Planning for & Responding to Threats to the U.S. Homeland

FINAL REPORT

FROM A CONFERENCE
ORGANIZED BY
Institute for Foreign Policy Analysis
International Security Studies Program of
The Fletcher School, Tufts University

WITH THE SPONSORSHIP OF
United States Northern Command
Defense Threat Reduction Agency
Institute for Foreign Policy Analysis, Inc. (IFPA) provides innovative studies, reports, briefings, publications, workshops, and conferences on national security and foreign policy issues. IFPA’s products and services are designed to assist senior government policy-makers, industry leaders, and public policy communities in making informed decisions in the uncertain global security environment of the early twenty-first century. The Institute maintains a core staff of analysts at its offices in Cambridge, Massachusetts and Washington, D.C.

International Security Studies Program (ISSP) is dedicated to teaching and research across the international security spectrum. As a distinct field of study within the multidisciplinary curriculum of The Fletcher School, Tufts University, the ISSP offers a full schedule of graduate-level courses and seminars. The ISSP sponsors a diverse range of “outside the classroom” educational activities, including annual conferences devoted to critical defense-related issues, a simulation exercise, a lecture series, field trips, and publications.

U.S. Northern Command (USNORTHCOM) was established by the Department of Defense in 2002 to consolidate, under a single unified command, existing missions that were previously executed by other military organizations. USNORTHCOM’s missions are homeland defense and civil support. Specifically, the Command conducts operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility; and, as directed by the President or Secretary of Defense, provides military assistance to civil authorities, including consequence management operations. USNORTHCOM has few permanently assigned forces, but it will be assigned forces whenever necessary to execute missions ordered by the President.

Defense Threat Reduction Agency (DTRA) safeguards America and its friends from weapons of mass destruction (chemical, biological, radiological, nuclear, and high explosives) by reducing the present threat and preparing for future threats. Under DTRA, Department of Defense resources, expertise and capabilities are combined to ensure the United States remains ready and able to address the present and future WMD threat environment.

This report does not necessarily reflect the views of the cosponsors or organizers.
Final Report

ORGANIZED BY
Institute for Foreign Policy Analysis
International Security Studies Program of
The Fletcher School, Tufts University

WITH THE SPONSORSHIP OF
United States Northern Command
Defense Threat Reduction Agency
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>v</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>vii</td>
</tr>
<tr>
<td>Welcoming Remarks and Conference Overview</td>
<td>1</td>
</tr>
<tr>
<td>Opening Keynote Address</td>
<td>4</td>
</tr>
<tr>
<td>Session 1</td>
<td>10</td>
</tr>
<tr>
<td>Anticipating and Assessing U.S. Vulnerabilities in a Changing Threat Environment</td>
<td></td>
</tr>
<tr>
<td>Session Two</td>
<td>21</td>
</tr>
<tr>
<td>The Intelligence Conundrum: Developing Actionable Intelligence for Homeland Defense/Security</td>
<td></td>
</tr>
<tr>
<td>Day One Luncheon Address</td>
<td>31</td>
</tr>
<tr>
<td>Securing an Open Society: Canada's National Security Policy</td>
<td></td>
</tr>
<tr>
<td>Session 3</td>
<td>37</td>
</tr>
<tr>
<td>Relating Homeland Defense to Homeland Security</td>
<td></td>
</tr>
<tr>
<td>Session 4</td>
<td>48</td>
</tr>
<tr>
<td>Essential Capabilities for a Layered and Integrated Homeland Defense</td>
<td></td>
</tr>
<tr>
<td>Dinner Address</td>
<td>58</td>
</tr>
<tr>
<td>Keeping America Safe: Progress and Partnerships in the 21st Century</td>
<td></td>
</tr>
<tr>
<td>Session Five</td>
<td>63</td>
</tr>
<tr>
<td>Anticipating and Defending against Bioterrorism</td>
<td></td>
</tr>
<tr>
<td>Session 6</td>
<td>77</td>
</tr>
<tr>
<td>Strengthening International Cooperation</td>
<td></td>
</tr>
</tbody>
</table>
Day Two Luncheon Address
Protecting the Homeland: Progress at Home and Abroad

Session 7
Emerging Technologies for Homeland Security/Defense:
Governmental and Industry Perspectives
In the three years since the 9/11 attacks, new institutions and strategies have been established to meet the new challenges to the security of the United States. With the creation of U.S. Northern Command (NORTHCOM), the Department of Homeland Security (DHS), and the publication of the first National Strategy for Homeland Security, there are numerous lessons to be learned and new challenges to overcome as the United States organizes its defenses to address the threats of the early twenty-first century. These issues are discussed in detail in the Conference Report.

In order to examine these diverse issues and challenges and to better understand their impact on homeland defense and homeland security, the Institute for Foreign Policy Analysis (IFPA) and the International Security Studies Program of The Fletcher School, Tufts University, with the cosponsorship of U.S. Northern Command, and the Defense Threat Reduction Agency, convened the 35th IFPA-Fletcher Conference on National Security Strategy and Policy focusing on planning and responding to threats to the U.S. homeland. Topics addressed include anticipating and assessing U.S. vulnerabilities in a changing threat environment; identifying intelligence requirements for homeland defense/security; relating homeland defense...
to homeland security; identifying essential capabilities for layered, integrated homeland defense and homeland security; anticipating and defending against bioterrorism; strengthening international cooperation; and government and industry perspectives on emerging technologies for homeland security.

In the Executive Summary, we have listed key conclusions as well as policy options that emerged from the conference discussions. Obviously, not all speakers shared all conclusions, nor does our list necessarily imply endorsement by the conference organizers and cosponsors.
Since 9/11, the United States has developed an extensive strategy for homeland security, but much remains to be done. We have not been attacked again for several reasons: power projection, a seizure of operational initiative from the enemy, and the courage of young Americans in uniform. We face fundamental changes in how wars are fought. The enemy is brutal. We must have a defense that is in-depth, layered, and active.

The Department of Defense (DOD) has drafted and is modifying a homeland defense and civil support strategy, with objectives including: achieving maximum awareness of potential threats; interdicting threats far from the United States; providing mission assurance; ensuring DOD’s ability to support civil authorities in consequence management activities; and improving domestic and international partner capabilities for homeland defense and homeland security.

New capabilities and missions have been developed for the maritime, land, and air domains and for emergency preparedness and response situations. Organized responses have been formulated to handle chemical, biological, radiological, and nuclear (CBRN) attacks with the Marine Corps and National Guard units taking
the lead. The government has worked with the private sector on new technologies for the detection of weapons of mass destruction (WMD), biometric identification of the enemy, and more affordable and effective communications equipment supporting interoperability among civilian, military, and first responder personnel. Military capabilities alone will not defeat al-Qaeda.

Session 1
Anticipating and Assessing U.S. Vulnerabilities in a Changing Threat Environment

Since 9/11, the United States has confronted an unprecedented threat environment. Besides hostile rogue states, terrorist groups with global reach have sought to acquire WMD and other lethal capacities. This panel analyzed these threats and U.S. vulnerabilities. Topics include: nuclear/radiological terrorism; protecting critical infrastructure; identifying and coping with future threats; electromagnetic pulse (EMP) attack; enhancing horizontal integration; and involving the private sector in homeland security.

Key conclusions include:

• Efforts to reduce the risk of nuclear terrorism should focus on eliminating the supply of fissile material at its source: no loose nukes, no new nascent nukes and no new nuclear weapons states. The U.S. government should work with Russia to assure the security of its nuclear weapons and material and develop comprehensive standards to secure global stockpiles; prevent the development of new highly enriched uranium (HEU) or plutonium programs; and reverse North Korea’s nuclear programs.

• Effective security planning in the new threat environment requires that we abandon the artificial separation between “national security” and “homeland security.” Emerging threats span borders and target our critical infrastructure. America will remain vulnerable if “national security” officials define these threats as “homeland security” and therefore the responsibility of other officials. Dividing “homeland defense” from “homeland security” exacerbates this problem, since the former,
concerned with countering attacks on the U.S. homeland from abroad, has little operational relevance today since terrorists will attack the homeland from inside and outside our borders.

- Relying on offensive military operations and good intelligence to avert attacks on our critical infrastructure is problematic, since neither our Armed Forces nor intelligence agencies are currently structured to fight transnational terrorism. Our power is dependent on interconnected global networks (transportation, logistics, energy, information, finance, etc). A better strategy for reducing their vulnerability to terrorism is boosting critical infrastructure protection. For instance, making our electricity system more resilient to EMP attack enhances the protection of other sectors, and also provides security against related hazards such as lightning, floods and geomagnetic storms.

- The lack of horizontal integration across government departments inhibits effective planning. DOD’s requirements are not effectively linked with those of other agencies to develop joint strategic plans against such threats as an EMP attack and nuclear terrorism. We should create institutional structures modeled on the new National Counterterrorism Center to enhance the government’s ability to develop, update and implement operational plans across executive departments.

Session 2
The Intelligence Conundrum: Developing Actionable Intelligence for Homeland Defense/Security

This panel assessed the role of intelligence in countering terrorism, especially in the aftermath of 9/11. It is necessary to develop “actionable” intelligence that allows policy makers to anticipate and respond to threats. Another requirement is to enhance intelligence sharing across federal departments and agencies and between the federal government and state and local authorities. Key topics include: improving information sharing and deciding who has a need to
know; integrating and disseminating actionable intelligence; bridging the intelligence-law enforcement divide; developing priorities and resource requirements for collection capabilities; enhancing coordination between foreign and domestic intelligence; and gaining greater public support in the war on terrorism.

The panelists, all of whom have extensive experience in the U.S. intelligence community, assessed current intelligence practices and evaluated recommendations for improvement in light of emerging twenty-first-century security challenges. A common theme was the notion that developing and sharing actionable intelligence is based as much on intangible factors as on the application of technology and rigorous analytical methods. For instance, whether a particular data point is “actionable” may be in the eye of the beholder, depending on the willingness to act despite whatever collateral damage such action would entail. Intelligence analysis itself is more art than science, since typically very little useful threat information is available. Building effective relationships between local law enforcement authorities and the broader public could help generate more actionable intelligence. Effective intelligence dissemination involves judgments on how much and to whom actionable intelligence should be shared.

Key conclusions include:

• Reform should focus simultaneously on improving domestic intelligence and foreign collection capabilities. Enhancing trust and cooperation between local law enforcement and members of the public with information of intelligence value is vital for uncovering terrorist cells and their financial backers in the United States. In order to penetrate al-Qaeda cells, we must increase human intelligence capabilities and rely more on non-official cover. Creating a National Intelligence Director might help improve the coordination of foreign and domestic intelligence, but intelligence reorganization has been largely overemphasized and threatens to do more harm than good.

• The requirement for military intelligence must be balanced with the need to protect civil liberties. We should fuse foreign intelligence with domestic intelligence.
intelligence with information from law enforcement operations, but to incorporate the latter it must have some connection to a foreign intelligence or terrorist operation. A military intelligence organization should not involve itself in domestic law enforcement activities unrelated to a foreign threat.

- Balance is important in thinking about information sharing, because real constraints exist on the amount of sharable information. These include the need to protect sources and methods, liaison relationships, ongoing operations and civil liberties. Sharing also does not automatically produce “knowledge,” and increased sharing could simply result in being wrong faster. The Terrorist Threat Integration Center (TTIC) Online is developing the IT architecture and sharing protocols needed to effectively share intelligence data of different levels of classification with various end-users.

- We must establish appropriate incentives to encourage information sharing between state and local law enforcement agencies which, along with first responders, provide most of the actionable intelligence but are not legally required to share information. Clear incentives include improvements in law enforcement (if information is shared) and sharing Federal Bureau of Investigation (FBI) information with local and state officials.

**Luncheon Address**

**Securing an Open Society: Canada’s National Security Policy**

Rob Wright, National Security Advisor to the Prime Minister of Canada and Associate Secretary to the Cabinet

Canada remains committed to North American security and to cooperation with the United States. The two nations share a critical economic, political, and security relationship and have a strong commitment to the security and prosperity of our continental space. Long before 9/11 the two nations developed a close security partnership. Their airspace defense was integrated with the establishment
of the North American Aerospace Defense Command (NORAD) in 1958, and their intelligence communities share much information on threats to North America. Canada is intensely focused on homeland security and has adopted a number of measures since 9/11, such as the Smart Border Action Plan, to enhance cooperation on border security.

The Canadian Prime Minister has established a new Cabinet Committee on Security, Public Health and Emergencies, and appointed a National Security Advisor to assist the Prime Minister. The National Security Advisor has helped the Deputy prime minister prepare and implement Canada’s first comprehensive statement on national security, *Securing an Open Society: Canada’s National Security Policy*, which was released on April 27, 2004. The National Security Policy defines three core interests of Canada: to protect Canada and Canadians; to ensure that Canada is not a base for threats to its allies; and to contribute to international security. It also identified six areas for action for building an integrated Canadian security system: intelligence, emergency planning, public health emergencies, transportation security, and international security. For this framework policy to work, Canada must continue to integrate its efforts with the United States.

**Session 3**

**Relating Homeland Defense to Homeland Security**

The relationship between homeland defense and homeland security, and the organizational, bureaucratic and legal challenges of forming and implementing policies located in the intersection between them was the focus of this session. Important topics include: identifying lead responsibilities; the role of DOD, NORTHCOM and other government agencies in homeland defense and civil support missions; the role of the National Guard in providing military assistance to state and local authorities; and public/private sector partnerships in homeland security strategy.

An underlying theme throughout this session was the role of the military in domestic contingencies, and balancing the military’s effectiveness with the imperative of maintaining civilian
control. Panelists stopped short of calling for altering the 1878 Posse Comitatus Act, which limits the domestic application of the Armed Forces to a few specific situations, but some emphasized that it should be examined to allow for the greatest possible flexibility. Greater integration across government agencies is needed to eliminate operational seams at the intersection of homeland defense and homeland security. This will require procedures to improve collaboration between military and civilian organizations, including clarifications on chains of command for homeland defense and homeland security missions.

Key conclusions include:

• Homeland security and homeland defense operations should focus more on proactive missions that detect, deter and prevent threats rather than simply respond to them, and DHS should lead these missions within the United States. For example, if al-Qaeda was interested in attacking our subways, DHS could coordinate a deterrence mission by sending the Guard to patrol the New York and Washington, DC subways. Command relationships for these missions are not clearly established, creating operational seams the enemy can exploit. While DHS should lead these missions, operational control of military forces should remain within a military chain of command.

• In the new threat environment, distinctions between homeland security and homeland defense, and between military assignments and civilian functions, have been blurred if not eliminated. We therefore should reexamine the processes used to formulate and execute national military strategy and homeland security/defense strategy. Our military and civilian capabilities, technology and planning should be more fully integrated to develop a unified approach to domestic incident management. We should also establish an interagency process to assess national security and homeland security threats and vulnerabilities. We may need to reevaluate some of the basic roles and missions of the Armed Forces to allow the military to participate
in homeland security missions or even some law enforcement operations, such as eradicating the Afghan opium trade.

