sharing between the intelligence and law enforcement communities, defining new crimes, and streamlining processes for prosecuting terror-related crimes. Despite safeguards and the requirement for congressional oversight built into the act, opponents have charged that it does not do enough to protect individual privacy and leaves the door open for abuse.[7] Provisions of the act have been challenged with varying success in the courts, and the debate over the optimal limits of government authority in combating terrorism continues.

Taken as a whole, the enormous post-9/11 organizational, policy, and legislative reforms were designed with one purpose: facilitating rational action to protect the homeland. As discussed in the next section, however, *rational* action is difficult to define or achieve—decisions on what specific actions to take and where to allocate scarce resources to maximize homeland security must weigh many factors, and they are made in a complex political environment.

Challenges in Homeland Security Planning and Execution

Securing the homeland is fundamentally a matter of risk management, in which limited resources are applied to an essentially unlimited list of potential tasks. An open society, individual liberty, and a vibrant free market economy result in tremendous vulnerability. All levels of government must therefore make difficult choices on what to protect and how to protect it, allocating limited financial and personnel resources to deter or prevent attacks and mitigate the effects of attacks

FIG. 6.2 Daily U.S. Security Challenges



Source: Northern Command Briefing Materials, 2005

or disasters when they occur. Decisions at the federal level impact subsequent risk calculations at the state and local levels, and vice versa. And there are myriad security challenges, as reflected in Figure 6.2.

The Risk Management Process. Theoretically, the risk management process is straightforward, if complex. In deciding what to protect, homeland security risk can be conceptualized as the product of three factors:

1. *Threat:* the probability that a specific type of attack or disaster will occur, as determined by intelligence or other indicators
2. *Vulnerability:* the probability that an attack or disaster will result in damage
3. *Consequences:* the costs of an attack or disaster[8]

For example, the threat of damage from hurricanes may be highest in major cities along the Gulf Coast or Atlantic seaboard. The threat of terrorist attacks is probably higher in major metropolitan areas, such as New York City, or such cities as Washington, D.C., with higher concentrations of important symbolic targets than in less densely populated rural locations. Vulnerability is a function of variables, such as how physically hardened potential targets are, the likelihood that a

threat against an area will be discovered before an attack or disaster occurs, and the anticipated response times and effectiveness of people and organizations that could prevent or defeat an attack. Consequences may include the predicted injuries or loss of life from an attack, direct and indirect financial losses, and psychological impacts.[9] An absence of redundancy in key systems, such as electrical grids, could result in higher costs if a single critical node were destroyed.

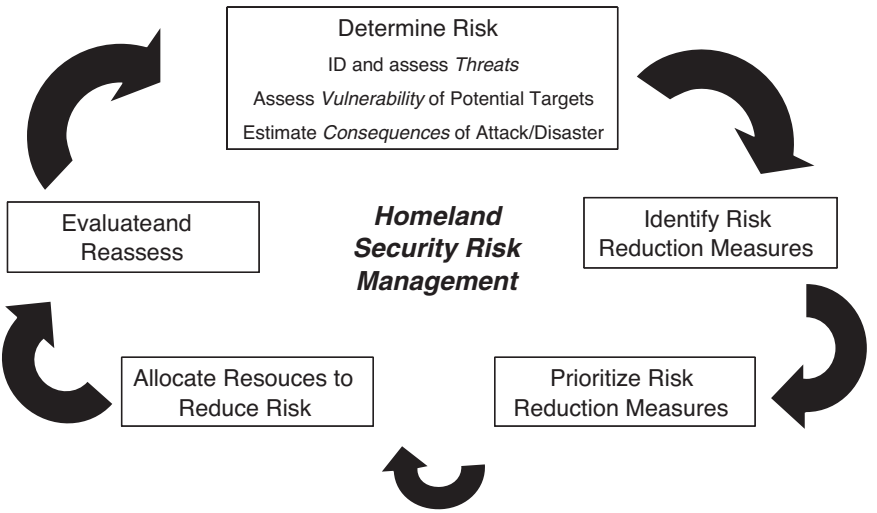
Given the observed tendency of such terrorist organizations as al-Qa'ida to seek high-profile strikes against targets of symbolic value or mass transit systems in densely populated areas, a shopping mall in suburban middle America could be characterized as having a low threat of terrorist attack using small arms and explosives (absent intelligence to the contrary). However, a lack of sizeable, well-trained security organizations and intrusive inspection procedures could make the same mall highly vulnerable—that is, an attack, if launched, would have a good chance of succeeding. The consequences of such an attack, in terms of potential loss of life and general panic, could be moderate to high. On the other hand, the threat to the Empire State Building may be high (as it fits the profile of desired terrorist targets), and the consequences of an effective attack would certainly be high, but it may be less vulnerable as a target due to existing security measures. In practice, of course, it is difficult to assign values to threat, vulnerability, and consequences and rank-order possible targets; risk management often involves as much art as science. However, such initiatives as the DHS's effort to identify and manage risk to critical U.S. infrastructure demonstrate that a reasonable assessment can be accomplished, given considerable time and attention.[10]

Once a risk assessment is complete and a rough priority of what ought to be protected is decided upon, the next logical step, which adds a significant layer of complexity, is to determine how to protect it. In other words, policy makers must then determine the most efficient and effective risk-reduction measures. For example, policy makers must decide how to apportion resources among the following tasks:

- *Reduce threat:* Deter attacks, disrupt terrorist networks that may plan attacks at a future time, or attempt to alter conditions that may increase the susceptibility of populations to radicalization and terrorist recruitment.
- *Reduce vulnerability:* Prevent or defeat attacks once they are planned or attempted, through such measures as improved airport baggage-screening procedures or enhanced intelligence sharing.
- *Reduce costs:* Mitigate the effects of attacks, for example by improving the capability of local first responders to assess damage and save lives.

