Intelligence and Warning

Terrorism depends on surprise. With it, a terrorist attack has the potential to do massive damage to an unwitting and unprepared target. Without it, the terrorists stand a good chance of being thwarted by authorities, and even if they are not, the damage from their attacks is likely to be less severe.

It follows that the United States must take every appropriate action to avoid being surprised by another terrorist attack. To secure the homeland, we must have an intelligence and warning system that is capable of detecting terrorist activity before it manifests itself in an attack so that proper preemptive, preventive, and protective action can be taken.

This is not the first time in American history that we have had to focus on our early warning capabilities. The Japanese attack on Pearl Harbor on December 7, 1941, demonstrated the catastrophic consequences of allowing an enemy to achieve even tactical surprise. With the dawn of the nuclear age, early warning became essential to national survival. The United States spent billions of dollars during the Cold War on ground- and space-based sensors that had one principal, overriding purpose: to detect indications of a nuclear attack by the Soviet Union. These early warning systems were the foundation for strategic nuclear deterrence because they provided the President sufficient lead-time to make retaliatory decisions.

Early warning of an impending terrorist attack is a far more difficult and complex mission than was early warning of a strategic nuclear first strike. Whereas we almost always know the identity, location, and general capabilities of hostile nations, we frequently do not know the identity or location of non-state terrorist organizations. The indications of terrorist intent are often ambiguous. Terrorists are able to infiltrate and move freely within democratic countries making themselves effectively invisible against the backdrop of an enormously diverse and mobile society. Efforts to gather intelligence on potential terrorist threats can

affect the basic rights and liberties of American citizens.

Moreover, the question of how to achieve early warning of terrorist threats is inseparable from the question of what to do with some warning information once it is in hand. What preventive action should be taken? What protective action should be taken? To whom should the information be provided on a confidential basis? Should the public be informed and, if so, how and by whom? These very concrete decisions can have life-or-death implications. Unfortunately, the ambiguous nature of most intelligence on terrorist threats means that these decisions must often be made in conditions of great uncertainty.

America's intelligence community has made significant contributions to our national security and is now making adjustments to help meet the increased needs for homeland security. At present, we have insufficient human source intelligence developed overseas about potential terrorist activities in the United States. Agencies at all levels of government have not always fully shared homeland security information due to real and perceived legal and cultural barriers, as well as the limitations of their information systems. The United States needs to do a better job of utilizing information contained in foreign-language documents that we have obtained. In addition, our intelligence community must identify, collect, and analyze the new observables that will enable us to better understand emerging unconventional threats.

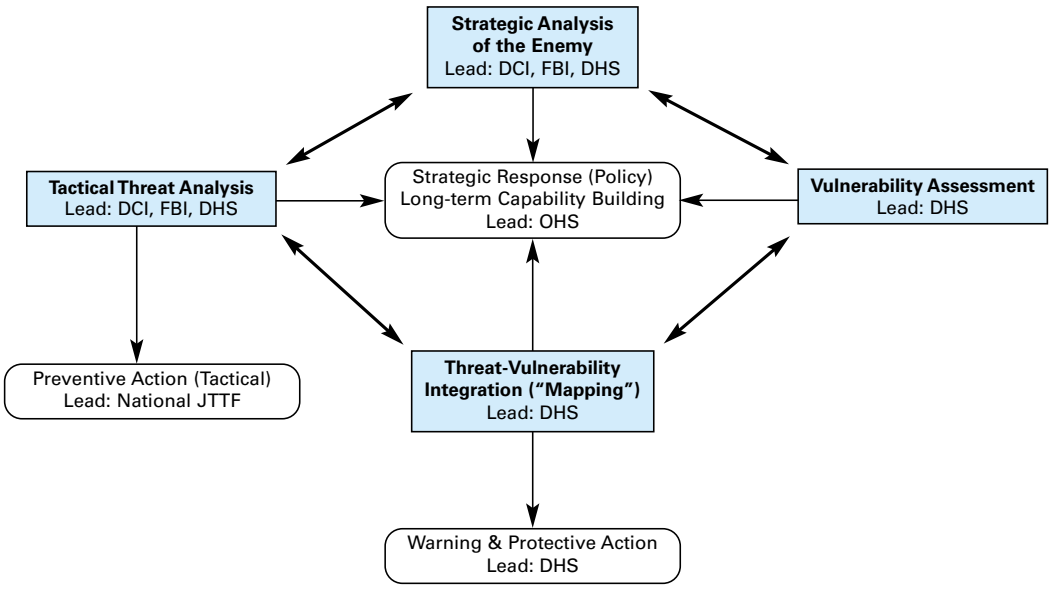
The *National Strategy for Homeland Security* reflects the concept that intelligence and information analysis is not a separate, stand-alone activity but rather an integral component of our Nation's overall effort to protect against and reduce our vulnerability to terrorism. The basic roles and responsibilities in this *Strategy* are depicted in Figure 1.