- We should utilize the unique capabilities and organizational structure of the National Guard to close existing gaps between homeland defense and homeland security. Through the Joint Forces Headquarters (JFH) in every state, the Guard provides military assistance to either combat commanders or to civilian authorities for emergency management or consequence management missions. Through the JFH structure, the Adjutant General has military command responsibilities and is also the senior official responsible for emergency management functions within each state.

- The private sector should be incorporated more fully into planning responses, since it owns much of the nation’s critical infrastructure. Private sector preparedness should be encouraged as a good investment. Tangible guidance should be offered in how operations can be safeguarded. Furthermore, the public and private sectors need to cooperate in allocating risk management responsibilities and associated costs, and eliminating resulting coverage gaps.

- We may not need to revise the Posse Comitatus Act, but we should at least determine whether it allows for sufficient flexibility. Before making any changes we should ask several fundamental questions. For instance, which missions would require manpower in excess of the total number of guardsmen, and are these missions not covered by the numerous exceptions to the Act which already exist?

Session 4
Essential Capabilities for a Layered and Integrated Homeland Defense

Establishing layered and integrated homeland defenses is vital for countering emerging threats since time and space considerations factor prominently in reducing our vulnerabilities. Layered and integrated defenses permit the early and persistent detection and interception of threats far from our borders, and therefore repre-
sent the most effective means of managing risks in the new security environment. This session addressed several topics: defense against missile attacks; protecting maritime approaches; leveraging the capabilities and command structures of the national guard for homeland defense and homeland security missions; and relating NORTHCOM to other military as well as civilian agencies for establishing integrated homeland defenses.

Panelists described how their respective organizations were developing the capabilities, relationships and bureaucratic structures necessary for layered and integrated defenses. The importance of integration between technological systems and across organizations was emphasized. Integrated technological systems permit greater domain awareness and enable the persistent application of counter-threat measures at a distance far from the United States. Effective coordination between local, state, federal and military organizations is necessary. The National Guard plays a key role, integrating the demands of various stakeholders while also possessing versatile capabilities usable in a range of homeland security and homeland defense missions. Panelists concurred that the tremendous progress made since 9/11 in establishing layered and integrated defenses provided an effective foundation to build upon.

Key conclusions include:

• Although NORTHCOM has made tremendous progress in building effective relationships with DHS, the National Guard Bureau and the Coast Guard, it must continue to grow and build on its successes. The United States needs a more robust capability to counter WMD threats. This includes defenses against cruise missiles and unmanned aerial vehicles (UAVs). NORTHCOM must continue to work closely with federal agencies such as the Federal Emergency Management Agency (FEMA) and the FBI, and with international partners and the private sector.

• The National Guard is a versatile force capable of contributing substantially to layered and integrated defenses. It is engaged in a variety of civil and military missions. These include providing depth to active units in combat missions
overseas, supporting law enforcement at home and furnishing consequence management capabilities in support of civil agencies. By serving as an intermediary between combat commanders, Adjutants General and the Departments of the Army and Air Force, the National Guard Bureau helps foster integration between civilian and military organizations tasked with coordinating and implementing homeland defense and homeland security missions.

- Through the *Maritime Strategy for Homeland Security*, the Coast Guard is helping to construct layered defenses by enhancing maritime domain awareness and creating and overseeing multiple security regimes. Improved domain awareness requires better intelligence. Therefore, the Coast Guard is expanding its maritime domain awareness surveillance system, and adopting advanced technology such as automatic information systems in order to enhance informational awareness and thus increase the geographic depth of maritime defenses. Furthermore, the Coast Guard has helped establish international security regimes like the International Ship and Port Facility Code, which requires all ships and overseas port facilities to have security plans and security officers.

- Missile defenses are needed to counter missile proliferation. A nuclear North Korea with intercontinental missiles could hold U.S. cities hostage. We are rapidly developing layered missile defenses that will employ land, sea and space basing modes, with a variety of interceptors that can target and shoot down an incoming ballistic missile in either the boost, midcourse or terminal phase. Each of these systems will be integrated with a family of sensors, so that once a missile is launched, the information will be shared throughout the entire system, thereby expanding the detection and engagement zone.
Defeating the new threat of terrorism will require a constant sense of urgency, resolve and dedication as well as a commitment to transformation to ensure that we possess the right capabilities and organizational practices for the best possible defense. Resolve, dedication and innovation represent core values at DHS, and they guide us as we seek to develop new security paradigms that balance the need for increased security while protecting our civil liberties and allowing our economy to function smoothly.

DHS has begun to meet this challenge. New policies and innovations have been introduced that improve airport security and streamline the customs and immigration processes at airports, at little inconvenience to the public. We are allocating more money to improve communications interoperability between first responders, and we created the Homeland Security Information Network to link state and local authorities with their federal counterparts. The old security paradigm which focused solely on prevention, response and consequence management has been rejuvenated through an increased emphasis on information and domain awareness. We face a number of important challenges, such as enhancing information sharing and the protection of our critical infrastructure, integrating all the ports and borders of North America, investing in next-generation technology, and developing 21st-century personnel, procurement and information systems that incorporate the best practices from both the public and private sectors. By relying on resolution and innovation – key aspects of the American spirit – we will overcome the terrorist challenge and secure our homeland.
Session 5
Anticipating and Defending Against Bioterrorism

This session assessed the main issues associated with bioterrorism and the respective roles of federal, state, local, and private sector capabilities in managing this threat. The discussion reflected the diversity of biological agents themselves by focusing on both known biological agents as well as potential new bioweapons. The main topics that were addressed include: lessons from the anthrax crisis of 2001; emergency response and support, including critical surge capabilities; consequence management; threat monitoring and incident assessment; resource requirements and coordination; the diversity of the bioterrorist threat; legal and civil-military action and cooperation; and public health issues, including surveillance and testing, immunizations, isolation or quarantine.

During the session several contributors noted the unique aspects of a bioterrorist attack. It will likely be well underway before we are aware of it and the specific agent used, and attacks can easily spread, given the mobility of our society and the transferability of biological agents. Reversing this escalatory dynamic will likely require federal assistance, both civilian and military, which places a premium on their effective coordination with each other and with local and state authorities. Local public health authorities will play a key role in the early detection of a bioterrorist attack, stopping its spread, and providing a foundation upon which to build external assistance.

Key conclusions include:

- Effective communication is vital during a public health crisis, in order to build public confidence in the government’s ability to manage a crisis. The first priority is to assess the environment, which will be characterized by heightened emotion and limited access to facts, and to provide the public with accurate and timely information they can trust. Information dissemination should be coordinated region-wide, and information that is known to be false should never be conveyed, since credibility is extremely important in building trust. We should also pay more attention to the psycholog-
- Establishing good relationships between military and civilian leaders is vital for providing effective military support to civilian authorities. NORTHCOM has few assigned forces, and therefore it is essential to develop the relationships that allow NORTHCOM to identify and access relevant DOD, federal, state and local medical capabilities before an event. DOD provides policy guidance for assistance to civil authorities, with NORTHCOM responsible for tactical implementation. It will take another two or three years of progress before DOD processes can ensure the rapid and effective availability of U.S. military assets for domestic consequence management missions. We need to create processes that enable flexible responses tailored to the requirements of a particular emergency.

- The 2001 anthrax attacks and the outbreak of West Nile Virus in August 1999 have led to the emergence of a new public health perspective about infectious diseases. We now realize that local infectious disease outbreaks can soon impact our national security and the global economy, and we appreciate more the need for a rapid and collaborative response to outbreaks. We need to strengthen collaboration with veterinarians, since the biological agents of greatest concern are often of animal origin. We also need to utilize environmental microbiology to help us detect and quantify bioterrorist agents, determine their survival times, and disinfect them in various environments. We also need to strengthen partnerships between clinicians and public health agencies at the local level, and enhance our relationships with foreign and international agencies.

- We no longer face a known list of biological threats against which we can concentrate our defense efforts, since new threats are constantly emerging. The scientific challenge is to develop versatile capabilities that can work against unknown pathogens. Instead of developing a vaccine against every possible
biological threat, we should develop the means to enhance our innate immunity, such as by blocking the pathways through which pathogens can enter the body.

- We need to standardize the procedures used by the civilian and military sectors to analyze environmental samples for determining potential disease outbreaks. Environmental samples are now analyzed separately and each side is unlikely to accept the test results of the other at face value. This lack of trust and coordination will be highly debilitating during a crisis. The military and civilian response communities also need to develop similar means to establishing situational awareness and a common operational picture.

Session 6
Strengthening International Cooperation

This session examined the international dimension of homeland security strategy. Building robust global partnerships against terrorism is vital in establishing homeland defenses with global reach. The main topics that were addressed include: improving American and European collaboration in the fight against terrorism; enhancing cooperation with Mexico; the State Department’s counterterrorism strategy; and NATO’s contributions to the Global War on Terrorism (GWOT).

Improving Mexican-American counterterrorism cooperation is vital to creating a North American defensive perimeter. As U.S homeland security measures drive terrorists further from the United States, they may find Mexico a more target rich environment, given the numerous American interests and large numbers of tourists in the country. In pursuing American interests, U.S. policymakers will have to diffuse traditional Mexican worries concerning infringements of national sovereignty, and overcome lingering bitterness over perceived failures in past counter-narcotics cooperation. Effective transatlantic cooperation is also vital to defeating terrorism, and during the session it was noted that transatlantic alliance structures were not being fully utilized in the war on terror. The North Atlantic Council offers the opportunity to address nearly fifty NATO
members and partner countries, and despite its formal structure, the alliance allows for creativity in terms of informal meetings between national delegates, where policy coordination is often achieved. Fully utilizing this forum could help mobilize European governments and societies in the war on terror.

Key conclusions include:

- We should more actively involve the American scientific establishment in the war on terror. Its contributions were vital to winning World War II, and it can provide the decisive edge in overcoming the new threats. We should also utilize NATO and specifically the North Atlantic Council to harmonize national counterterrorism policies and to actively involve the European scientific establishment in the war on terrorism.

- While the United States will use all elements of its power to fight terrorists, including direct and unilateral military strikes, the success or failure of our global campaign against terrorism hinges on building the will and capacity of other nations to fight terrorism on their own soil and in their own interest. Public diplomacy is also important. Changing perceptions represent core power, and we should devote more attention and resources to understanding how to utilize global communications to build goodwill towards America.

- To advance Mexican-American security cooperation, Mexican security interests must be incorporated in bilateral discussions and adopted policies. Building trust would ensure a more robust level of security cooperation, and confidence-building measures, such as bilateral cooperation on WMD detection and consequence mitigation within Mexico, would help since Mexico lacks these capabilities. Some form of Mexican participation in NORAD, and the granting of export licenses for the sale to Mexico of highly desired defense items, would also garner Mexico’s enthusiastic participation in bilateral counterterrorism efforts.

- Transatlantic cooperation is essential to defending our common values and overcoming common threats, and NATO mem-
bers will fight it together as long as necessary. The alliance is actively engaged in the global fight against terrorism. In August 2003 the alliance took control of the International Security Assistance Force (ISAF), and at the 2004 Istanbul Summit the alliance agreed to provide training, equipment and technical assistance to nascent Iraqi security forces. It has also developed a number of CBRN defense initiatives, including a deployable nuclear, biological and chemical (NBC) analytic laboratory, to counter the threat posed by WMD proliferation.

Luncheon Address
Protecting the Homeland: Progress at Home and Abroad
The Honorable Frances Fragos Townsend, Assistant to the President for Homeland Security

The United States has three strategic objectives in the global war on terror: defeating the terrorists and their network both at home and abroad; working with partners to isolate terrorists and outlaw regimes while supporting the rise of democracy; and transforming the federal government to effectively fight terrorism. We are now effectively marshalling all of our capabilities – military, diplomatic, intelligence, economic and law-enforcement – to win the war on terrorism. And we are taking the war to the terrorists, with much success. We have killed or taken into custody three-quarters of the senior al-Qaeda leadership, operational managers and key facilitators, and we have denied them their sanctuaries in Afghanistan and Iraq as well as reduced their financing by freezing their assets and denying them access to the international financial system. The governments of both Pakistan and Saudi Arabia are now important allies in fighting terrorism, while Libya and the A.Q. Khan network no longer present a WMD proliferation threat.

Our ultimate objective is to create an international environment inhospitable to terrorists and their supporters. Our efforts to promote democracy in Afghanistan and Iraq are predicated on
our belief that the hopes and aspirations of freedom will supplant the hatred, despair, and destructive visions which terrorists seek to exploit. And we are working with our allies in this endeavor. Sixty-four countries are assisting Central Command (CENTCOM) at its Tampa headquarters, and all of our NATO allies have troops in Afghanistan, Iraq, or both.

The federal government is also undergoing a sweeping transformation to enhance its ability to defeat terrorism and support democracy. DHS is now leading a unified effort to secure the United States from terrorist attacks, and the Homeland Security Council is coordinating policy across the multiple departments and agencies involved in the homeland security mission. NORTHCOM now provides an integrated approach to homeland defense and coordinates DOD support to federal, state and local civilian authorities. And the National Counterterrorism Center further institutionalizes the war on terror by serving as the intellectual repository on terrorists and their networks, while also providing strategic operational planning for U.S.-wide counterterrorism activities that integrate all instruments of national power.

Session 7
Emerging Technologies for Homeland Security/Defense: Governmental and Industry Perspectives

A common theme throughout the conference was the importance of mobilizing all instruments of national power to defeat the new threats. America’s unsurpassed scientific and technological base rep-
resents a vital resource that must be leveraged in the GWOT. This panel examined the ways in which technology can be harnessed to prevent, detect, deter and respond to a WMD attack. The major topics that were addressed include: developing chemical, biological, radiological, and nuclear countermeasures; developing systems for detecting hostile intent; applying biometric technology to identification devices; building layered defenses with network-centric technology and operations; and improving intercommunications and information sharing between first responders.

Panel members provided examples of how technology can be applied to overcome the seemingly insurmountable problem of filtering out the flow of terrorists and WMD materials from legitimate cross-border trade and movement of peoples. For instance, establishing informational awareness is difficult since relevant data will often reside in the incompatible IT systems of various government agencies. Products such as Raytheon’s Genesis overcome this problem by accessing data from different IT architectures and thereby enable informed intelligence decisions by border guards, analysts and other end-users. Several panelists noted that the adoption of technology by the public sector will be guided by the logic of “technological push” rather than “requirements pull.” DOD has already developed technology for other purposes that will be useful for homeland security/defense, and new uses will be found for private sector advances in network-centric technology.

Key conclusions include:

- The U.S. government has established organizational routines for incorporating enabling technologies developed in the private sector. Every year the Office of Science and Technology Policy (OSTP) with Office of Management and Budget (OMB) provides guidance to federal agencies on R&D budgets, and coordinates the science and technology activities for all federal agencies through the National Science and Technology Council (NSTC). Advanced technology has already been utilized in several programs, such as BioWatch, BioShield and BioSense, to improve our detection and response capabilities in case of a bioterrorist attack, and we are aggressive-
ly researching, testing and evaluating biometric identification systems to improve border and port security.