George W. Bush's arguments justifying preemptive attacks to prevent states or terrorist networks from acquiring weapons of mass destruction (WMDs) were in part based on the belief that such a course would be more effective and efficient than other possible risk-reduction measures. The claim that "the greater the threat, the greater is the risk of inaction—and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time

FIG.6.3 Homeland Security Risk Management



and place of the enemy's attack" is inherently a judgment about risk-management strategy.[11]

Once potential risk-reduction measures are determined and prioritized, finite resources may be dedicated accordingly. Risk is reduced in some areas and, inevitably, accepted in others. Evaluation of the effectiveness of risk reduction measures and continuous monitoring of any changes to previous assessments of threat, vulnerability, and consequences then are used to inform future decisions. In summary, risk management for homeland security is conceptually a continuous, rational process, conducted by governments at the federal, state, and local levels, which includes the general steps outlined in Figure 6.3.

Challenges in Practice. Despite the analytical clarity of this model, in practice it is extraordinarily difficult to apply in an orderly way. Part of the reason is that, as mentioned, estimating risk and gauging the likely efficiency and effectiveness of risk-reduction measures is not a scientific process. Witness the intense debate over preemption as an integral part of homeland security strategy. Although some maintain that striking threats before attacks take place is preferable to defending at home, others claim operations abroad could breed anti-American resentment and increase the pool of potential terrorists while draining attention and resources from more productive efforts to reduce vulnerability in the homeland.[12]

Another intractable problem is that politically, homeland security presents a classic collective action dilemma.[13] As decisions are made regarding allocation of scarce resources, if political leaders at all levels attempt to secure resources for their jurisdictions (of which there are some eighty-seven thousand in the United States) rather than support a "national interest" in homeland security (especially

because this "national interest" is a difficult-to-define product of many subjective assessments and therefore easy to dispute), the result is likely to be political bargaining and a pattern of resource allocation that differs greatly from what a rational risk-management process would prescribe. Emergency responders across the nation will all want the most advanced equipment, regardless of the probability they will have to use it. Members of Congress will lobby for awarding homeland-security-related contracts to firms in their districts. Mayors will attempt to ensure that key facilities in their towns are included in lists of critical infrastructure, if inclusion means additional funding or security. The combined result will inevitably be suboptimal from a national perspective.

In fact, this predicted dynamic has been observed repeatedly in the allocation of homeland security grants. In the wake of 9/11, Congress took several actions to provide money through states to local jurisdictions to reduce vulnerabilities and enhance the ability to prevent and mitigate the effects of disasters and attacks. These included doubling funding for the Firefighter Investment and Response Enactment (FIRE) Act and authorizing the State Homeland Security Grant Program and the Urban Area Security Initiative. For each of these programs, risk did not appear to be the foremost determinant of fund distribution. For example, Montana received $9.33 per capita in FIRE grants made through February 2004, while California (a far more likely terrorist target) received $0.86 per capita; additionally, Republican (majority party) districts on balance received more FIRE funding than Democratic districts. State Homeland Security Grant Program funding included a "floor" (mandated by the Patriot Act) that ensured rural states benefited disproportionately. Even the Urban Area Security Initiative, intended to provide funding for America's fifty most vulnerable cities without any minimum distribution requirement, resulted in many grant results that seemed out of proportion to risk. For example, New Haven, Connecticut, received $77.00 per capita compared to New York City's $5.84 per capita in fiscal year 2004.[14]

Making decisions about government allocation of resources for homeland security is crucial, but homeland security action is by no means limited to government. Public and private companies, nongovernmental organizations, and individual citizens are also involved. For example, an estimated 85% of critical infrastructure in the United States is owned by the private sector. An issue area of critical importance to both security and economic prosperity is information technology and communications networks. Each nongovernmental entity must also make decisions about identifying and reducing risk, and preparedness efforts vary widely, just as they do among various state and local jurisdictions. To summarize, leaders at all levels apply a risk management process, explicitly or implicitly, in a politically charged environment that includes many public and private players and interests. The overall result is a highly complex, loosely integrated system for protecting the homeland.

Homeland Security and Civil Liberties

In addition to the factual and theoretical considerations discussed above, there is a significant normative aspect to homeland security choices. As demonstrated by

the debate over provisions of the Patriot Act, the United States maintains a dynamic balance between two fundamental and sometimes conflicting imperatives: protecting the homeland and safeguarding the freedoms upon which the country was founded. In short, the organizations, policies, and actions that may be most effective in preventing attacks on the homeland may threaten civil liberties and run counter to basic American values; however, American citizens may be willing to accept some reduction of liberty to increase their security. The result of this interplay tends to be a somewhat cyclical process in which institutions and policies to increase security are strengthened during times of perceived danger, weakened (often through enhanced congressional oversight) when liberty is unduly restricted or abuses take place, and then strengthened again if the institutions appear to be ineffective at accomplishing their missions.[15]

Taking a wide view of recent history, this cycle appears to be in evidence. In 1975 and 1976, the U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee) conducted an investigation that led to several significant recommendations to limit the power of intelligence agencies and draw a clearer line between intelligence and law enforcement. This use of congressional oversight was a response to FBI actions, including unauthorized searches and electronic surveillance, used to monitor and disrupt domestic dissident groups. It also resulted from the conclusion that the Central Intelligence Agency (CIA) had engaged in unauthorized domestic activities and gone too far in conducting covert operations abroad. The Church Committee's recommendations helped produce the Foreign Intelligence and Surveillance Act of 1978, which established procedures and restrictions on gathering foreign intelligence information. (This act was modified by the Patriot Act in 2001.)