This framework recognizes four interrelated but distinct categories of intelligence and information analysis, as well as three broad categories of actions that can follow from this analysis. The analytic categories are as follows.

Tactical threat analysis. Actionable intelligence is essential for preventing acts of terrorism. The timely and thorough analysis and dissemination of information about terrorists and their current and potential activities allow the government to take immediate- and near-term action to disrupt and prevent terrorist acts and to provide useful warning to specific targets, security and public safety professionals, or the general population.

Strategic analysis of the enemy. Our intelligence agencies must have a deep understanding of the organizations that may conduct terrorist attacks against the United States. Knowing the identities, financial and political sources of support, motivation, goals, current and future capabilities, and vulnerabilities of these organizations will assist us in preventing and preempting future attacks, and in taking long-term actions that can weaken support for organizations that seek to damage U.S. interests. Intelligence agencies can support the long-term U.S. strategies to defeat terrorism by understanding the roots of terrorism overseas, and the intentions and capabilities of foreign governments to disrupt terrorist groups in their territories and to assist the United States.

Roles & Responsibilities of Homeland Security Intelligence and Information Analysis



Vulnerability assessments. Vulnerability assessments must be an integral part of the intelligence cycle for homeland security issues. They allow planners to project the consequences of possible terrorist attacks against specific facilities or different sectors of the economy or government. These projections allow authorities to strengthen defenses against different threats. Such assessments are informed by the use of tools such as computer modeling and analysis.

Threat-Vulnerability integration. Mapping terrorist threats and capabilities—both current and future—against specific facility and sectoral vulnerabilities will allow authorities to determine which organizations pose the greatest threats and which facilities and sectors are most at risk. It will also allow planners to develop thresholds for preemptive or protective action.

Figure 1 also depicts three broad categories of action that can result from this analysis.

Tactical preventive action. Analysis can, and must, be turned into action that prevents terrorists from carrying out their plots. The United States has at its disposal numerous tools that allow for the disruption of terrorist acts in the United States and the detention of the terrorists themselves. These tools can be deployed as soon as the analysis uncovers evidence of terrorist planning. This analysis and assessment will help support and enable the actions taken by the U.S. government to prevent terrorism.

Warning and protective action. Inclusive and comprehensive analysis allows the government to take protective action, and to warn appropriate sectors and the public. Defensive action will reduce the potential effectiveness of an attack by prompting relevant sectors to implement security and incident management plans. In addition, defensive action works as a deterrent to terrorists weighing the potential effectiveness of their plans. Warnings allow entities and citizens to take appropriate actions to meet the threat, including upgrading security levels in any affected sectors, activating emergency plans, dispatching state and local law enforcement patrols, and increasing citizen awareness of certain activities.

Strategic response (policy). The enemy of today is far different from those we have faced in the past. The strategies and operating procedures used to fight the traditional strategic threats of the 20th century are of little use in the war on terrorism. We need to develop and create new capabilities specifically designed to defeat the enemy of today and the enemy of the future. This immediate- and long-term strategic capability building will be shaped through budgetary allocations, and will be informed by the careful analysis and assessment of homeland security information.

Understanding terrorist organizations will allow policymakers to fashion policies that build international coalitions against terrorism, and eliminate sources of support or sanctuary for terrorists.

National Vision

The collection and analysis of homeland security intelligence and information has become a priority of the highest measure. The intelligence community must enhance its capacity to obtain intelligence relevant to homeland security requirements. The intelligence profession must attract America's brightest and most energetic and allow them to acquire and apply the expertise needed to assure homeland security. In addition, the intelligence community must expand human source intelligence, and develop and utilize technology to enhance analytic, collection, and operational efforts throughout the counterterrorism community. Homeland security intelligence and information must be fed instantaneously into the Nation's domestic anti-terrorism efforts. Those efforts must be structured to provide all pertinent homeland security intelligence and law enforcement information—from all relevant sectors including state and local law enforcement as well as federal agencies—to those able to take preventive or protective action. Under the President's proposal, the new Department will provide real-time actionable information—in the form of protective actions that should be taken in light of terrorist threats, trends, and capabilities, and U.S. vulnerabilities—to policymakers, federal, state, and local law enforcement agencies and the private sector, based on the review and analysis of homeland security information.

Major Initiatives

Enhance the analytic capabilities of the FBI. The Attorney General and the Director of the FBI have established the FBI's top priority as preventing terrorist attacks. They are creating an analytical capability within the FBI that can combine lawfully obtained domestic information with information lawfully derived from investigations, thus facilitating prompt investigation of possible terrorist activity within the United States.