- The National Nuclear Security Administration (NNSA) is developing new technologies to improve our ability to detect illicit trafficking of nuclear materials through seaports and land crossings. For instance, we developed Palm Pilot and cell-phone based equipment to improve standoff detection for shielded nuclear materials, and we have made substantial progress in developing real-time isotope identification systems that reduce the economic costs while increasing the effectiveness of port detection activities. Implementing these and other advanced technologies will increase domain awareness and push out the boundaries of homeland defense.

- Interoperable communications equipment is vital in responding to a crisis, as it enables effective collaboration between various first responders and enhances integration among federal, state, local, military and private sector officials in consequence management missions. Rather than simply replacing every communications device in the nation with a single format, a more cost-effective method is developing technology that enables communications between previously incompatible systems. With technology developed by Raytheon, the entire County of Los Angeles could be made interoperable for $7.5 million.

- We should employ network-centric operations to build effective layered defenses. For example, we will never develop the technology for the perfect biosensor, but a set of layered, networked sensors would provide greater security. They can provide the right information to the right people at the right time, and will help us achieve the level of situational and domain awareness needed for the early detection and elimination of threats.
Day One
Dr. Robert L. Pfaltzgraff, Jr., President, Institute for Foreign Policy Analysis, and Shelby Cullom Davis Professor of International Security Studies, The Fletcher School, Tufts University

In 2001, even before the tragic events of 9/11, IFPA and The Fletcher School began planning for a homeland security conference that was held in 2002. The 35th IFPA-Fletcher Conference is part of an ongoing effort that builds upon previous conferences. Our goal is to produce important new ideas as we plan for and respond to homeland security and defense threats in the years ahead.

• We need to understand and contribute to the development and integration of strategic thinking and analysis about homeland security and homeland defense as they relate to each other and to broader issues of national security. This is a vitally important public and private sector cooperative effort.

We developed this conference with several key goals in mind:
• To anticipate and assess our vulnerabilities in the post-9/11 threat environment, including what we have done to mitigate threats and vulnerabilities and what still remains to be done;
• To understand intelligence requirements and to determine the nature of actionable intelligence;
• To set forth organizational and other challenges as we relate homeland defense and homeland security to each other within and among various levels of government, from local to state to federal, between the civilian and military components, and between government and private sector;
• To set forth requirements and priorities for an integrated, layered homeland defense, including a broad range of capabilities and cooperative efforts;
• To assess issues of bioterrorism and how we are and should be preparing to anticipate and defend against these threats, including emergency response and support and public health issues;
• To survey major issues of international cooperation with regards to trans-Atlantic and broader global dimensions, but especially how to strengthen cooperative efforts with our Canadian and Mexican neighbors; and
• To examine requirements and prospects for new technologies for homeland security, bringing together government and industry perspectives on how to develop and utilize new technologies to detect, thwart, and counter terrorism.

The conference was designed to bring together a broad spectrum of expertise, knowledge, and perspectives focused on major homeland security and homeland defense issues. We are grateful to NORTHCOM and to the Defense Threat Reduction Agency for their cosponsorship.

**Lieutenant General Joseph R. Inge, USA, Deputy Commander, U.S. Northern Command**

We do live in troubled times. At this particular time in our nation’s history, one of the things that all of us and most citizens would
agree with is that it is essential to study our nation’s security, and particularly the security of our homeland.

- Therefore, it is fitting to have a conference focused on planning for and responding to threats to the homeland.
- We have people here from industry, from the public, from the media and from the Department of Defense and other government agencies to address an important topic that will remain at the forefront of this nation’s priorities for many years to come.

Thank you to the Institute for Foreign Policy Analysis and the International Security Studies Program of The Fletcher School, Tufts University, for doing so much to support and be a partner to national security and events such as this. Thanks to everyone for your participation and to you and your colleagues for making this possible.

*Lieutenant General Joseph R. Inge, USA*
SUMMARY

The nature of war has fundamentally changed within the past two decades. Our national security has evolved from being threatened by a hostile state (the Soviet Union), or a coalition of nation states (the Warsaw Pact), to being threatened by transnational terrorist groups that are unaffiliated with any state. These non-state actors have created safe havens in other countries and are highly mobilized individuals who seek to acquire weaponry to be used against the United States and its allies. The extent to which they sought to harm the United States was seen on September 11, 2001. These events forced us to realize that we are susceptible to attack and that we need to plan and organize our forces accordingly in order to respond to the new threat. We can no longer have a defense that is passive and reactive. We need a defense that is in-depth, layered, and active.
Recognizing the need to address the threat, the Secretary of Defense, under the direction of the President, created NORTHCOM.

- NORTHCOM’s area of responsibility was derived from the Unified Command Plan.\textsuperscript{1} Canadian, Mexican, and U.S. air space and maritime approaches were assigned to NORTHCOM to protect our nation’s citizens, property, and constitutional freedoms.
- NORTHCOM’s mission is homeland defense and civil support.

The Homeland Defense office has drafted a Homeland Defense and Civil Support Strategy that is still being modified. We have identified five principal objectives that the strategy hopes to achieve. These include:

- Achieve maximum awareness of potential threats to anticipate, deter, detect, and defeat an attack proactively;
- Interdict and defeat threats at a safe distance from the United States, U.S. territories, and possessions;
- Provide mission assurance and, in the event of an attack, be able to continue our mission requirements so that no enemy will degrade our ability to project power;
- Assure DOD’s ability to support civil authorities in domestic WMD and CBRN consequence management activities; and
- Improve domestic and international partner capabilities for homeland defense and homeland security.

The Department of Defense has developed capabilities within the past three years to make our nation safer and to defend more effectively against the transnational terrorist threat. We have established a layered defense, including quick reaction forces drawn from active duty military capabilities, National Guardsmen working with civilian authorities, and civilian law enforcement.

\textsuperscript{1} The Unified Command Plan (accessible at \url{http://www.defenselink.mil/specials/unified}) allocates responsibilities among the ten combatant commands. It establishes the commands’ missions, responsibilities and force structure. The plan also defines the geographical commands’ areas of responsibilities.
• We need a continuous defense of U.S. domestic airspace. Over major American cities and critical infrastructure, we have F-15s and F-16s continuously in the air, often flown by the Air National Guard. Additional aircraft on short strip alert are prepared to defend against an attack. We will continue to develop an effective and deployable defense against cruise missiles, particularly one that will employ a maritime platform to be launched off the coast of the United States.

• In the maritime domain, we are prepared to conduct maritime intercept operations of WMD on the high seas. Basic component parts of terrorist WMD, especially radiological or nuclear, will likely be obtained overseas. There have been proposals for the concept of a maritime NORAD and the need for integrating assets of the various agencies and services for maritime security. We cannot think about maritime defense exclusively in terms of just better port security. We must push out the boundaries of our maritime defense with a more focused reliance on evolving technologies. The United States needs better capabilities for the remote detection of WMD, better surveillance and tracking capabilities, and the development of a common operating picture within the maritime domain. Better methods of container inspection will help to detect and intercept WMD that might enter the United States.

DOD has been working in close partnership with DHS to develop true maritime domain awareness for a clearer picture of emerging threats.

• Issues have been raised as to the kinds of platforms that might be appropriate for new maritime missions. There have been suggestions of incorporating littoral combat ships into a maritime defensive posture. Discussion has also taken place about training boarding parties to board a ship with hand-held or transportable WMD detection capabilities in the case that there is a possible threat aboard.

• Under the command and control of NORTHCOM, the U.S. Navy will take the lead in international waters. However, this
effort will be unsuccessful unless we incorporate the combined capabilities of the Navy, the Coast Guard, the FBI, the Department of Energy, and other agencies to be responsible for detecting and defeating WMD on the high seas. Bringing together partnerships enhances our maritime intercept operation capabilities.

- In regard to the land domain, we have forces today trained and equipped for a quick reaction within our own country. Soldiers and Marines are on alert and ready to deploy within the country. We are prepared to conduct war-fighting operations on U.S. soil under the extraordinary circumstance of a terrorist attack.

- We need to be prepared for WMD or CBRN attacks. The U.S. Army and other services have personnel that would migrate to NORTHCOM if the need arises for consequence management following multiple CBRN attacks. The Joint Task Force-Civil Support (JTF-CS) is an emerging capability located at Ft. Monroe, Virginia and is a subordinate command to NORTHCOM to respond to CBRN attacks. The U.S. Marine Corps is providing mentoring capabilities to the National Guard and other military capabilities to ensure that we will have multiple task forces, robust in size, well trained, well equipped, and working in partnership with FEMA and civilian capabilities.

- The National Guard will continue to be a force engaged in overseas war fighting and homeland defense missions, and participate in homeland security operations. The Guard is geographically dispersed throughout the United States and can flexibly respond in either active duty status or Title 32 under the command and control of the Governor. The Guard can provide immediate capabilities that can augment and reinforce civilian law enforcement authorities in compliance with

---

2 Title 32 of the U.S. Code states, “To carry out the National Guard Program in a state, the Secretary of Defense shall enter into an agreement with the Governor of the state...under which the Governor or commanding general will establish, organize, and administer the National Guard Challenge Program in the state.” (accessible at http://caselaw.lp.findlaw.com/casecode/uscodes/32/chapters/5/sections/section_509.html)
the *Posse Comitatus Act*. The Guard will also be developing additional civil support teams for assessing WMD contaminants. Military capabilities alone will not defeat transnational terrorist groups. It takes the collective capabilities of our entire society. We must prepare to respond to attacks at multiple locations throughout our country. Civilian authorities in DHS and at state and local levels may require DOD support for an effective response. Request for this type of assistance would come from a Presidential directive most likely through FEMA or DHS.

- We have a close partnership with FEMA and we are building a similarly effective relationship with DHS. We are building on the *Stafford Act* model for natural disasters. DOD has military personnel prepared to work with civilian counterparts to respond to attacks.
- Active duty military within the homeland should only be used if the threat exceeds the capabilities of civilian law enforcement. It is important for the military to achieve its mission without usurping the responsibility and leadership of the civilian authorities. This balance is needed to prevent an increased military role in domestic society which may,

---

3 *The Posse Comitatus Act of 1878* (18 USC 1385) (accessible at [http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/PosseComitatus.htm](http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/PosseComitatus.htm)). The act proscribes the use of the Army and Air Force to “execute the laws” except where expressly authorized by the Constitution or Congress. Limits on the use of the military for civilian law enforcement also apply to the Navy by regulation. In December 1981, additional laws were enacted clarifying permissible military assistance to civilian law enforcement agencies. Posse Comitatus clarifications emphasize supportive/technical assistance while generally prohibiting direct participation of DOD personnel in law enforcement (e.g., search, seizure, and arrests). For example, Coast Guard Law Enforcement Detachments serve aboard Navy vessels and perform the actual boarding of interdicted suspect drug smuggling vessels.

4 *The Robert T. Stafford Disaster Relief and Emergency Assistance Act* (accessible in full at [http://www.fema.gov/library/stafact.shtm](http://www.fema.gov/library/stafact.shtm)), enacted in 1974 and amended, most recently, in October of 2000, establishes the process of and conditions necessary for federal assistance to state and local governments in the event of natural disasters or other emergency situations. Such assistance becomes available after a presidential declaration of a state of emergency, and is implemented by FEMA.
consequently, degrade the role of civilian leadership and constitutional freedom.

Defeating transnational terrorist groups will require technology from the private sector that is now in the process of being developed.

- Help needed from the private sector includes improved chemical, biological, radiological, and nuclear countermeasures; better protective suits for military and civilian missions conducted in a WMD-contaminated environment; and improved non-lethal weaponry. Among the uniformed services, the Marine Corps has taken the lead on this issue area.
- We need innovative systems and effective, humane use of microwave systems allowing us to protect sites against attacks without endangering civilians.
- We need to be able to perform biometric identification of the enemy, which requires new tools.
- We need more affordable and effective communications equipment to support interoperability between civilian and military personnel—from first responders to hazardous material personnel and emergency managers at the state and local level and the National Guard.
- We need equipment for the movement of large numbers of injured personnel, patients, and casualties in the event of an attack.
Session 1

Anticipating and Assessing U.S. Vulnerabilities in a Changing Threat Environment

MODERATOR
Dr. Robert L. Pfaltzgraff, Jr.

SPEAKERS
Dr. Graham T. Allison, Jr., Douglas Dillon Professor of Government and Director, Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University

Dr. Stephen E. Flynn, Jeane J. Kirkpatrick Senior Fellow for National Security Studies, Council on Foreign Relations

Dr. Lowell L. Wood, Jr., Senior Staff Scientist, Lawrence Livermore National Laboratory, and Commissioner, Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack

Dr. Philip D. Zelikow, Director, The Miller Center and White Burkett Miller Professor of History, The University of Virginia, and Executive Director, National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission)
Summary

Dr. Graham T. Allison, Jr.

Nuclear terrorism is the greatest danger facing the United States today.

• Both President Bush and Senator Kerry highlighted this threat in their first presidential debate.
• Al-Qaeda and other terrorist groups have been actively seeking nuclear weapons and radiological materials.

We must do everything technically feasible to avert nuclear terrorism.

• Like nuclear war itself, the threat of nuclear terrorism falls under the “zero-infinity paradox.” The risk of a terrorist using a nuclear weapon is very low, but the consequences to the United States from such an event would be that of negative infinity.

Thus far, our record in managing this threat is poor.

• We have made less progress during the last two years securing potentially vulnerable nuclear weapons in Russia than we did during the two years before 9/11.
• North Korea has withdrawn from the Nonproliferation Treaty, expelled International Atomic Energy Agency (IAEA) inspectors, and begun reprocessing enough plutonium to make six nuclear bombs. Given their history of trafficking in missiles and narcotics, it cannot be excluded that the North Koreans will sell their nuclear weapons materials, or even nuclear weapons themselves.
• Iran also has advanced to within months of completing its nuclear weapons infrastructure.

We have a fortunate fact in that a strategic chokepoint exists. If we squeeze hard enough, we could reduce the likelihood of nuclear terrorism to zero.

• A happy syllogism of physics exists: no fissile material, no fission explosion, no nuclear terrorism.
• We therefore must do everything technically possible on the supply side to prevent terrorists from acquiring highly enriched uranium or plutonium.
The opportunities for the defenders are best at the supply source and worst for the terrorists. We should follow the doctrine of the Three No’s: no loose nukes, no new nascent nukes, and no new nuclear weapons states.

- **No Loose Nukes** should include engaging Russia to assure the security of its nuclear weapons and materials, developing a new “gold standard” for the security of the world’s nuclear weapons and materials, and launching a Global Cleanout campaign to recover HEU from both Soviet- and U.S.-supplied research reactors as fast as possible.

- **No New Nascent Nukes** should entail such measures as closing loopholes in the NPT, preventing the development of new national HEU enrichment or plutonium reprocessing, guaranteeing the supply of reactor fuel to non-nuclear weapons states at low cost, securely storing spent fuel from civilian reactors, and persuading all states to sign the IAEA Additional Protocol.