During the early years of the Reagan administration (1981–1985), CIA covert operations, especially in Central America and Afghanistan, again grew in frequency and significance. In 1986, revelations that the NSC staff had coordinated a program to provide aid to the Contra rebels in Nicaragua using profits from arms sales to Iran (in clear violation of congressional intent) led to a new wave of congressional oversight regarding covert operations and intelligence activities.

Many have charged that, during the 1990s, the CIA's human intelligence capability was overly curtailed in favor of technological means of collection, policies on recruiting foreign agents were too restrictive, and the line between intelligence and law enforcement became a barrier to reasonable information sharing. The country's inability to discover and stop the 9/11 attacks has been attributed in part to these shortcomings. The perception of increased danger following 9/11 then provided an environment conducive to passage of the Patriot Act.

Much of the "liberty versus security" discussion also hinges on expectations. What is an acceptable level of violence for the United States, and what financial and nonmonetary costs are the public willing to pay to achieve this standard? The United States suffers over forty thousand fatalities due to automobile accidents and over fifteen thousand murders each year; absent major efforts to reduce them, these numbers appear acceptable from a macro perspective. If the expectation is

that the country should never again experience a fatal terrorist attack, deterrence and prevention activities would logically demand great sacrifice in terms of resources and limitations on personal freedom. If the country is willing to live with low levels of terrorist violence and infrequent major attacks, the calculus changes significantly. Leaders thus face the difficult task of gauging the public's demand for security (and willingness to bear the costs to achieve it), developing policies and allocating resources in accordance with this demand, and attempting to ensure that public expectations are aligned with the realities of risk management. The dissonance of messages along the lines of "a future attack is inevitable, but we don't need to make radical changes to our daily lives" is understandable in this context. The unsteady American equilibrium between maintaining civil liberties and protecting the homeland will be a permanent aspect of the political environment in which homeland security decisions are made.

Homeland Security Issue Areas

Is the United States safer now than it was before 9/11? In addition to making the major organizational changes discussed above, the U.S. government has focused on increasing its capability to reduce homeland security risk through programs and plans in several specific areas. Assessments of progress have been mixed, with many critics arguing that many important homeland security initiatives have still not received adequate resources or attention.[16] This section outlines efforts to counter two of the more significant threats: terrorist attacks using nuclear devices and an outbreak of pandemic influenza. These examples illustrate many of the challenges of securing the homeland covered throughout this chapter.

Nuclear Terrorism. In July 2004, the HSC, in partnership with the DHS, published a list of fifteen all-hazards scenarios for use in federal, state, and local homeland security preparedness planning and other activities.[17] Scenario 1 is "Nuclear Detonation—10-Kiloton Improvised Nuclear Device" in a large city. Estimates of fatalities from such an attack range into six figures; treating hundreds of thousands of injuries and decontaminating up to thousands of square miles would make for a very difficult, costly recovery period. These enormous costs, in light of the threat posed by transnational terrorist organizations that have attempted or stated their intent to acquire nuclear material, make preventing this scenario a clear priority in any homeland security risk-management system.

The U.S. approach to countering the possibility of nuclear terrorism includes a mix of interrelated actions to reduce the threat, vulnerability, and consequences of an attack. In terms of reducing threat, operations to kill or capture terrorists abroad, combined with international efforts to disrupt terrorist financing and enhanced domestic surveillance and information sharing, are designed to reduce the ability of transnational terrorist networks to plan and execute operations against the United States. These actions are, in theory, integrated into a broader diplomatic, informational, military, and economic strategy to lower motivation for anti-American terrorism, especially among radical Islamist groups.

With regard to the specific threat of nuclear terrorism, most major U.S. policies and programs have been designed to reduce vulnerability. Conceptually, a terrorist group attempting to execute this type of attack must perform several general functions, not necessarily in this exact order: acquiring nuclear material, building a workable device, delivering it (and, if necessary, operatives) to the United States, planning and organizing for the attack, and carrying it out. The likelihood that a potential attack will succeed can be reduced by making any of these functions more difficult.

Preventing terrorist acquisition of nuclear material or nuclear weapons requires close international cooperation, and the United States has developed several major programs to this end. The Cooperative Threat Reduction (CTR) Program, established in its original form in 1991, is designed to provide funding and expertise to prevent the spread of WMDs and related materials, technologies, and expertise from former Soviet states. The Global Threat Reduction Initiative, launched in 2004, is a similar effort to secure vulnerable nuclear and radiological materials worldwide. Related bilateral and multilateral agreements, such as the 2006 Global Initiative to Combat Nuclear Terrorism and the 2005 U.S.-Russian Bratislava Nuclear Security Cooperation Initiative, also seek fundamentally the same objective—keeping nuclear material out of terrorist hands.