The FBI is instituting several changes as it redefines its mission to focus on preventing terrorist attacks. To

enhance the FBI's analytic capabilities, the Director is seeking to increase the number of staff working to analyze intelligence more than fourfold compared to pre-September 11 figures. The Bureau will hire analysts with specialized expertise, including foreign language capacity, computer skills, and science and engineering backgrounds. The CIA will send approximately 25 of its analysts to the FBI, enhancing not only the FBI's analytical capabilities but also the relationship between these two entities.

Build new capabilities through the Information Analysis and Infrastructure Protection Division of the proposed Department of Homeland Security. The President's proposal to create the Department of Homeland Security would build new and necessary capabilities into the Information Analysis and Infrastructure Protection Division of the Department. Currently, the U.S. government does not perform comprehensive vulnerability assessments of all our Nation's critical infrastructure and key assets. Such vulnerability assessments are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given facility or sector, and then to invest accordingly in protecting such facilities and sectors. The Department of Homeland Security would have the responsibility and capability of performing these comprehensive vulnerability assessments. (See *Protecting Critical Infrastructure and Key Assets* chapter for additional discussion.)

The vulnerability assessments, important in their own right, are also building blocks for a key homeland security function that currently is not being performed: threat-vulnerability integration. Today, no government entity is responsible for analyzing terrorist threats to the homeland, mapping those threats against our vulnerabilities, and taking protective action. Our intelligence and federal law enforcement agencies focus on the detection and disruption of each individual threat. The Department of Homeland Security, informed by intelligence and information analysis and vulnerability assessments, would focus on longer-term protective measures, such as the setting of priorities for critical infrastructure protection and "target-hardening." (See *Protecting Critical Infrastructure and Key Asset*s chapter for additional discussion.)

To perform this function, the Secretary of the new Department of Homeland Security would have broad statutory authority to access intelligence information, as well as other types of information, relevant to the terrorist threat to our Nation. Indeed, the President's proposal not only permits, but requires, each executive agency to promptly provide the Secretary all reports, assessments, and analytical information relating to the missions of the new Department. The Department would also work with state and local law enforcement and the private sector to leverage the critical homeland security information in the possession of these entities.

In addition to transforming homeland security information into long-term protective action, the Department of Homeland Security would also turn the information into useful warnings. The Department would serve as the primary provider of threat information to state and local public safety agencies and to private sector owners of key targets, thereby minimizing confusion, gaps and duplication.

The combination of these new capabilities within the Department of Homeland Security and the existing and enhanced capabilities of our Nation's intelligence and law enforcement communities would enable the federal government to combat terrorism with maximum effect.

Implement the Homeland Security Advisory System. The Homeland Security Advisory System disseminates information regarding the risk of terrorist acts to federal, state, and local authorities, the private sector and the American people. The Advisory System creates a common vocabulary, context, and structure for the ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work. The Department of Homeland Security would be responsible for managing the Advisory System.

The Advisory System provides a national framework for public announcements of threat advisories and alerts to notify law enforcement and state and local government officials of threats. They serve to inform the public about government preparations, and to provide the public with the information necessary to respond to the threat. The Advisory System characterizes appropriate levels of vigilance, preparedness, and readiness in a series of graduated threat conditions. Each threat condition has corresponding suggested measures to be taken in response. Such responses include increasing surveillance of critical locations, preparing to execute contingency procedures, and closing public and government facilities.

Utilize dual-use analysis to prevent attacks. Terrorists use equipment and materials to carry out their criminal acts. Such equipment and material can include items such as fermenters, aerosol generators, protective gear, antibiotics, and disease-causing agents. Many of these items are "dual-use" items—they have not just terrorist applications, but also legitimate commercial applications, and can often be bought on the open market. If

suspect dual-use acquisitions are identified, cross-referenced with intelligence and law enforcement databases, and mapped against threat analyses, the U.S. government's ability to detect terrorist activities at the preparation stage will be enhanced. Therefore, the federal government, led by the Department of Homeland Security, will evaluate and study mechanisms through which suspect purchases of dual-use equipment and materials can be reported and analyzed. (See *Defending against Catastrophic Threats* chapter for a discussion of the Select Agent Program.)

Employ "red team" techniques. The Department of Homeland Security, working with the intelligence community, would utilize "red team" techniques to improve and focus of the Nation's defenses against terrorism. Applying homeland security intelligence and information, the new Department would have certain employees responsible for viewing the United States from the perspective of the terrorists, seeking to discern and predict the methods, means and targets of the terrorists. Today's enemies do not think and act in the same manner as yesterday's. The new Department would use its capabilities and analysis to learn how they think in order to set priorities for long-term protective action and "target hardening." Employing "red team" tactics, the new Department would seek to uncover weaknesses in the security measures at our Nation's critical infrastructure sectors during government-sponsored exercises. (See *Protecting Critical Infrastructure and Key Assets* chapter for additional discussion.)