- **No New Nuclear States** means treating as the highest priority averting North Korea’s development of nuclear weapons and ratifying the Comprehensive Test Ban Treaty.

**Dr. Stephen E. Flynn**

The U.S. national security establishment has shown an unwillingness to confront the new realities that are threatening us.

- 9/11 illustrates how warfare will be conducted against the United States in the 21st century. It will involve the use of catastrophic terrorism directed at the non-military elements of our power: our civil society and critical infrastructure.

- Adversaries know that they cannot overcome our conventional superiority, so they will seek out other opportunities to hurt us.

Our society is dependent on several essential global infrastructure networks, including those for transportation, logistics, energy, information, finance, and intellectual capital. Four imperatives have governed how we have managed these networks in the past:

- Making them as open as possible
- Making them as efficient as possible
• Making them as reliable as possible
• Making them cost as little as possible

Improving the security of these networks will require reducing their openness, efficiency, and reliability, as well as increasing their costs.

• These networks, like all market mechanisms, require public trust and confidence to work.
• 9/11 demonstrated the effectiveness of targeting these networks.

Rather than face the new realities of the national security environment, we defined these problems as falling under the concern of “homeland security.”

• This characterization has allowed the people responsible for “national security” to continue to focus on threats from other countries, including from state sponsors of terrorism.
• “Homeland security” has come to be seen as a purely domestic enterprise.

Dividing “homeland defense” from “homeland security” has further exacerbated the problem.

• The national security community defines “homeland defense” as when an adversary attacks U.S. territory from outside the United States. The U.S. Department of Defense assumes the lead role in this mission area.
• Except for a direct attack from a foreign country against the United States, the accepted definition of homeland defense is not very useful. The terrorist adversary will attack the United States from both inside and outside our borders.
• Much of our vulnerable critical infrastructure is located offshore and is privately owned.

The terrorists will exploit these vulnerabilities.

• We cannot assume that we can avert attacks against our critical infrastructure just by relying on good intelligence or offensive operations.
• It will take years to develop either an effective counterterrorism force to preempt these threats or the highly precise intelligence we need to avert them.
• We are spending too little on homeland security – just five percent of what we spend on national security. The paucity of spending on port security is especially disturbing. We need to overcome national security stovepipes and debate more directly whether, for example, to spend the next federal dollar on enhancing the defenses of Long Beach or acquiring another F-22.

• We also need to draw more on the strength of our civil society. We practiced this tradition most recently in the Second World War, but moved away from it during the Cold War, when we relied on an increasingly paternalistic and insular national security establishment.

• The private sector lacks sufficient incentives to undertake the necessary corrective measures itself. We face a “tragedy of the commons” problem. No single private sector actor owns the entire critical infrastructure, so the incentives to free ride on others’ efforts are great. The presence of many free riders means that little private spending on critical infrastructure protection has occurred since 9/11. The federal government will need to intervene directly rather than rely on the free market to finance the necessary improvements.

• Horizontal integration must be a bottom-up rather than a top-down process. We need a federal security reserve system modeled after the Federal Reserve system. Communities must recognize the vulnerabilities that arise from the interconnectedness of their local assets with other sectors.

**Dr. Lowell L. Wood, Jr.**

The Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack identified several potential dangers.

• The members focused on threats from high altitude nuclear explosions that might occur during the next fifteen years.

• An EMP attack represents one of the few ways in which the United States could die as a nation. Such an attack could devastate the U.S. civilian infrastructure and result in the eventual deaths of tens of millions of Americans.
The Commission generated numerous studies and reports. The unclassified versions are available at the Commission’s web-site (http://empcreport.ida.org/). Congressional testimonies by Commission members are also available at various levels of classification.

The EMP Commission employed a capabilities-based approach to the problem because we cannot estimate reliably the probabilities of such threats over a fifteen-year timeframe. The EMP threat to the United States has been recognized for several decades.

The STARFISH high-altitude nuclear weapons test (1962) highlighted the potential negative effects of EMP when the detonation, which occurred nearly 1,500 kilometers from Honolulu, caused substantial damage to Hawaii’s civilian infrastructure. The explosion also devastated commercial satellites that orbited near the test location.

Neither country focused on EMP effects during the Cold War because they were considered merely as a potential side effect of a much more devastating nuclear exchange.

The end of the Cold War has led experts to address EMP as a distinct problem.

The threat to the United States from an EMP attack is real.

Both nuclear weapons and the means to place them in space near the United States have proliferated.

Even short-range ballistic missiles or low-yield nuclear weapons tailored for EMP purposes are sufficient to present grave threats to American civilization.

The costs of acquiring the means for an EMP attack lie within the purchasing ability of even a moderately wealthy individual, let alone a terrorist organization.

The number of opportunities available to adversaries to attack the United States with EMP is very large.

Knowledge about Americans’ vulnerability to an EMP attack is also widespread.
The main U.S. vulnerability to EMP attack is our critical infrastructures.

- The American electric power grid is especially vulnerable to EMP. In theory, an attack could produce cascading effects that would bring down the American electric power grid on a nationwide scale.
- An EMP attack on the U.S. electric grid would produce long-lasting effects. We would not just have a blackout. We would have a “stayout” because some critical fraction of the equipment would be destroyed rather than just disrupted. Replacing these components could take a long time because much of the key equipment associated with the U.S. civilian electrical infrastructure is not manufactured in the United States.
- The various elements of U.S. civilian and military infrastructure are tightly intermixed, a situation that increases Americans’ vulnerability to an EMP attack. Such cross coupling is quite evident in the areas of electricity, communications, and finance.
- Even U.S. military systems are currently vulnerable to EMP attack. If anything, this risk is increasing.
  - The U.S. military’s dependence on electronics and electricity is growing.
  - Potential adversaries increasingly appreciate U.S. vulnerabilities in this area.
  - The hardness of the strategic forces against EMP has weakened substantially since the end of the Cold War. The current situation is unsatisfactory and continues to deteriorate.
  - Our general purpose forces are even more vulnerable, as hardening them against an EMP attack was never a priority. The prospect of an electromagnetic Dunkirk looms in the near future.

The United States can take steps to mitigate substantially its vulnerability to EMP attacks.

- The two basic approaches are (1) preventing EMP attacks and (2) limiting the damage should they occur. A multi-layered defense would include measures to enhance prevention, preparation, protection, and recovery.
• Effective Cold War practices to enhance the military’s EMP defenses could be revived.
• The costs of these measures would not be great.
• Both DHS and DOD have a role to play in reducing U.S. vulnerabilities.

The federal government will need to work closely with the private sector to counter EMP threats to critical U.S. commercial infrastructures.

• The owners, operators, builders, designers, and maintainers of these networks should work with government employees to define requirements for improvement.
• Attempts by the government to impose unfunded mandates on the private sector will not work. The federal government itself will need to pay for improving the ability of the U.S. commercial infrastructure to resist an EMP attack.
• The costs for hardening commercial networks would amount only to one percent of total expenditures if preparations are undertaken at the time when a plant is under construction. We are talking about spending approximately $10 billion annually for one, two, or three decades.
• Enhancing EMP robustness would also reduce infrastructure vulnerabilities against other related hazards such as lightning, floods, and geomagnetic storms.

Dr. Philip D. Zelikow
Four issues are especially important when evaluating the methods by which this country and government analyze threats and prepare to meet them.

• Analysis
• Warning
• Net assessment
• Joint planning

The U.S. intelligence community has become overwhelmingly focused on providing current intelligence.
• The intelligence community produces a lot of newspaper-like articles that describe what has just happened.
• The analysis that is offered typically just provides some context for the description.
• The reasons for this phenomenon are that the members of the intelligence community compete with the 24-hour news cycle, and producing largely descriptive pieces is bureaucratically safe since no one can be accused of politicizing analysis.
• We rarely produce synthesis documents or strategic analysis.
• Before 9/11, the last national intelligence estimate on terrorism was produced in 1995. It was only superficially updated in 1997.

During the Cold War, the U.S. intelligence community developed effective methods of warning against a surprise attack.
• Analysts appreciate that you cannot consistently rely on individual genius or imagination to anticipate an attack. You need to find ways of routinizing and institutionalizing the practice of imagination even within government bureaucracies with their constant changes in personnel.
• The craft of warning involves identifying the most dangerous forms of likely attack, determining indicators that could suggest that such an attack is being prepared, collecting against these indicators, and designing safeguards to prevent surprises or at least obtain additional warning time.

The 9/11 story is remarkable not because these long-established methods failed, but because they were not even applied against the adversary that was most likely to launch a surprise attack against the United States at that time.

We did not analyze the most dangerous ways we could be attacked.
• CIA analysts never worked out a scenario positing a terrorist suicide attack against the United States involving commercial aircraft as weapons.
• The notion that suicide bombers could move from trucks to other vehicles did not require revolutionary insight. A trial attorney in the Department of Justice thought the scenario so obvious that he undertook a substantial analysis to eval-
uate the legal issues associated with a decision to authorize U.S. military aircraft to shoot down commercial airliners.

- The Office of Civil Aviation Security in the Federal Aviation Administration discounted the danger of suicide hijackings because they would not offer the attacker “opportunities for dialogue.” If they had consulted experts on al-Qaeda, they would have learned that its members were not seeking such opportunities.

Analysts ignored telltale indicators of terrorist plans to attack the United States with hijacked commercial airliners.

- We did not collect against signs that terrorists were trying to learn how to fly large jet aircraft.

No effort was made to design safeguards to prevent surprise attacks involving hijacked commercial airliners, or even to obtain additional warning time against them.

- Local plans existed to deal with suicide aircraft attacks against the White House and other targets, but no nationwide plans were developed.

- NORAD considered the possibility, but always anticipated that the aircraft would come from outside the United States. The assumption was that we would have adequate time to react as the aircraft flew across the Atlantic or Pacific oceans.

The United States is not getting a level of effort equal to the amount of resources it devotes to security.

- We currently spend $550 billion on national and homeland security, and it is doubtful we can afford much more.

- The main problem is a lack of mechanisms for effective horizontal integration in the U.S. government.

- We need to better link DOD’s requirements with those of other U.S. government agencies to develop joint strategic plans against such threats as EMP and nuclear terrorism.

- The federal executive management system operates according to the finest management principles of the 1950s. We still have large, vertically integrated behemoths. We have not yet applied on a wide scale matrix organizations or the
other techniques of modern executive management that have existed in the private sector for more than a generation.

• The National Security Council, despite the growth in its staff, lacks the ability to provide effective horizontal integration. We need a national counterterrorism center, a national counterproliferation center, and other innovative structures to enhance the federal government’s ability to develop, update, and implement operational plans across the executive departments.
MODERATOR

Dr. Richard H. Shultz, Professor of International Politics and Director, International Security Studies Program, The Fletcher School, Tufts University

SPEAKERS

R. James Woolsey, former Director, Central Intelligence Agency

Michael Noll, Director for Intelligence (J-2), U.S. Northern Command

Russell E. Travers, Deputy Director for Information Sharing and Knowledge Development, Terrorist Threat Integration Center

Dale Watson, former Executive Assistant Director for Counter-Terrorism and Counter-Intelligence, the Federal Bureau of Investigation

SUMMARY

Mr. R. James Woolsey

For a long time we have been at war with three totalitarian movements in the Middle East.
The Baathist parties have been fighting us since the early 1990s. Founded in the 1920s and 1930s, they were intentionally modeled after the fascist and later communist parties. Their dream of a united Arab Middle East resembles Hitler’s dream of a 1,000-year Reich. Supported by Baathist Syria, they presently fight us in the streets of Iraq, seeking to reestablish Baathism in that country.

Our second and third enemies are Islamists. They both represent totalitarian movements that seek power under the auspices of religion.

The first of these hostile Islamist movements follows the leadership of Iran’s supreme leader Ayat Allah Ali Khamenei, who himself follows the precepts of his predecessor, Ayatollah Ruhollah Khomeini. Khamenei stands at odds both with Iranian popular opinion and the historic tradition of Shiite Islam, which favors the separation of mosque and state. This category includes the world’s most dangerous terrorist organization, Hezbollah. The Shiite Islamists have been at war with us for at least a quarter of a century, beginning with their seizure of our hostages in Iran in 1979.

The Sunni Islamists represent our third enemy. This category includes al-Qaeda and its ancillary organizations. The angry Wahabism found in Saudi Arabia, whose population includes several families that fund terrorist movements, underpins them. The fearful Saudi authorities have sought to avert attacks against themselves by both bribing the Islamists and overlooking their terrorist attacks outside the kingdom. The Sunni Islamists have been at war with us for about a decade.

Our weak response to terrorist attacks before 9/11 encouraged our enemies to attack us further. We repeated the same mistake we made when confronting Japanese aggression before Pearl Harbor.

We must recognize that we will have very little intelligence available on many important matters.

During the Cold War, we could count on collecting much useful data through satellites, listening devices, spies, and
other instruments. Both our strategic and our tactical military intelligence at the time were really quite good.

- These tools have proven much less effective against non-state terrorist groups.
- Al-Qaeda’s recent metastasizing into a number of highly autonomous terrorist cells further complicates our ability to collect intelligence on them.
- Local ordinances in the United States impede the ability of law enforcement officers to exchange information on potential terrorists with federal immigration authorities. We have unduly tied our own hands in these instances.

We must take several steps to improve our intelligence practices and enhance our security.

- We must strengthen our society’s defenses and mitigate our vulnerabilities, such as those associated with the electric grid and our other critical infrastructure.
- We must substantially improve our domestic intelligence. Improving trust and cooperation between local authorities and U.S. residents who might know of potential terrorist activities in their neighborhood is essential for uncovering terrorist cells and terrorist financing operations.
- We need to do a better job collecting intelligence overseas. For penetrating al-Qaeda cells, improving our capacities for human intelligence is much more important than strengthening our technical intelligence. We need to rely more on intelligence case officers operating under non-official cover.

The importance of intelligence reorganization has been exaggerated.

- Some intelligence reorganization might help, particularly if it improves the fusion of domestic and foreign intelligence, but the measures just mentioned are far more important than most of the recommendations offered at the end of the 9/11 Commission report. It is often said that, to a hammer everything looks like a nail. To a government commission, everything looks like a reorganization opportunity.
• Creating an “intelligence czar” would not help matters. Appointing a National Intelligence Director might help coordinate domestic and foreign intelligence, but it risks damaging the relationship between the Secretary of Defense and the military intelligence agencies that currently report to him.

To some extent, “actionable” intelligence is in the eye of the beholder. There is no objective standard.

• On the eve of the Battle of Antietam in 1862, McClellan received the greatest intelligence gift that was ever given to any American general: a copy of Lee’s battle orders that was found by a Union cavalrymen. Nevertheless, McClellan could only achieve a draw because he famously waited too long in the hope that things would get even better.

• During the late 1990s, we had opportunities to go after Bin Laden, but we declined to act because of various concerns, including over collateral damage.

Mr. Michael Noll

Intelligence is a sum of data that is aggregated into information and, ideally, turned into knowledge. This is all-source analysis.