Should these international efforts fail, the next objective is preventing delivery of nuclear weapons or materials to the United States; this could be accomplished at the point of embarkation, in transit, or at the U.S. border. The Container Security Initiative, in place at over forty major international seaports, allows for but does not ensure prescreening of most cargo containers bound for the United States. The Department of Energy's Second Line of Defense Program provides radiation-detection equipment to key foreign airports, seaports, and borders. The Domestic Nuclear Detection Office, established within the DHS in 2005, is responsible for developing and planning for employment of radiological-detection technology in the United States. The amount of cargo scanned at U.S. ports of entry has been increased dramatically but is still, as of 2007, far from sufficient.

As a complement to programs targeted at finding nuclear materials, enhanced border security measures and immigration policies may prevent the movement of terrorists to the United States. Under the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, almost all visitors to the country provide digital finger scans and digital photographs, which are checked against terrorist-related watch lists. All applicants for U.S. visas are similarly screened. Especially along the U.S.-Mexican border, improved—but still inadequate—security infrastructure, such as fencing and detection capability, seeks to make illegal entry more difficult. Operation Jump Start in 2006 saw the deployment of approximately six thousand National Guard troops to the four southwest border states to assist the growing border patrol by providing surveillance, infrastructure development, and logistical support.

If terrorists nevertheless manage to bring nuclear material to the United States, the onus for preventing an attack shifts to law enforcement organizations at the federal, state, and local levels. There are approximately eight hundred thousand

full-time sworn law enforcement officers in the country; the major challenge facing them is sharing intelligence and connecting disparate bits of information that may reveal a planned attack. The FBI's National Joint Terrorism Task Force and a system of smaller Joint Terrorism Task Forces in one hundred major cities (including over thirty-five hundred members, over four times the pre-9/11 number) are designed to perform part of this role.

Should a nuclear or radiological attack succeed, as for other major attacks or disasters, the DHS would have overall responsibility for coordinating the national response to mitigate its effects. The National Response Plan, discussed in more detail below, includes a Nuclear/Radiological Incident Annex outlining responsibilities for major actions. Recent years have seen a growth in national, state, and local capability for nuclear incident response, with funding provided through such sources as the DHS Homeland Security Grant Program. In addition, the National Guard is fielding WMD Civil Support Teams in each state and territory to support initial consequence management operations if required.

Overall, this diverse array of U.S. actions to counter the threat of nuclear terrorism provides an instructive example of the sort of layered, interconnected planning required in many homeland security areas. The strategy involves a complicated system of responsibilities and activities at the international, federal, state, and local levels. Given limited resources, prioritizing is an essential task, especially because each agency and jurisdiction is likely to argue for the criticality of its role. Many critics of the U.S. effort against nuclear threats maintain that international initiatives, such as the CTR Program, have been underemphasized relative to their importance, because stopping terrorists from acquiring nuclear materials in the first place may be the most effective way to prevent an attack.[18]

As with all homeland security choices, measures to prevent nuclear terrorism come at a price: Intrusive or time-consuming inspection procedures hinder the flow of commerce; overly restrictive immigration policies run counter to America's political culture as a country of immigrants; and effective domestic surveillance measures risk violating individual liberties. Weighing these factors against the catastrophic cost of failure calls for delicate judgment.

Pandemic Influenza. Although the thrust of U.S. efforts regarding nuclear terrorism has largely been on prevention through international cooperation, enhanced detection capability, and border control measures, countering an outbreak of pandemic influenza is primarily a problem of mitigation. Many analysts fear that a type-A strain of influenza virus capable of efficient and sustained human-to-human transmission will develop. If this occurs, completely preventing its spread would not be possible.

The human and economic consequences of an influenza pandemic could be catastrophic. The Spanish Flu pandemic of 1918 caused over five hundred thousand deaths in the United States (including over forty-three thousand U.S. military service members) and over 50 million fatalities worldwide. Estimates of possible U.S. fatalities if an outbreak of avian influenza occurs in the near future, likely through multiple waves of infection, range well into the hundreds of thousands.

Many more people would become ill, and work absenteeism would severely hamper economic productivity. As opposed to most sudden attacks and natural disasters, an avian influenza pandemic would cause a sustained public health emergency requiring a well-coordinated response over the course of several months.[19]

The U.S. approach to pandemic influenza centers on dampening these effects by limiting the spread of the disease to and within the United States and taking action to minimize its health, social, and economic impacts. In November 2005, George W. Bush published the *National Strategy for Pandemic Influenza*, which was augmented by a more detailed implementation plan in May 2006. The strategy calls for a massive cooperative effort among a complex and diverse group of international, federal, state, local, and private-sector organizations.

Internationally, the World Health Organization (with considerable financial and planning support from the United States) is the United Nations agency responsible for coordinating the global response to human cases of avian influenza. Major responsibilities include providing early diagnosis and warning of an outbreak, containing an outbreak if and when it occurs, and coordinating research and planning efforts to increase worldwide capacity to cope with a pandemic.

Within the United States, under the overall lead of the DHS, the Department of Health and Human Services is assigned responsibility for coordinating the U.S. public health response. Its major tasks include providing assessments and guidance to state and local agencies and the public and managing the national effort to create and distribute vaccines. Other key federal players include the Department of State, responsible for coordinating U.S. involvement in the international response; the Department of Agriculture, responsible for veterinary response and food safety; the Department of Transportation, responsible for managing the country's transportation system to limit the spread of disease while preserving economically essential movement; and the DoD, responsible for providing assistance as required to maintain public order, distribute vaccines, and continue essential government services. The 2006 implementation plan includes over three hundred specific tasks for federal agencies; monitoring performance and ensuring all agency efforts are complementary is an enormous management challenge.

Federal plans and programs notwithstanding, effective response to limit the impact of pandemic influenza will hinge on state, local, and private-sector efforts. Prioritizing recipients of vaccines, planning for the continued delivery of such essential government services as law enforcement, and maintaining key infrastructure and systems remain largely state responsibilities. As with natural disasters and other emergencies, however, state autonomy often leads to considerable variation in the approach and quality of plans. Specifically, state plans for detection and monitoring, vaccination, and containment in case of a pandemic influenza outbreak are, in many cases, inconsistent.[20] Similar dynamics also occur with local and private-sector efforts, adding to the coordination challenge.[21] Homeland security decision makers must weigh the requirement for coherent national action against the benefits of allowing lower jurisdictions to shape a strategy that addresses their unique circumstances.

The challenge of ensuring unity of effort is compounded by the fact that there are many unknowns involved in pandemic influenza planning. The time and place of outbreaks, the virulence of the disease, the effectiveness of vaccines, and the reaction of the public cannot be determined in advance; disagreements over planning assumptions are inevitable. In addition to these factual issues, an outbreak of pandemic influenza would present difficult normative choices. Questions of who should receive limited vaccines and what restrictions on travel and other personal liberty would be acceptable in trying to limit the spread of disease will have great political consequences.

The Utility of Homeland Security Planning. The threats of pandemic influenza and nuclear terrorism are representative of the breadth and complexity of most major homeland security issues. Thinking in detail about these scenarios, actions, and systems designed to reduce the risks of nuclear terrorism or pandemic influenza may also be helpful in addressing other threats; most homeland security functions are not threat specific. For example, border control measures that make it more difficult for terrorists to bring nuclear material into the country may also reduce vulnerability to other types of terrorist attacks or slow the influx of illegal drugs. Systems for providing medical care to victims of an influenza outbreak may be equally useful following natural disasters or other mass-casualty events, especially bioterrorist attacks. In addition, planning, coordination, and exercises among the many agencies and jurisdictions with a stake in preventing nuclear terrorism or limiting the impact of pandemic influenza may facilitate cooperation on other homeland security issues.

One agency with critical responsibilities and interests in almost all homeland security scenarios is the DoD. The next section will explore its involvement in protecting the homeland in greater depth.

The Military's Role

Since the days of colonial militias, American military forces have played a prominent, continuous role in securing the homeland against state and nonstate threats and in providing internal order when required. In addition to more traditional roles, such as fighting in the War of 1812 and the Civil War, conquering American Indian tribes, and providing coastal defense, military forces have been employed in the homeland to suppress rebellions and riots, explore the American West, put down strikes, enforce school desegregation, and respond to the full gamut of natural and man-made disasters. Despite American unease with using military forces (especially regular forces) in domestic roles, their manpower, resources, planning capability, and surge capacity ensure that they will always be considered as an option when nonmilitary security and relief organizations appear inadequate.[22]

The Creation of NORTHCOM. As with homeland security in general, the national reaction to the 9/11 attacks involved a more focused debate on the desired

role of the military and led to rapid organizational change. The major development was the creation in October 2002 of U.S. Northern Command (NORTHCOM), a combatant command with responsibility for a geographic area including the United States, Canada, Mexico, the Gulf of Mexico, and portions of the Atlantic and Pacific oceans. NORTHCOM is charged with deterring, preventing, and defeating threats to U.S. territories and interests within this area and providing assistance to U.S. civil authorities as directed. The former role is known as *homeland defense*, the latter as *civil support*.[23]

In its brief history, NORTHCOM has further defined and planned for its homeland defense responsibilities while executing multiple civil support operations. Many missions are conducted in close coordination with North American Aerospace Defense Command (NORAD), the U.S.-Canadian organization responsible for aerospace warning and aerospace control for North America. NORTHCOM's civil support tasks have included supporting the National Interagency Fire Center in fighting wildland fires, providing security for such high-profile national events as presidential inaugurations and national political conventions, and offering detection and monitoring assistance to federal agencies interdicting drugs and other illicit traffic across U.S. borders. Major actions related to homeland defense have included the designation of quick-reaction land forces to respond to threats, enhancement of the awareness of potential maritime threats through better information sharing, preparation to fire ground-based interceptors as part of the emerging ballistic missile defense system, and deployment of an integrated air defense system for the Washington, D.C., area. Forces that may be necessary for NORTHCOM operations, both those permanently assigned as well as those assigned for specific missions, are kept at various stages of alert based on intelligence about potential threats.

Considerations for Domestic Use of the Armed Forces. Refining the capability to conduct effective military operations in and near the homeland is part of a broader strategy of creating a layered, in-depth defense for the United States. Given the choice, it would normally be more desirable to engage threats abroad, before they reach the homeland. Of course, it may not be possible to detect or defeat all threats outside U.S. territory, and some threats may not be apparent until an attack is imminent. In these cases, an appropriate response may require action by law enforcement organizations, the DHS, the military, or a combination. When the employment of military forces is necessary, operating in the U.S. homeland presents at least three unique challenges.