• The J-2’s job is to communicate that knowledge, in a way that is both clear and convincing, to the right people at the right time.

• The NORAD/NORTHCOM J-2 must assess the full spectrum of threats to North America. These include both traditional strategic threats and the threat of terrorism.

• This process must contribute to both homeland defense and to the military’s support for homeland security.

• We must provide warning based on our threat assessments.

• This entire process represents more an art than a science. The principles we adhere to in providing actionable intelligence is “each according to his mission needs, their ability to understand, and their ability to safeguard secrets.”

• From our perspective as a military command operating at the theater strategic level, intelligence is actionable if it can help prevent surprises, give our leadership time to think through a problem, allow time for planning and preparation, and set
the stage for informed decision making on issues appropriate for our command.

• Sorting out the wheat from the chaff is particularly difficult. We undertake triage by evaluating the credibility of the source when presenting intelligence to decisionmakers.

Intelligence sharing at NORAD/NORTHCOM involves an extended conversation.

• Every day I discuss the threat situation in considerable detail with the command’s senior leaders.

• Achieving such understanding involves a cumulative process. It does not occur in a single moment or in a single piece.

• Intelligence sharing is still unnecessarily impeded at the lower levels of the intelligence and law enforcement communities. We must be able to see all the dots in order to connect them properly. We also must be able to create trusted networks between analysts rather than insist upon staying in our lanes.

• We share intelligence extensively with Mexico and especially with Canada. NORAD’s J-2 has Canadian intelligence officers fully integrated into its operations.

The requirement for military intelligence cannot trump civil liberties.

• Protecting civil liberties is what the war on terrorism is all about. That is what the enemy is attacking.

• We need to fuse foreign intelligence with information derived from law enforcement operations, but we must limit such fusion to information of clear intelligence value. NORAD/NORTHCOM does not collect or retain law enforcement information.

• The Office of the Secretary of Defense runs an intelligence oversight program to ensure that DOD intelligence components respect civil liberties.

• There must be a foreign threat nexus for a military intelligence organization to legitimately use information concerning domestic issues. The nexus could be a foreign intelligence operation or a foreign terrorist operation. Military intelligence should not be involved if the matter concerns simple
criminal behavior, civil disobedience, or other domestic activities not linked to a foreign threat.

One of our intelligence procedures is operational net assessment. It involves taking three different looks at any given threat, problem, or issue:

- Blue’s view of red (i.e., the intelligence picture derived from fusion)
- Blue’s view of blue (i.e., analyzing our vulnerabilities)
- Red’s view of blue (i.e., “red-teaming,” which is very demanding but essential to avoid mirror-imaging)

How you organize the information you present is very important. We often organize the information into three distinct categories

- What do we know?
- What do we not know?
- What do we think?

Success in intelligence depends on excellence in fundamentals and the performance of intelligence personnel.

- These fundamentals are recruiting, training, tactics, discipline, and retention.
- Undertaken successfully, they help mold a successful group of intelligence analysts.

Effective intelligence also requires us to know ourselves. Such self-knowledge allows us to exploit our strengths and mitigate our weaknesses.

- We Americans are fond of technology, have difficulties understanding the darker side of the world, and are very risk averse.
- We are good at technical intelligence, but bad at human intelligence.
- We are rich in resources, but impatient in applying them.

We must respect and acknowledge the unknown, and factor that into our assessments.

- What we know about a threat can be likened to an iceberg of which only ten percent is visible above the water.
- A lot of what we see is wrong.
• So the really good piece is quite small in terms of the total-
ity of the threat.
• The art of intelligence lies in assessing the whole of that ice-
berg from that tiny piece.
• But we must also push the edges with our analysis, take
some risks, and use our imagination, constantly reassessing
our assessments as new information becomes available.

Mr. Russell E. Travers
We need some balance in how we regard information sharing. Too
often it receives almost canonical status.
• Information sharing among intelligence analysts definitely
has increased in recent years. The amount of originator-con-
trolled information has declined dramatically, while the use
of tear lines has grown substantially.
• However, real constraints exist on the sharing of informa-
tion. These include the need to protect sources and methods,
liaison relationships, ongoing operations, and the privacy of
Americans. Technical barriers to interoperability also pres-
ent formidable barriers.

“Horizontal integration” is the DOD euphemism for informa-
tion sharing.
• It occurs near the data end of the data-information spec-
trum.
• But most of our failures have occurred at the “knowledge”
pole of the spectrum.
• So better information sharing will not solve all our intelligence
problems. It could result in the intelligence community simply
being wrong faster.

TTIC began operations in May 2003.
• TTIC is the one organization that by law is supposed to
have access to all information regarding terrorism collected
by the U.S. government, whether domestically or abroad. It
reports to the Director of Central Intelligence.
• TTIC is trying to remove impediments to information shar-
ing in a commonsense manner.
The planned National Counter-Terrorism Center would subsume TTIC’s functions. TTIC employs a hub-and-spoke concept of intelligence sharing. We both collect information from a number of partner organizations, including some foreign government entities, and distribute intelligence to them. An overwhelming amount of data flows across the twenty-nine separate networks linking TTIC with the other federal government agencies involved in combating terrorism. We are developing a “sanctum architecture” that will allow analysts to conduct searches across multiple networks. TTIC Online, which was established in October 2004, includes perhaps four million documents. These often have a very high level of classification. Over 120 organizations with some 3,500 users currently have access. We do not deal directly with state and local authorities or the private sector. TTIC provides information to DHS and the FBI so that they can undertake such vertical information sharing.

Last year the President directed that TTIC would become the single repository for all information on terrorist identities.

Before 9/11, there were four separate terrorist identities databases and thirteen national watch lists. This information was not very interoperable or accessible. TTIC will now store this information and provide it, in an unclassified form, to the Terrorist Screening Center.

We have many analysts involved in intelligence sharing, but few of them actually expand our knowledge of the threat.

Since 9/11, thirty to forty intelligence fusion centers have begun operating. Their sizes range from tens to hundreds of people.

But approximately half of their personnel perform support functions (e.g., producing products, managing overhead, and maintaining the IT infrastructure). Even the fifty percent who allegedly conduct “analysis” consists largely of watch officers, warning officers, and those who compose morning
intelligence briefings. Only a few people actually produce knowledge rather than simply repackage it.

- When you share information with all these fusion centers, you end up with a lot of redundant and often shallow analysis from enthusiastic amateurs. A lot of trash comes across the wires, and we must be careful about who is receiving and acting on it.

- Some people mistakenly believe that the dots will get connected randomly, that you can just throw information over the transom and somebody will come up with the next 9/11 plot. Instead, extraneous background noise likely will obscure the data that would have averted the next intelligence failure.

- Unfettered information sharing without the appropriate business process can have a pernicious impact. The proposed National Counter-Terrorism Center should help establish the correct business process.

**Mr. Dale Watson**

State and local law enforcement agencies as well as local responders play the lead role in protecting us against the next terrorist threat. They will supply most of the intelligence that is truly “actionable.”

- The United States has some 600,000 police officers, over 18,000 police departments, and more than 3,200 sheriff departments.

- These individuals, and not national or foreign intelligence agencies, are best situated to detect and avert terrorist attacks in the United States because they are near or on the scene of the act.

No federal law or other legal instrument requires state and local law enforcement agencies to share information. We must establish appropriate incentive structures to encourage voluntary cooperation.

- Clear incentives for such collaboration do exist. Information sharing makes local law enforcement better. In addition, all of those involved in law enforcement want to contribute to the war on terrorism.
• The greatest incentive for local actors is that they want federal agencies such as the FBI to share information with them. The federal government also can supply money and other resources.

• Existing technology is adequate for sharing information between state and local law enforcement officers and their federal counterparts.

• But you need rules to govern such information sharing. They must address such questions as what to share and what penalties apply when someone violates the rules.

• Systems and rules for information sharing must be built from the bottom up. Washington can no more determine these processes than it could the growth of the Internet.

Since 9/11, the American public has become much better educated about potential terrorist threats. People are prepared now to inform law enforcement representatives about potential threats. Nevertheless, we may need to reevaluate the red-yellow-green terrorist warning system.

• It is not clear what it asks the American people to do.

• The system must better distinguish between nationwide and local threats.

• We must not inadvertently alert the bad guys that we are on to them.
SUMMARY

Canada and the United States not only share a unique and critical economic relationship, but we share a deep commitment to common values which are basic to both our countries. We have defended those values together through several wars, including today’s fight against terrorism. Canada has pledged $300 million in humanitarian aid and reconstruction assistance in Iraq, and we are training Iraqi police. Canadian Prime Minister Paul Martin created a new department to bring together a number of capabilities, including security and intelligence, federal policing and enforcement, emergency preparedness, and border security.

- The Prime Minister also formed a new Cabinet Committee on Security, Public Health and Emergencies. The new position of National Security Advisor has the role of assisting the Deputy Prime Minister to pre-
pare and implement Canada’s first statement of national security policy, *Securing an Open Society: Canada’s National Security Policy*, which was released on April 27, 2004.5

- After 9/11, the Canadian government took steps to enhance security. Legislation was introduced and passed strengthening Canada’s security and intelligence. The “Smart Borders” process was launched by the Deputy Prime Minister and by U.S. Homeland Security Secretary Tom Ridge.

Osama bin Laden has identified Canada as fifth on the list of countries to attack. We see the current terrorist threat as our problem too. Prior to September 11, airline terrorism had taken place in Canada, with the June 1985 bombing of Air India flight 182 killing 278 Canadians and twenty-two U.S. citizens. There are also health threats such as SARS and electrical blackouts such as the one in 2003 that affected both Canada and the United States. The National Security Policy begins with an assessment of threats to Canada and Canadians and also by setting out an approach to national security based on our values, such as democracy, rule of law, respect for human rights and pluralism.

- The policy statement defines three core national security interests of Canada, which are: 1) protecting Canada and Canadians at home and abroad; 2) ensuring that Canada is not a base for threats to our allies; and 3) contributing to international security.

- There is a commitment to building an integrated security system framework. First, a government threat assessment capability residing in the new Threat Assessment Center is part of Canadian Security Intelligence Services. All information on threats to Canada is brought together in one place, analyzed, and disseminated. Next is the development and deployment of protection and prevention capabilities, with the new Department of Public Safety and Emergency Preparedness leading the effort. This strengthens relationships between federal and provincial agencies, first responders, and

action with the United States. Thirdly, more effective consequence management capabilities are required. Finally, a flexible and adaptive system needs continuous evaluation coupled with oversight and review. All of these activities in the integrated system will connect provinces, first responders, international partners, and the private and public sectors.

• The National Security Policy sets forth the importance of building an integrated security system. There are six particular areas for action: intelligence, emergency planning, public health emergencies, transportation security, and international security.

• Security intelligence is a top priority. Canada is adapting to U.S. systems and developments. In emergency management, we are modernizing government emergency operations centers, creating a new critical protection strategy and cyber security task force, and working with the U.S. Secretary of Homeland Security. SARS and the electrical blackout brought more effort to our attention. The strategy provides a structure for a robust public health emergency system as a critical element in defense against threats. Transportation security involves enhancing maritime security and securing ports, cargo, and background checks for workers. There must be an integrated approach with all agencies in government, such as the Navy, Coast Guard, Fisheries, the Department of Transportation and the border agencies. Our air systems are integrated with those of the United States with an open skies agreement and NORAD.

• Border security improvements include the Smart Borders plan between the United States and Canada, established in 2001. Biometrics are being applied to passports. A broader international trade agenda with U.S. partners is important.

• Risk management progress has been made in implementing the Free and Secure Trade (FAST) program and NEXUS, Canada/U.S. programs for low risk, pre-approved travelers and commercial goods. We also have border enforcement teams of American and Canadian representatives.
We must not allow terrorists to determine our future. This includes our economic future and prosperity. We have found solutions with business leaders that protect our economic security and physical security. The following are statistics that reinforce the vital importance of this type of security.

- Canada and the United States have the largest bilateral trading partnership in the world. The U.S. market is important to Canada.
- Canada is the number one export destination for the United States.
- U.S. foreign direct investment in Canada was $228 billion in 2003. This is over eleven percent of American investment abroad.
- Forty percent of trade between our countries is intrafirm trade between the same company that operates on both sides of the border.
- Highways and railway infrastructure are tightly integrated.
- Canada is America’s number one energy partner. Canada is the single largest exporter of oil and refined products to the United States. We supply seventeen percent of all American imports, more than Saudi Arabia. We supply ninety percent of natural gas imports and one hundred percent of United States uranium imports.

We must have a mutual commitment to the security and prosperity of our continental space. Canada is intensely focused on homeland security. But there is more work to do. In terms of border security, far more immigrants enter the United States illegally than enter Canada and more than one-third of our refugee claimants enter Canada through the United States. None of the September 11th hijackers got into the United States from Canada. In both countries there are people who are intent on taking advantage of our openness. It is our challenge to make sure they don’t succeed.

- Ahmed Rasam was apprehended by a border guard from Canada in December 1999. Subsequently, there was intense bilateral cooperation in investigation of that incident. Rasam
was considering a range of targets in Canada. This was a sobering wake-up call.

- The United States and Canada both accept an almost equal portion of refugee claimants.

The National Security Policy also recognized that the security of Canadians is enhanced by investments in participation in international peace and stability. The Policy envisages additional investments in our military; enhanced efforts at capacity-building assistance for failed and failing states; activities to prevent weapons of mass destruction proliferation, such as participation in the Proliferation Security Initiative; and activities to defuse inter- and intrastate conflicts. Canada has worked with the United States in integrating efforts to enhance our security.

- We have enhanced our defense cooperation in North America and engaged our military bilaterally on continental security by entering NORAD in 1958. The aerospace defense efforts of our two countries have become fully integrated and are continually evolving. Our respective intelligence communities have established a very close relationship, sharing information on threats to North America.

- Maritime security has been enhanced and we work with the United States in the binational planning group to explore cooperation in NORAD and to extend it to the maritime sector.

- Beyond North America, Canada cooperates daily in the war against terrorism.

As outlined in our National Security Policy, our top priorities are to protect Canada and Canadians against threats, and to ensure that we are not a source of threat to our ally, the United States. For this framework and our actions to be effective, Canada must integrate efforts with the United States. We are partners. It is in our vital interest to make sure this partnership grows. In a recent meeting between the Canadian Deputy Prime Minister, Anne McLellan, and Homeland Security Secretary Tom Ridge, they called for officials to look at a comprehensive framework to tie all of the cooperation together and strengthen it. Canada remains
committed to North American security and committed to a collective effort with the United States.
Session 3

Relating Homeland Defense to Homeland Security

MODERATOR
Dr. Jacquelyn K. Davis, Executive Vice President, Institute for Foreign Policy Analysis

SPEAKERS
Lieutenant General Edward G. Anderson III, USA (Ret.), former Deputy Commander, United States Northern Command
The Honorable Stephen M. Duncan, Director, Institute for Homeland Security Studies, National Defense University
Andrew Howell, Vice President for Homeland Security, U.S. Chamber of Commerce

SUMMARY
Lieutenant General Edward G. Anderson III, USA (Ret.)
A recent NORTHCOM publication\(^6\) noted that homeland security strategy is focused on preventing and responding to terrorist attacks

within the United States, while homeland defense is concerned with the protection of U.S. sovereignty, territory, domestic population and critical defense infrastructure against external threats and aggression, and not simply those emanating from terrorists.