Legal and Policy Restrictions. The first challenge is that, resulting from traditional American concerns, there are significant legal and policy restrictions on the domestic use of military forces. One commonly cited example is the Posse Comitatus Act of 1878, as amended[24]:

> Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.

Originally intended to prevent local sheriffs and U.S. marshals from using federal troops to enforce the law in the South, the Posse Comitatus Act in effect restricts the ability of active-duty forces to act in a law-enforcement capacity. There are important exceptions, however. Most notably, Congress has long authorized the president, through the Insurrection Act of 1807 (broadened in 2006 and renamed the Enforcement of the Laws to Restore Public Order Act), to use federal troops to restore public order under a variety of circumstances, and federal troops have been authorized in law to assist civil authorities in some counterdrug operations and disasters involving WMDs.[25]

There are also legal and policy restrictions on the use of military assets for domestic intelligence collection and storing of information on U.S. persons. In general, domestic military intelligence activities are limited to analysis of information gathered by other sources to anticipate potential homeland defense threats. Even for actions unrelated to intelligence, government policy limits the ability of military commanders to employ forces domestically. Although they vary with the level of threat, systems for authorizing movement of forces and engagement of threats in the U.S. homeland generally require approval at high civilian levels. For civil support operations, such as disaster relief, authorization by the president or secretary of defense is required for federal forces to act.

Interagency Cooperation. The second challenge for military operations in the homeland is that, to a much greater degree than for actions abroad, federal forces are unlikely to ever operate alone; domestic missions will inevitably involve a large group of other federal, state, and local organizations, and the federal military does not have lead responsibility in most cases. The DHS and multiple law enforcement agencies are frequent partners, and the National Guard is likely to be involved in any major domestic operation. In responding to emergencies or providing security for designated events, the National Guard generally acts under the control of state governors, which is referred to as State Active Duty or Title 32 status (Title 32 refers to the title of the U.S. Code that pertains to the National Guard. It is in contrast to Title 10 of the U.S. Code, which pertains to federal armed forces). The advantage of this arrangement is that National Guard forces retain law enforcement authority when they are not federalized—Posse Comitatus Act restrictions only apply to federal (Title 10) forces. However, coordination challenges may result when separate chains of command for state and federal forces are in place, making unity of effort harder to ensure. The following chart provides a basic comparison of command and control, funding, and law-enforcement capability for troops in a Title 10, Title 32, and State Active Duty status (see Table 6.1).

Table 6.1 Military Forces: Duty Status Comparison

	Command and Control	*Funding*	*Law Enforcement Authority*
Title 10 (Active Duty and Federalized Forces)	President and secretary of defense	Federal	No (Posse Comitatus Act applies)
Title 32	State governor	Federal	Yes
State Active Duty	State governor	State	Yes

The fundamentally interagency nature of homeland defense and civil support operations places a special premium on effective interagency cooperation, which is often difficult to achieve. Government organizations are frequently concerned with guarding their autonomy and minimizing uncertainty; therefore, they are often reluctant to enter into interdependent relationships or cede control over their activities to others.[26] Realistic homeland security and homeland defense exercises involving all major players, the extensive use of liaisons, and frequent communications between military and civilian organizations are needed to strengthen cooperation in deterring, preventing, defeating, or mitigating the effects of attacks and disasters.

The Need for Unique Capabilities. The third challenge is that the probable types of military operations in the homeland call for a somewhat different set of capabilities than combat operations abroad. If detected in time, the most likely terrorist threats could be defeated without placing a large strain on military capabilities, but any use of military force for homeland defense would have to take significant political sensitivities into account. A great degree of precision and limitation of collateral effects, rather than application of a blunt instrument, would generally be required. For example, if military forces were directed to shoot down a hijacked civilian airliner or defend a base against attack, limiting damage in the area would be critical. Troops deployed to restore order in an area with widespread rioting would face the challenge of minimizing casualties and avoiding the use of lethal force when possible.

In addition, homeland defense operations are likely to be extremely time sensitive. If threats are not detected until an attack is ongoing or imminent, an effective response would demand having trained and ready forces on short alert. Finally, military forces must be prepared and equipped to assist with a variety of consequence management scenarios in the homeland. If an attack with a WMD succeeds, elements of the U.S. Armed Forces would undoubtedly be called on to help mitigate its effects. Development of the types of military capabilities that may be required in the homeland—precision engagement; rapid response capacity; enhanced detection and tracking systems; and the ability to respond to chemical, biological, radiological, and nuclear attacks or disasters—requires the dedication of financial resources and training time.

Case Study: Hurricane Katrina Relief and the National Response Plan

The response to Hurricane Katrina reveals many of the issues that will likely face the United States in any scenario involving preparedness for and response to major natural or man-made disasters. A brief overview of the case provides a useful illustration of the challenges of homeland security planning and execution described in this chapter.

Katrina, which ravaged the city of New Orleans as well as large swaths of the Mississippi and Alabama coast on August 29, 2005, was the costliest natural disaster in U.S. history. It resulted in over $80 billion in property damage, including

approximately three hundred thousand destroyed or severely damaged homes. The hurricane caused over eighteen hundred deaths and displaced approximately seven hundred seventy thousand people. The disaster occurred *after* many relevant reforms had recently been made: The DHS had been created, the National Incident Management System and National Response Plan were published in 2004 (together, these provide a framework for managing disaster preparation and response activities across all levels of government), and NORTHCOM had been created to plan and execute military civil support operations. Nevertheless, the government response to Katrina was widely and rightly criticized.

Reflecting the U.S. federal system of government, the National Response Plan essentially establishes a *bottom up* or *pull* model for disaster response. By design, local and state leaders request federal assistance when their resources are exhausted or overwhelmed. Federal assistance is provided through emergency support functions, such as transportation, communications, and urban search and rescue, each led by the appropriate federal agency and coordinated by interagency centers at the local through national level. Agencies request support from other federal organizations, including the DoD, as required to implement their emergency support functions.

In the case of Katrina, the magnitude of the initial damage and especially the flooding resulting from levee breaks in New Orleans prevented a rapid, comprehensive assessment of needs. Local, state, and federal organizations could not accurately describe the assistance they required. This problem was exacerbated by the breakdown in communication infrastructure and power supply during the critical days after Katrina's landfall. As a result, there were well-publicized delays in relief reaching the affected areas, which led to additional suffering and increased civil disorder. There was a three- or four-day gap between the presidential disaster declaration for Louisiana on August 29 and specific formal requests for federal assistance from the state. Significant relief for the approximately nineteen thousand people at the Morial Convention Center did not begin until September 2.

Another explanation for the delays was that FEMA, the DHS organization primarily responsible for the coordination of the federal response to disasters, was overwhelmed by the massive scale of Katrina and unable to deploy adequate command and control capability and basic supplies (such as food, water, and ice) in a timely manner. According to most assessments, whether through lack of staffing, planning, or leadership, FEMA was simply not up to the task of quickly coordinating the enormous relief effort. This effort involved many government organizations and civilian relief organizations, such as the American Red Cross and Salvation Army, that also bring response and recovery resources to devastated areas.

As is normal for any large disaster, the military was called upon to bring its comparative advantage in deployable manpower and large-scale logistical capability to bear following Katrina. More than twenty thousand active troops and fifty thousand National Guard troops from all fifty-four states and territories were involved in the operation, primarily in Louisiana and Mississippi. Among other tasks, they performed search-and-rescue missions in coordination with the U.S.

Coast Guard, provided medical care, established air traffic control for the area, and moved and distributed humanitarian relief supplies. Despite the magnitude of this effort, the speed and coordination of the military response also received criticism. Joint Task Force Katrina, built around the First U.S. Army, was activated on August 31, and military leaders acted on guidance to "lean forward" as much as possible by positioning supplies and equipment in the area without specific requests. However, significant numbers of active-duty ground troops did not reach New Orleans until September 6. Just as some of the FEMA delay was due to the lack of clear requests from the affected states, a large part of the delay in employing military assets can be attributed to the absence of clear requests for assistance from FEMA. A response system that relies on requests from local, state, and federal organizations will not work optimally if those requests are not timely and accurate.

The military response was also marked by inadequate coordination between active-duty forces and the National Guard, which operated under control of the state governors in a State Active Duty and then a Title 32 status. There was only a relationship of coordination between commanders of active forces and the State Adjutants General that commanded National Guard troops, and nothing mandated that these distinct chains of command exchange information. Especially given the complexity and time sensitivity of the initial response, it is unsurprising that the efforts of active and National Guard troops were not always complementary. For example, there were anecdotes of search-and-rescue teams from both components going to the same locations while other citizens waited for rescue, and lower-level leaders often did not have a clear picture of what units were near them and what missions they were performing. Maintaining separate chains of command has advantages. National Guardsmen in a Title 32 status retain some law enforcement authority, and the governor retains the ability to direct his or her state's troops, which may be politically important. However, the disadvantage is that separate chains of command will always create a coordination challenge, especially in a crisis situation. Coordination challenges are exacerbated if the ultimate commanders of the components—the president for Title 10 forces and the governors for Title 32 forces—do not agree on priorities for military action.

Although there is certainly much to criticize in the local, state, and federal preparation and response to Katrina, many of the difficulties resulted from the bottom-up National Response Plan model being overwhelmed by the historically rare scale of the disaster. For the vast majority of incidents, however, this model is effective, and it is a logical fit for a federal system of government. Reversing it and guaranteeing immediate federal assistance for all disasters could run the risk of reducing the incentive for local and state jurisdictions to plan and prepare for disaster response.

Much of the analysis of Katrina has centered on recommendations to anticipate and improve plans for circumstances in which a disaster is so catastrophic that federal assistance, including military aid, is immediately pushed to affected areas.[27] These plans may be especially important in the case of a no-notice terrorist attack, such as a nuclear detonation in a populated area, or a natural disaster, such as a major earthquake. For hurricanes, though precise damage cannot always be

estimated, there is at least some warning and a preparation period when evacuations can be ordered and supplies pre-positioned.

The debate on the homeland security issues raised by Katrina will certainly continue. In the end, decisions about assigning responsibility for disaster preparedness and response in a federal system, allocating resources, and defining the desired role of active-duty and state military forces will always be subject to the same types of risk-management and political considerations that influence all homeland security efforts.

Enduring Considerations

The specific issues and threats at the top of the U.S. homeland security agenda will vary over time; however, the fundamental factors that make protecting the homeland such a difficult task will persist. These considerations define the environment in which homeland security choices are made.