- For homeland security missions, particularly those within the homeland, DHS is in the lead with NORTHCOM providing support. DOD, however, would take the lead in homeland defense activities, generally understood to encompass those undertaken to counter foreign threats.
- Often, the difference between homeland security and homeland defense is driven less by operational than by resource issues, especially in planning the “response” function for a particular homeland security or homeland defense mission.
- Scenario-based exercises that focus on “responding” to an event, such as Determined Promise ’03 and Determined Promise ’04, as well as the TOPOFF series, have clearly had DHS in the lead coordinating local, state, federal and military resources.

Both homeland security and homeland defense strategy needs to focus on proactive measures, specifically actions that detect, deter, and prevent incidents, rather than simply responding to them. But we currently lack clearly defined command relationships for these missions.

- We should be in the prevent phase of a mission if we have specific information regarding a particular domestic attack. Otherwise, we should be in the deter phase, and local, state, federal and military agencies can offer valuable contributions at that stage.
- Command relationships, however, are unclear for these types of missions. Which agency is identifying, coordinating and synchronizing the mission requirements and integrating the contributions made by different organizations? Who is developing a common operating picture, or developing alternative courses of action if deterrence fails and prevention becomes necessary? Too often disparate organizations are acting inde-
pendently, without any coordination and synchronization of efforts.

- Confusion over command relationships for these types of missions offers the enemy an operational seam through which he can attack our vulnerabilities.

We should establish a permanent standing taskforce of representatives from local, state, federal, military and private sector organizations, tasked with coordinating efforts and developing a common operating picture.

- It could help develop and execute deterrence plans. For instance, if there were indications that al-Qaeda wanted to target our subway systems, the taskforce could coordinate deterrence missions, such as deploying the National Guard to the New York City and Washington, DC subways. Such measures would disrupt the planning cycle associated with the threat.

- The interdiction of a ship represents another deterrent mission to which local, state, federal and military forces could actively contribute.

- We need to undertake these types of missions, and DHS, not DOD, should lead them.

DHS should be responsible for carrying out the war on terrorism within the homeland.

- All capabilities – local, state, federal and military – should be made available for utilization in a coordinated fashion.

- In proactive homeland security missions, the military should maintain operational control over military forces, but DHS should have overall command.

- The more successful we are in detecting, deterring and preventing incidents, the less we will have to respond to them.

- We are capable of carrying out the response phase of a mission, but we need to place greater emphasis on detection, deterrence and prevention.

**The Honorable Stephen M. Duncan**

There are several reasons for the separation between homeland security and homeland defense.
• It reflects the policy preference of the current Secretary of Defense. In November 2002, Secretary Rumsfeld noted that, if asked, the military could provide help with domestic emergency assignments, but only on a short-term basis. And in March 2003, he noted that the best way of defending America was by taking the fight to the enemy abroad.

• Other governmental institutions may be more appropriate for a particular task. The Armed Forces is highly regarded in American society, and Congress is eager to assign the military new missions, as occurred in 1989 when it was tasked with fighting the international drug war. Yet other agencies may be better suited for a given task, and many of them, such as the Coast Guard in the past, are fearful of DOD encroaching upon their turf.

• The Posse Comitatus Act contributes to the distinction between homeland security and homeland defense. But there are a number of statutory exceptions to that act, such as those involving missions related to counter-drug operations and threats arising from weapons of mass destruction. We may not need to change it, but given the rapid pace of change today, we should examine ways it could allow for greater flexibility in achieving policy objectives.

• A final reason involves money. DOD’s budget far exceeds that of other governmental agencies, and therefore agency leaders, and also governors, are tempted to find ways of utilizing DOD resources without having to cede substantial authority to them.

The distinction between homeland defense and homeland security is no longer useful. We are now engaged in a war of a different kind, and the lack of horizontal integration between government agencies is unacceptable.

• Terrorism today neither stops nor starts at our borders. There is less of a difference between foreign and domestic, between war and crime, and between military assignments and civilian functions.

• The American homeland is now part of the battle space.
• There is too little coordination between DOD and civilian agencies. A recent report\(^7\) by the Defense Science Board (DSB) noted that DHS has very little understanding of NORTHCOM's role, and that, as of early 2003, the senior DOD leadership had not actively sought partnerships with civilian agencies.

• Similarly, both military and DHS planners remain uncertain about the relationship between DOD and DHS, a factor which negatively impairs the process of planning a response for a major attack. For instance, planners at other agencies remain uncertain as to how many hospital beds DOD could make available in case of a catastrophic attack.

We must integrate all of our military and civilian experience, capabilities, technology and planning to meet the new threat.

• Under Homeland Security Presidential Directive-5, issued in early 2003, the United States government is responsible for establishing a single, comprehensive approach to domestic incident management, and ensuring that all levels of government have the capability to work efficiently and effectively together.

• Effective integration will require unprecedented interagency cooperation in the assessment of national security and homeland security threats and vulnerabilities.

• It may require an interagency budgetary planning process with the OMB involved from the beginning, so the President can know how to decide on resource issues.

Successfully waging the war on terrorism may necessitate a reevaluation of some of the basic roles and missions of the Armed Forces.

• Military units may have to be pre-assigned exclusively to homeland security missions.

• The military may need to engage in operations regarded by some as law-enforcement missions. Recently, senior military officers rejected calls for involving the Armed Forces

---

\(^7\) There are two volumes to the report, which were completed in 2003/04. Volume I represents the consensus view of the task force. Volume II is a compilation of four sub-panel reports whose findings may not represent the consensus view of the task force. They can both be found at [http://www.acq.osd.mil/dsb/reports.htm](http://www.acq.osd.mil/dsb/reports.htm).
in a direct role in combating the illegal narcotics trade in Afghanistan. Revenues from opium funds al-Qaeda and other anti-coalition forces. While the military is currently over-extended, this decision should have been made within the overall context of the war on terrorism, not within the narrower context of its near-term impact on the Armed Forces.

- We may need to consider the complete restructuring of the Armed Forces, both active and reserve components. It won’t happen in the short-term, given the global war on terror. It will likely require the creation of a commission, not unlike the 9/11 commission, making recommendations on the force structure needed to meet future security threats.

Now is the time to be bold and candid, and to reexamine objectively the processes we use to formulate and execute both national military strategy and our strategy for homeland defense and homeland security.

- General Peter Pace, Vice Chairman of the Joint Chiefs of Staff, noted that the interagency process is effective in terms of presenting the President with options, but that there is little coordination in executing decisions.
- He suggested the establishment of a joint interagency task force, where the designation of the lead agency would depend upon the nature of the mission assigned to the taskforce, and it would be responsible to the National Security Council.
- We need to improve horizontal integration to better determine the relative importance of our vulnerabilities, to establish budgetary priorities, and to execute policy decisions.

Major General Timothy J. Lowenberg

The DSB 2003 summer study called for leveraging the unique capabilities of the National Guard and other reserve components to address gaps that arise from overly fixed divisions between homeland defense and homeland security. These gaps create vulnerabilities to our security, and there were four factors that led the DSB to make this recommendation:

- The Guard’s established command, control and communications infrastructure and capabilities;
• The Guard’s demonstrated record of effectively responding to catastrophic emergencies both before and during 9/11;
• The Guard’s responsibilities under existing state laws in several states and territories; and,
• The relationship that Adjutants General and other senior National Guard officials have with governors and other local, state, and federal officials.

There are a number of ways for leveraging the capabilities of the National Guard
• A majority of Adjutants General, besides having military command responsibilities within their respective state, are also the senior official responsible for managing emergency management tasks within their respective states.
• The JFH in a majority of states also carries out civilian emergency management and consequence management functions.\(^8\)
• The National Guard has a physical presence throughout the country, while there are vast regions without an active duty Army or Air Force presence, and the major installations for the Navy, Marine Corps and Coast Guard are largely confined to maritime port areas. The National Guard’s extended presence is important when considering that every terrorist attack is local.
• The Emergency Management Assistance Compact, a mutual aid agreement between states, allows for the provision of out-of-state personnel and equipment when in-state resources are overwhelmed.
• A highly robust IT system underpins the National Guard’s command and control arrangements, allowing every Adjutant General to both provide and access information. Ideally NORTHCOM should be able to access this information to enhance situational awareness.

---

\(^8\) There is a standing Joint Force Headquarters in 50 states, two territories, the Commonwealth of Puerto Rico and the District of Columbia. Each is led by its respective Adjutant General (or, in the case of the District of Columbia, by the Commanding General), who is responsible to the Governor of the state.
Within Washington State, the domestic security infrastructure encompasses a number of committees that facilitate the provision and exchange of information from relevant individuals and organizations, and which assist the Adjutant General as the senior emergency management official for the state.

- The Emergency Management Council (EMC) advises the Adjutant General and the Governor on the state’s overall readiness for all hazards, and among its membership are police and fire chiefs, city administrators, county officials, state agency representatives, and private sector officials.

- The Committee on Homeland Security, a subcommittee to the EMC, includes representatives from both the Washington State Hospital Association and the Washington Public Ports Association, in recognition that both medical surge capacity and port security represent two vital concerns.

- The E-911 Advisory Committee ensures that the 911 system is effective, and our meetings include representatives from the telecommunications industry.

- The State Interoperability Executive Committee ensures, among other things, that spectrum allocation is coordinated with the Federal Communications Commission, and that emergency communications equipment is interoperable.

- Lastly, the Domestic Security Executive Group, formed shortly after 9/11, involves the governor and senior cabinet executives, the attorney general, the Adjutant General, the governor’s chief of staff and includes senior policy advisors.

  - This structure represents a system of systems, with the Adjutant General facilitating horizontal integration between the different units and stakeholders. It has enabled us to respond to numerous in-state disasters over the last several years.

  Through partnerships with foreign countries, the National Guard from individual states has worked towards creating a layered defense on a global basis.

  - We have established partnerships with countries in central and Eastern Europe, the former Soviet Union, South America and Asia, and Africa.
• We have helped the Thai National Security Council establish a national call center to help combat a Muslim insurgency in two southern provinces.
• We are also providing Thailand with assistance on port security to ensure that cargo leaving from the Port of Laem Chabang, destined for the U.S. west coast, is more secure.

Before amending the *Posse Comitatus Act*, we should ask several fundamental questions.
• What is the likelihood that we will require manpower levels in excess of that in the National Guard to execute domestic laws?
• What is the need for a force above and beyond that attainable through using the numerous exceptions that already exist within the Act?
• Are there any risks associated with altering the Act to provide a manpower surge capacity above and beyond what is currently available and legally feasible?

**Mr. Andrew Howell**
The private sector needs to be involved with all levels of government – federal, state and local – in terms of planning and responding to terrorism, natural disasters, and other hazards.
• A first responder will often be from the private sector. Planning exercises need to incorporate not only conventional first responders – police, fire departments, the Emergency Medical Service – but also the private sector.
• We have had success in coordinating planning between hospital associations and the hospital bed industry in developing surge capacity and, in particular, ensuring that there would be a sufficient number of burn beds as part of a response function.
• The private sector is now involved in scenario-based exercises like TOPOFF, and it provided valuable input into the DHS *National Response Plan*.9

---

9 The *National Response Plan* establishes a comprehensive, all-hazards approach to enhance the ability of the United States to manage domestic incidents. It can be accessed at [http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf](http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf)
The best way to secure the private sector’s active participation in planning is by emphasizing that preparedness is a good investment.

- Contingency planning helps ensure business continuity, a primary interest of shareholders. Through acting on these incentives, the private sector would further both private and public interests.
- The private sector also needs tangible guidance. For instance, DHS’s *ReadyBusiness* website provides small and medium-sized companies with useful information on what they can do to safeguard their operations from a variety of hazards.\(^\text{10}\)
- Framing the issue in terms of risk management may also encourage greater private sector participation in planning. The average owner of a small- and medium-sized enterprise does not believe their company will actually be targeted by terrorism. But they are more likely to engage in planning if they understood that terrorism could disrupt their supply chains or have other indirect effects upon their business.

The National Guard is a shared human resource, and from the perspective of the private sector, predictability in their use is important.

- National Guardsmen are predominantly employed by the private sector, and firms need to know how for long their employees will be called up, for what purpose, and when they will return. Currently there is too much unpredictability, given the foreign deployment of the Guard and the Reserves.
- Both the private sector and the Armed Forces provide training to Guard and Reserve members, and therefore both sectors of society benefit. It is critical for the private sector to continue employing Guard and Reserve members, and continued unpredictability is going to increase the challenges on small- and medium-sized enterprises.
- We should be asking fundamental questions in terms of human resource management. Specifically, what type of skills are required for Guard and Reserve members, and how will they

\(^{10}\) The website can be accessed at [www.ready.gov/business/index.html](http://www.ready.gov/business/index.html).
be used in the future? How can both the Armed Forces and the private sector jointly build careers for these individuals? Both the public and private sector need to cooperate in terms of allocating risk management responsibilities.

- The private sector owns much of the nation’s critical infrastructure, has been protecting it for years, and from its perspective the core challenge is risk management.
- Both the public and private sectors need collectively to determine the risk management responsibilities each will assume and pay for. This dialogue is only in its initial stages.
- Inevitably there will be coverage gaps, and ultimately these need to be mitigated by determining who will pay to close them.
- There has been much information sharing, but we need to create more incentives for encouraging the public sector to provide information useful for homeland protection.
Session 4

Essential Capabilities for a Layered and Integrated Homeland Defense

MOMERATOR
Dr. Robert L. Pfaltzgraff, Jr.

SPEAKERS
Lieutenant General Joseph R. Inge, USA, Deputy Commander, U.S. Northern Command
Lieutenant General H. Steven Blum, USA, Chief, National Guard Bureau
Vice Admiral Terry Cross, USCG, Vice Commandant, U.S. Coast Guard
Lieutenant General Henry A. Obering III, USAF, Director, Missile Defense Agency

SUMMARY
Lieutenant General Joseph R. Inge, USA
Our nation is at war, and many of our sons and daughters have placed themselves in harm’s way to serve their country.

• Our military, and especially the Reserve and the National Guard, represent a national treasure that other nations do not possess.
• Through education provided by the Guard, and through the experience gained from serving in combat situations, many
in the Guard will be well-placed to assume positions of leadership in the future.

- The country will be well-lead. The Guard will be an educated force, eager to serve their country.

NORTHCOM is a product of 9/11, having been formed in October 2002, to have a full operational capability by October 2003. We have a number of capabilities in place that allow us to contribute to homeland security and homeland defense missions.

- The JTF-CS provides support to the lead federal agency in managing the consequences of a chemical, biological, radiological, nuclear or high-yield explosive incident in the United States, its territories and possessions.
- Joint Task Force-North in the past provided counter-drug support to federal, regional, state and local law enforcement agencies throughout the continental United States. Recently its mission was expanded to include counter-terrorism.
- NORTHCOM understands that a civil agency will lead consequence management missions. Military forces, operating within a military chain of command, will work in support of the designated lead federal agency.