Vulnerabilities will always exceed homeland security capability in a free society. The number of potential targets in the United States and the amount of traffic entering the country by land, sea, and air make it impossible to defend everywhere against any potential threat.

Even in a political vacuum, risk-management processes are hard to apply in making homeland security choices. If threats, vulnerabilities, and consequences can be agreed upon, which is no easy task, resources can still be applied in very different ways in terms of function (deter, prevent, defeat, or mitigate the effects of attacks and disasters), location (the homeland, approaches to the homeland, or abroad), and jurisdiction (local, state, federal, or international). There is considerable room for reasonable people to disagree on risk-mitigation strategies.

Political leaders making homeland security choices will often favor their constituencies rather than a national perspective. Decisions regarding homeland security grants and other homeland security actions are subject to the same considerations of distributional politics that accompany all federal, state, and local governmental-spending decisions.

Homeland security requires action by a huge number of public and private organizations, each of which has its own organizational interests. The country's federal system of government ensures that preparation for and response to attacks and disasters inevitably involves many players at the local, state, and federal levels. Even if they agree in general terms on a common goal, effective cooperation among large bureaucratic organizations is difficult to achieve. Concerns over guarding autonomy, reducing uncertainty, and increasing resources play a powerful role in shaping organizational behavior.

The military will always have a role in the homeland, and the country is likely to remain uneasy with it. Unless resources spent on homeland security are radically increased, some problems (such as major natural disasters or attacks with nuclear, biological, chemical, or radiological weapons) will require capabilities that only the U.S. Armed Forces can bring to bear. Especially in the case of federal forces operating in the homeland, traditional U.S. unease will

persist, and any major action is likely to renew debates about the military's proper role.

The optimal balance between securing the homeland and safeguarding civil liberties will remain a contentious issue. Shifts in either direction will continue to occur, in large part based on the level of threat the American public perceives and the amount of security it demands. Each shift will also be hotly debated. In a democratic state, founded upon individual freedoms and confronted by new threats and challenges, this dynamic is both inevitable and appropriate.

Discussion Questions

1. What is the acceptable level of loss to terrorist attacks for the American people, and how does it vary over time?
2. How is the acceptable level of risk shaped by U.S. willingness to pay associated financial and nonmonetary costs?
3. What principles should guide decisions about allocation of scarce resources for homeland security? Which functions (deter, prevent, defeat, mitigate), types of threat, and locations (local, state, federal, abroad) should be favored?
4. What are the most significant barriers to application of a rational risk-management process to homeland security choices, and how can they best be mitigated?
5. What lessons from the post-9/11 reorganization of government should guide similar actions in the future?
6. Do law enforcement and intelligence agencies have adequate tools to counter threats to the homeland? How should their powers be limited to protect civil liberties?
7. Is the National Response Plan model for disaster response appropriate, and what (if any) changes should be made to it?
8. What role should the U.S. military—both active and Reserve Component forces, including the National Guard—play in homeland security? Should the military be given a more significant role following catastrophic incidents?

Recommended Reading

Brinkerhoff, John R. "The Posse Comitatus Act and Homeland Security." *Journal of Homeland Security* (Feb 2002). www.homelandsecurity.org/newjournal/articles/brinkerhoffpossecomitatus.htm.

Eisinger, Peter. "Imperfect Federalism: The Intergovernmental Partnership for Homeland Security." *Public Administration Review* 66, no. 4 (July/Aug 2006): 537–545.

Flynn, Stephen. *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism.* New York: Harper Collins, 2004.

Howard, Russell D., James J. Forest, and Joanne C. Moore. *Homeland Security and Terrorism: Readings and Interpretations.* New York: McGraw-Hill, 2006.

Huntington, Samuel P. "American Ideals Versus American Institutions." In *American Foreign Policy: Theoretical Essays*, 2nd ed., edited by G. John Ikenberry, 251–283. New York: HarperCollins College Publishers, 1996.

Kohn, Richard H. "Using the Military at Home: Yesterday, Today, and Tomorrow." *Chicago Journal of International Law* 4, no. 1 (Spring 2003): 165–192.

Maxwell, Bruce. *Homeland Security: A Documentary History.* Washington, DC: CQ Press, 2004.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report.* Washington, DC: U.S. Government Printing Office, 2004.
Nicholson, William C., ed. *Homeland Security Law and Policy.* Springfield, IL: Charles C. Thomas, 2005.
Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Groups.* Cambridge, MA: Harvard University Press, 1965.
Sauter, Mark A., and James J. Carafano. *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism.* New York: McGraw-Hill, 2005.
White, Jonathan R. *Defending the Homeland.* Belmont, CA: Wadsworth, 2004.
The White House. *The Federal Response to Hurricane Katrina: Lessons Learned.* Washington, DC: The White House, February 2006.
Willis, Henry H., Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby. *Estimating Terrorism Risk.* Santa Monica, CA: RAND Corporation, 2005.
Wilson, James Q. *Bureaucracy: What Government Agencies Do and Why They Do It.* New York: Basic Books, 1989.

Internet Resources

Homeland Security Council, www.whitehouse.gov/hsc
Homeland Security Institute, www.homelandsecurity.org
U.S. Department of Homeland Security, www.dhs.gov
U.S. Government Accountability Office, Homeland Security Reports, www.gao.gov/docsearch/featured/homelandsecurity.html
U.S. Northern Command, www.northcom.mil