We have also made significant progress in terms of establishing effective cooperation with other military, as well as civilian, agencies.

- Shortly after joining NORTHCOM I met with General Frank Libutti, the Undersecretary for Information Analysis and Infrastructure Protection at DHS. We reviewed the existing collaboration between the two organizations, and as DHS and NORTHCOM mature there will be greater levels of interaction and integration.
- We are working closely with the Coast Guard, coordinating on maritime issues for both our inner waterways and the outer edges of NORTHCOM’s area of responsibility.
- We also have a very close relationship with the National Guard Bureau. Prior to becoming its Chief, General H. Steven Blum was Chief of Staff at NORTHCOM. There are multiple ways in which we can work with the Guard. In some instances, they
remain in Title 32 status, under the control of the adjutant general and the governor. In other cases, they can be led by a taskforce whose commander is operating under both Title 10 and Title 32. How they are utilized depends upon a determination of the best arrangement required to complete a particular mission.

- NORTHCOM also maintains an interagency cell with representation from fifty different agencies. NORTHCOM needs to continue to grow and improve, and there are a number of issues and areas that will receive greater attention in the future.

- As to legal reform, and specifically the Posse Comitatus Act, we should be pro-active and determine what actions need to be undertaken, rather than focusing on how our laws restrict courses of action.

- We need a more robust capability of countering the threat from WMD. We also need to develop defenses against cruise missiles and UAVs.

- Much progress has been made on facilitating intelligence sharing, and more progress is needed. However, I now worry more about what we do not know than whether or not we are sharing a sufficient amount of information.

- We need to ensure that our Armed Forces continue to be properly trained and ready for duty.

- We need to continue to work closely with federal agencies, such as FEMA and the FBI, with our international partners, and with the private sector.

**Lieutenant General H. Steven Blum, USA**

The National Guard has undergone a fundamental change since 9/11, assuming an active role in satisfying the requirements of a number of stakeholders.

---

11 Guardsmen are called up for active duty for national service under Title 10 of the U.S. Code. Title 10, Section 10103 states, “Whenever Congress determines that more units and organizations are needed for the national security than are in the regular components of the ground and air forces, the Army National Guard of the United States and the Air National Guard of the United States shall be ordered to active duty and retained as long as so needed.”
• The President is now asking the Chief of the National Guard Bureau whether the Guard is prepared to contribute to homeland defense, homeland security, and in-state missions, while engaged in combat.
• The Secretary of Defense is asking how the Guard can become more accessible to DOD and better support homeland defense and homeland security missions, as well as respond to multiple domestic events.
• Combat Commanders, such as those from NORTHCOM and U.S. Pacific Command (PACOM), are asking whether we can provide forces and capabilities that resemble those of the Marines or the Chemical Biological Incident Response Force (CBIRF).
• State governors want to be assured that they have both the required numbers and the correct composition of forces needed for in-state homeland defense and homeland security missions.

The National Guard is engaged in both civil and military activities, from combat missions overseas, to supporting law enforcement here at home and providing consequence management capabilities in support of civilian agencies.

• Recent civil missions include hurricane relief efforts in Florida. Through the Emergency Management Assistance Compact, we had twelve states provide assistance to Florida, with another twenty-one ready to offer assistance if asked.
• 115,000 Army and Air National Guardsmen are on active duty abroad, and the Guard is well-represented in Iraq.
• Guardsmen from Alaska and Colorado are providing assistance in operating our nation’s ballistic missile defense system.
• We are also actively engaged in forward deterrence in critical regions of the world through our military-to-military partnerships with foreign countries. For instance, General Lowenberg mentioned the assistance we are providing to Thailand in support of its efforts at combating its insurgency. These and similar efforts support combat commanders at PACOM, CENTCOM and U.S. Southern Command. Some of our for-
eign partners are now NATO members with forces in Iraq and Afghanistan, and our contributions were significant in assisting their military transformations.

At the strategic level, the Guard provides support to the combat commanders. At the tactical level, we provide assistance in support of a lead federal or state agency.

- The National Guard Bureau provides resources and policy guidance so that each state-level JFH is empowered to assist the combat commanders. We also serve as an intermediary between the combat commanders, the adjutants general and governors, and the Departments of the Army and Air Force.
- We provide depth to the active components. The Secretary of Defense wants all active forces to have both joint and expeditionary capabilities, capable of being deployed within seventy-two hours, for a thirty-day period. For longer missions, reserve components would provide assistance.
- Wherever possible, the National Guard will be on the scene within twenty-four hours for its Title 32 missions. It will be the first military responder for homeland defense missions and in support for homeland security operations.

Through unprecedented cooperation with NORTHCOM, Joint Forces Command, the Office of the Secretary of Defense, and the Departments of the Army and Air Force, we are now managing the human resource capability of the National Guard to enable it to successfully complete both its state and federal missions.

- Approximately twenty-five percent of the National Guard is already deployed, and another twenty-five percent is preparing to replace them. The remaining fifty percent of the National Guard is neither overseas nor scheduled to be sent abroad.

- Many of our capabilities were well-suited to countering the Soviet threat, and therefore require modification. For instance, the Guard has seventy percent of the Army’s artillery, and it is not deployable nor modernized. Many of our units will be
retrained with more pertinent skills, to allow them to function, for instance, as military police and medical units.

- Both the Army and Air National Guard possess resources and capabilities that could be melded and better utilized within a joint structure. It matters little whether a medic, truck, or military police are part of the Army or Air Guard. They can all be utilized within a joint structure, and doing so will allow us to leverage our resources.

- Almost every state currently has at least fifty percent of its National Guard available for deployment. In some cases, we have had to rebalance the mix of forces to ensure that governors have the proper combination of capabilities.

- The National Guard is now capable of sharing real-time information, allowing it to develop a common operating picture. We also established twelve CBIRF units through amalgamating resources and personnel from existing Army and Air Guard units. Previously, only one CBIRF team existed, covering the District of Columbia.

**Vice Admiral Terry Cross, USCG**

The challenge of establishing layered defenses within the maritime arena centers on being able to locate the enemy without disrupting the flow of legitimate commerce and without depriving law-abiding citizens of their civil liberties.

- We must be able to find the enemy amidst thousands of legitimate vessels, all looking alike.
- Our economy, and indeed the global economy, is dependent upon our maritime trade. Apart from bilateral trade with Mexico and Canada, ninety-five percent of the exports and imports into the United States arrive by sea.
- WMD adds further complications. They can be placed on a legitimate ship, operated by a legitimate captain and crew.

The Coast Guard can contribute to the war on terrorism by applying its experience in counter-narcotics and illegal migrant interdiction.

- With help from the U.S. Navy and other partners, this year we set a record for cocaine interdictions at 240,000 pounds.
Effective interagency and international cooperation, as well as access to specific intelligence, are some of the reasons for this success.

- It is also easier to operate in a low-density environment. Seventy-five percent of the cocaine was seized in the eastern Pacific, thousands of miles from the U.S. coastline.
- It is much more difficult, because of increased traffic density, to interdict terrorists or illegal drugs in the arrival zone near our ports. By the time a weapon has reached port, it is a serious problem.

The Coast Guard’s Maritime Strategy for Homeland Security encompasses four goals: (1) enhancing maritime domain awareness; (2) creating and overseeing a maritime security regime; (3) increasing operational presence and enhancing deterrence; and (4) improving our response posture.12 It provides depth in terms of geography, and in legislative reach, given the utilization of multiple security regimes.

- Enhancing maritime domain awareness, which is key for establishing defense in depth, requires improved intelligence. To achieve this, the Coast Guard has established Maritime Intelligence Fusion Centers on each coast, and we have more than tripled the number of personnel involved in information collection and analysis. The Coast Guard has also become a formal member of the intelligence community.
- We are also expanding upon our maritime domain awareness surveillance system. Already, we have expanded from twenty-four to ninety-six hours the advance notice of arrival for ships entering a U.S. port. This will allow us more time to check crew, passenger and cargo lists with our databases, and thereby prioritize ships for boarding or interdiction.
- Our domain awareness will also be enhanced with the application of advanced technology, such as automatic information systems. It will allow vessels to be identified and checked, and it will be a requirement for all ships coming to the United States and engaged in international trade with cargo over...
300 gross tons. It is a fairly short-range system, but we hope to have a longer-range system that would give us the ability to track vessels worldwide.

The Coast Guard has also made progress in achieving the other goals of its strategy.

- We have established domestic and international security regimes for combating terrorism and WMD proliferation. The International Ship and Port Facility Security Code require all ships and overseas port facilities to have security plans as well as security officers. Coast Guard security teams are currently involved in assessing security at overseas ports.
- The Maritime Transportation Security Act of 2002 is the domestic equivalent, having similar requirements for all U.S. vessels and ports. It also requires the development of area security plans and the establishment of area and port security committees with representation from state and local governments, port authorities and private industry.
- We are improving our response posture with the addition of hundreds of boats. This has allowed the Coast Guard to increase in size by twelve percent in the last three years.

**Lieutenant General Henry A. Obering, III**

We are currently in an evolving security environment with respect to missile proliferation and missile defenses.

- When we signed the Anti-Ballistic Missile Treaty with the Soviet Union in 1972, there were about eight countries with ballistic missile technology. Today there are over twenty, with many of them unfriendly towards the United States. Withdrawing from the treaty has allowed us to proceed on countering that threat.
- Weapons non-proliferation regimes are necessary, but alone are insufficient to deal with the threats presented by the Iranian and North Korean missile programs. A nuclear North Korea with intercontinental missiles could hold our cities hostage. The resources devoted to missile defenses protect us from that and similar contingencies. We cannot assume
the rationality of the state and non-state actors that wish to do us harm.

• Missile defense is rapidly becoming a core competency within the U.S. military, given the success of the Patriot Advanced Capability-3 (PAC-3) and Patriot systems in Operation Iraqi Freedom, and we are beginning to have the additional capability of countering long-range missile threats.

An effective missile defense will have a number of components and features. Most importantly, it will be a layered defense, facilitating synergy between the boost, midcourse and terminal phase of a missile’s trajectory.

• An effective defense will have a variety of basing modes (land, sea and space), which allows for both flexibility and persistence in terms of destroying incoming ballistic missiles.

• In the boost phase, it will employ an airborne laser, while ground-based missiles would be used in the midcourse range. The terminal phase will include the PAC-3 system, the Terminal High Altitude Area Defense (THAAD) system, and the Medium Extended Air Defense System (MEADS) that we are developing with our European partners.

• Each of these systems will be supported by a family of sensors, built upon the foundation of an integrated command and control battle management communication system. Once a missile launch is detected, that information could be shared with the other sensors in the system. The integration of our sensors and interceptors will expand both the detection and the engagement zone for each particular system.

In December 2002, President Bush decided that we would begin an initial set of deployments in 2004, which would serve as a starting point for fielding future capabilities.

• The first step in our implementation strategy is building a defensive capability against North Korea’s long-range missile programs, followed by developing a capability against threats emerging from the Middle East. We will then continue to expand our capabilities to include protection for our deployed forces and allies, and lastly, we will increase the
depth of our protection with additional layers of interceptors and sensors.

- As of October 2004, we had five interceptors installed in Alaska, and six by November. We added two more interceptors in California in December. In the Sea of Japan, we had two Aegis ships in October 2004, with five by the end of 2004.
- By the end of 2005 we will have eighteen ground-based interceptors, as well as eight sea-based Aegis Standard Missile-3 (SM-3) interceptors.
- Our testing program has built confidence. We have successfully tested three times the booster rocket that we have in Alaska. Since 2001, we have been successful in five of the last six tests of our kill vehicle prototype.

We expect a number of significant enhancements to our land, sea and space-based capabilities by 2007.

- We will have twenty-eight interceptors in Alaska and California.
- We will have deployed twenty-eight SM-3 interceptors on eighteen Aegis ships.
- We are on schedule for launching two space satellites. Boosting our space-based capabilities is vital, since it will allow for greater global coverage.
- The first flight of a kinetic energy interceptor will also occur in 2007.
- We recently awarded a contract for the development of a multiple kill vehicle. This capability will allow us with one interceptor to kill multiple warheads, and it will be available later in the decade.
Dinner Address

Keeping America Safe

Progress and Partnerships in the 21st Century

Admiral James M. Loy, USCG (Ret)
Deputy Secretary, Department of Homeland Security

SUMMARY

The post-9/11 security environment is as different from the pre-9/11 period as the challenges of the Cold War were different from the dangers of World War II.

• The terrorists are a very new kind of enemy. They have no flag, no president, no borders, and no nation.
• This new threat requires us to proceed with transformation in a robust way. It is by no means clear that the assets we inherited from the Cold War provide us with the correct algorithm of capability necessary to deal with our new enemy.

I would like to reinforce some of the themes that were raised earlier today at the conference. In particular, we need enhanced public/private partnerships that combine the best features of private sector experts and public sector rule makers.

• The value of such partnerships became apparent to me when the American Waterway Operators and the U.S. Coast Guard got together and developed the Responsible Carrier Program, which is far superior to anything the public or private sector could have developed on its own.
• The Coast Guard also has developed an effective partnership with the cruise ship industry regarding the control of illegal spills.

• Boeing, Lockheed-Martin, and other companies provided essential cooperation when we established the Transportation Security Administration (TSA).

Our security is built on three key elements that must be kept in constant balance:

• Our physical safety.

• The free flow of economic activity that underpins our quality of life.

• The civil liberties guaranteed to Americans in the Constitution.

We are working within DHS to develop a culture whose core values include both a sense of commitment and a sense of urgency. These values will enable us to overcome obstacles and complacency.

• DHS employees need a common vision that they can understand and articulate.

• We can strategically build goals and activities upon these values, with accountability and a metric-based compliance process at the tail-end of the strategic planning process.

The new department represents by far the most complex reorganization at the federal level since the 1947 National Security Act.

• The new DHS merged twenty-two disparate agencies with some 180,000 employees. They had twenty-two different human resource systems, thirteen different procurement systems, and thirty-seven different systems for administering government credit cards.

• This transformation occurred at the same time that we had to confront the challenges of defending the homeland on a daily basis.
Unlike in 1947, however, Congress has yet to restructure its oversight functions to correspond better to the new structure of the executive branch, despite the 9/11 Commission’s explicit recommendation that they do so. DHS still has to deal with eighty-seven committees or subcommittees as part of that oversight process. DHS already has many achievements. One of the most important has been the development of a system-of-systems for aviation security, which has put into place a very effective multi-layered defense.

- We now have a corps of newly trained and adequately paid airport screeners.
- We have thousands of air marshals ensuring the safety of our skies.
- We also have thousands of federal flight deck officers; these pilots have voluntarily undertaken the difficult training regimen that enables them to carry a weapon into the cockpit.
- That cockpit is now equipped with newly hardened doors.

Another achievement has been the establishment of a single face at the border. Americans returning from abroad no longer must pass through three separate checkpoints for customs, immigration, and agriculture. The U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program also has permitted us to develop an effective entry/exit system for the first time in our country’s history.

The federal government has both increased and better targeted its assistance to local first responders.

- Whereas much aid before 9/11 came with few conditions, federal assistance now consciously seeks to promote interoperability, information sharing, and better command and control systems.
- The new Homeland Security Information Network links state and local authorities directly with their federal counterparts as well as each other. It includes all fifty governors, all fifty state Homeland Security Advisors, and those responsible for the safety of the fifty largest urban areas in the United States.
DHS has overcome the old paradigm of prevention, response, and consequence management. We have been pushing for enhanced domain awareness as a mechanism to enhance all three missions. The Secretary of Homeland Security has identified the following priority areas for further improvement:

- Information sharing;
- Critical infrastructure protection;
- Interoperability, not only of communication but also of equipment and training;
- Integrating the ports and borders of all of North America;
- Investment in next-generation capabilities, including for detecting explosives;
- Local community preparedness;
- Reducing the immigration backlog;
- Developing 21st-century personnel, procurement, and information systems that incorporate best practices from both the private and public sectors.

As President Jefferson observed, the American character assumes that we can “surmount every difficulty by resolution and contrivance.”

- Resolution entails a sense of commitment and urgency.
- Contrivance involves creativity and innovation in the resolution of problems.
- Both these qualities will enable us to overcome the terrorist challenge and secure our homeland.
Day Two
Session Five

Anticipating and Defending against Bioterrorism

MODERATOR

Dr. Charles M. Perry, Vice President and Director of Studies, Institute for Foreign Policy Analysis

SPEAKERS

Brigadier General Lloyd E. Dodd, USAF, Command Surgeon, U.S. Northern Command

Dr. Charles Gallaway, Director, Chemical Biological Defense Directorate, Defense Threat Reduction Agency

Dr. James M. Hughes, M.D., Director, National Center for Infectious Diseases, Centers for Disease Control and Prevention

Patrick Libbey, Executive Director, National Association of County and City Health Officials

Dr. Ivan C.A. Walks, Senior Medical Advisor, E Team, CEO, Ivan Walks and Associates, and former Chief Health Officer for the District of Columbia
Dr. Charles M. Perry
There is probably not a more challenging threat that we and our allies must prepare to face than bioterrorism. Several characteristics of the bioterrorist threat make it uniquely disturbing:

- A bioterrorist attack will almost certainly be well underway before we even know what is happening and what biological agents it involves.
- The combined effect of the mobility of our society and the transferability of disease mean that the effects of a biological attack could spread rapidly over a wide area, with the probability of tens, if not hundreds, of thousands of casualties.
- What might begin as a local or state level contingency could rapidly escalate to the national or federal level.
- This escalatory dynamic means that federal military forces, as well as National Guard and Reserve units, could be called on to provide assistance much more rapidly than expected, calling into question their availability for war fighting missions elsewhere.
- These characteristics of a bioterror attack present difficult coordination problems among local authorities; the local, state, and federal levels; and between civil and military authorities. We need careful advanced planning and, if possible, prior agreement on pre-designated responsibilities and assignments across all these levels before we must respond to an actual incident.

Dr. Ivan C.A. Walks
During a public health crisis, people want “continuity.”

- They want to know if they can keep their kids in school, or how long before they can return them there.
- We tend to forget that we work in communities. Public health issues very early become community issues. We must address community challenges and not overlook community opportunities.
• We need to think more about peoples’ mental health needs and our mental health infrastructure. These are essential for allowing our communities to function after a crisis.
• Terrorist attacks, natural disasters, and other “psychosocial” events typically produce medically unexplained physical symptoms and long-term mass psychological consequences.

Risk communication is an interactive process involving the exchange of information and opinion among individuals, groups, and institutions about the nature of risk in an unstable information environment.
• The priority should be to assess this environment, which likely will be characterized by crisis, heightened public emotions, limited access to facts, rumor, gossip, assumptions, and speculation.
• The public needs accurate and timely information they can trust. Even when you do not have all the relevant information, you still have to be able to communicate in a way that maintains your credibility. You should never say things that you know are not true.
• Communication will involve numerous “relevant” publics that are:
  o culturally, ethnically, and linguistically diverse
  o physically and psychologically diverse
  o physiologically diverse
  o financially, socially, and “historically” diverse; and
  o diverse in their knowledge of public health issues
• It is essential to coordinate information dissemination throughout the relevant region – which could be a city, state, or half the United States, depending on the geographic extent of the crisis.
• We need secure systems for information and knowledge management. Establishing a centralized data repository for the most up-to-date information from multiple sources is also essential.
• A picture is worth a thousand lives. A map indicating safe and unsafe areas often is the easiest way to help people under-
stand why they have to go in one direction or the other. We should design systems so that people can easily use them.

- Tell people what to do as well as what not to do. Give them a positive message.

We need cross-jurisdictional system design, operation, and especially procurement.

- What cannot be measured cannot be valued.
- Public sector funding, which is typically allocated for a specific purpose, can create additional stovepipes.

We do not learn enough from typical, non-terrorist public health crises such as those caused by the West Nile Virus and the Flu.

- One important lesson is the need to avoid giving the impression that some people are undeservedly being better protected than others. The past histories of some communities make them especially attuned to such discrepancies.

Flexible implementation of plans is essential.

- If adversaries know your plans, you may need to implement them differently.
- Someone may schedule a rock concert at the same location where you had previously chosen to distribute medications.
- “Fail to Plan, Plan to Fail”
- Relationships matter.
- When things speed up, slow down. It is much harder to correct a mistaken statement or action than to prevent it in the first place.

Brigadier General Lloyd E. Dodd
This presentation discusses how the U.S. Department of Defense supports the efforts of civil authorities to manage the consequences of a disaster within the United States. NORTHCOM has two missions. First, its homeland defense mission requires it to deter, prevent, and defeat threats to U.S. territory. Second, it provides military assistance to civil authorities, including consequence management, as directed by the President or the Secretary of Defense.

- NORTHCOM’s creation in October 2002 created a unique situation. This was the first time that a military command had
been given explicit responsibility under the Unified Command Plan to support U.S. civil authorities.

- Its area of responsibility encompasses all of North America. Although PACOM owns the U.S. military forces deployed in Alaska, NORTHCOM has operational control over these assets.
- From a medical perspective, NORTHCOM's homeland defense mission could include protecting the health of American military forces and the critical health infrastructure located within the United States from enemy attack. These tasks are essential for mission assurance.

NORTHCOM's first commander, General Eberhart, laid out NORTHCOM's core tasks in May 2004:

- Remember that you are at war every day.
- Continually improve the system.
- Get ahead of the play (i.e., the threat).

Establishing good relationships between military and civilian leaders is an essential requirement for providing effective military support to civilian authorities.

- NORTHCOM has relatively few assigned forces. The way we get things done is by working with people who have access to the extensive medical and other capabilities located within our area of responsibility.
- I spend approximately seventy percent of my time cultivating such relationships. We try to develop relationships that will allow us to identify and access relevant capabilities before an event.
- When something does happen, we will coordinate the medical response within DOD, and the interface between DOD and the civilian authorities within other U.S. government agencies and their state and local counterparts.
- The same rules, philosophies, and missions apply in both peacetime and wartime situations. We support civil authorities coping with both natural disasters and terrorist incidents.

The Department of Defense's concept of supporting civil authorities is complex.
• NORTHCOM’s policy guidance comes from the Pentagon. In theory, this guidance emanates from the Office of the Secretary of Defense for Homeland Defense, headed by Assistant Secretary of Defense Paul McHale. In practice, it also comes from other policy offices within the Office of the Secretary of Defense, including Health Affairs, Reserve Affairs, and the office covering Special Operations and Low-Intensity Conflict.

• While policy is determined in the Pentagon, NORTHCOM is responsible for policy execution. We develop the doctrine and the concept of operations that determine how we implement what the Pentagon has told us to do.

• We undertake broad planning at headquarters. We then elaborate plans at the tactical level with our action components – JTF-CS, JTF National Capital Region, U.S. Army Forces Command, and other entities.

The Department of Defense has developed a wonderful system for supporting a war overseas. The processes for supporting civil authorities within the United States are still under development.

• We need to create processes that enhance our flexibility. Capability packages must be tailored to the specific emergency. Every situation is different.

• DOD can provide many types of assistance to civil authorities within the United States. Possible capabilities include subject matter experts: physicians, nurses, and medical technicians; laboratories and lab technicians; respiratory and other facilities and equipment; blood supply and pharmaceuticals; public health and vaccination teams; transportation assets; and manpower.

• Nevertheless, we are not allowed to buy new capabilities only for the purposes of civil support. We must dual and triple task existing resources within the Department of Defense to support our homeland defense and homeland security efforts. Some assets might be unavailable because they will be committed overseas when a domestic incident occurs.
• It will take an additional two or three years of solid work before DOD processes can ensure the rapid and effective availability of U.S military assets for any domestic consequence management operation.

Civilian authorities always will play the lead role in any domestic consequence management operation.
• Most incidents in this country will remain local.
• If the local authorities are overwhelmed, the states, perhaps operating on a region-wide basis, will get involved.
• If the scale of the problem is so great that the federal government must get involved, the President will identify a primary federal agency, not normally DOD, to lead the response.
• Only if the primary federal agency requests DOD's assistance, and the President and Secretary of Defense approve, does NORTHCOM get involved.
• DOD assets typically would be provided within four-to-six days following the onset of an incident. Some things can be done quicker. For many years, local military bases have had the ability to support their surrounding communities within two-to-three days following a request from the local authorities.
• Since these existing “immediate response authorities” may prove insufficient when local assets are too few or the crisis is too urgent, the Department of Defense is examining novel methods to provide greater emergency assistance faster. For example, we are evaluating whether to prepare in advance a standing execute order for the provision of military support to civil authorities in the National Capital Region.
• The National Guard, acting under Title 32 or perhaps even Title 10 status, would most likely provide the first military assets for any domestic consequence management operation.

Public fears and misperceptions impede DOD’s ability to provide support within the United States.
• Many civilians distrust the military and the rest of the federal government. We must overcome a history of misunderstandings.
• A related problem is the lack of common culture, language, and systems between military and civilian medical responders.

• Military and civilian medical personnel need to better appreciate the competence of the other. Once they begin working together, they invariably appreciate that both practice high-quality medicine.

• We need to deepen public/private and government/academic interactions in the area of public health consequence management.

Dr. James M. Hughes
Recent reports have highlighted weaknesses in the ability of the U.S. public health infrastructure to cope with infectious diseases.

• These reports also identified many factors that contribute to infectious disease emergence and reemergence. These include human demographics and behavior; technology and industry; economic development and changes in land use patterns; international travel and commerce; microbial adaptation and change, which is what make infectious diseases unique and particularly challenging; the breakdown of public health measures; human susceptibility to infection; changes in climate and the weather; changes in ecosystems; poverty and social inequality; war and famine; lack of political will; and the deliberate attempt to harm.

• The surprising discovery of the West Nile Virus in the Western Hemisphere in August 1999 reminded us that we do indeed live in a global village from the standpoint of infectious diseases.

• The 2001 anthrax attacks illustrate that we are likely to recognize a terrorist attack only when a patient shows up ill at a local medical facility. The attacks could have been much worse if they had involved multiple agents, multiple drug resistance, genetic engineering, transmission to animals, multiple modes of transmission, clinical surge capacity, multiple time zones, cases in other countries, or concurrent cyberterrorist attacks. Other agents might have been more difficult
to isolate or identify or involved person-to-person or vector borne transmission.

These incidents have resulted in the emergence of a new public health perspective about infectious diseases.

- We now better recognize that local infectious disease outbreaks can soon impact our national security and the global economy.
- We also appreciate the necessity for rapid and collaborative responses to such outbreaks.

The Centers for Disease Control and Prevention’s (CDC) Bioterrorism Program began in 1999.

- The program encompasses many CDC centers and programs. It employs the concept of “dual” or “full” use.
- The program’s focus areas include preparedness planning, epidemiology and surveillance; strengthening biological and chemical laboratories; improving communications; enhancing education and training; and developing the Strategic National Stockpile.

The biological agents of greatest concern, the so-called Category A agents, and the diseases they cause are often of animal origin. We need to strengthen collaboration with veterinarians to best confront animal diseases that can be transmitted to humans. The United States is conducting a number of bioterrorism preparedness initiatives. Three of the most important are BioShield, BioWatch, and BioSense.

- BioShield aims to accelerate the development of medical countermeasures, including vaccines, therapeutics, and diagnostics.
- BioWatch is deploying environmental air samplers in key locations to detect the release of biological agents.
- BioSense is a public health surveillance system that enhances the detection of bioterrorist attacks through improvements in our ability to access and analyze diagnostic and pre-diagnostic health data.

We are enhancing the capabilities of both components of the Strategic National Stockpile Program.
The first component consists of twelve push packages that can arrive anywhere in the United States within twelve hours. These packages can fill a 747 airliner. One of these packages was sent to New York City on September 11, 2001.

The other component, the Vendor Managed Inventory, takes longer to arrive (within twenty-four to thirty-six hours of activation), but its contents (treatments, vaccines, and diagnostic supplies) can be tailored to the exigencies of a particular emergency.

We are also enhancing the support provided by our Laboratory Response Network (LRN), which has at least one facility in each state.

- The LRN involves agent-specific protocols, standardized reagents, a lab referral directory, a secure communications system, the training of personnel, proficiency testing, and the provision of appropriate immunizations to laboratory staff participating in this network.
- The LRN played an important role in dealing with the outbreaks of anthrax, SARS, and monkey pox.
- The LRN laboratories also participate in the BioWatch program.
- The CDC also is funding the development of eight different National Institute of Allergy and Infectious Diseases Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases. This initiative is creating a unique consortium of academic institutions involved in these areas.

A Committee of the National Research Council, chaired by Dr. Gerald Fink, issued a report in early 2004 that provided examples of the types of experiments that researchers should avoid because of their potential contribution to bioterrorism. These included demonstrating how to render a vaccine ineffective; conferring antibiotic resistance to therapeutically useful agents; enhancing the virulence or capability of an organism to cause disease, or, even worse, rendering a nonpathogen virulent; experiments that might increase transmissibility or alter a host’s range; those that would enable
invasion of diagnostic or detection modalities; and facilitating the 
weaponization of an agent or toxin.

We already have learned several lessons regarding how to manage 
better the threats from infectious diseases and bioterrorism:

• We need to understand better the potential contribution of 
environmental microbiology for analyzing bioterrorist agents. 
In particular, environmental microbiology can help us detect 
and quantify bioterrorist agents, determine their survival 
times, and best disinfect them in various environments.
• We need to strengthen partnerships between clinicians and 
public health agencies at the local level.
• We need to engage veterinarians more. Dr. Lonnie King, 
Dean of the College of Veterinary Medicine at Michigan 
State University, correctly observed, “We have a new world 
in terms of the epidemiological convergence of animal health 
and human health.”
• We need to enhance our relationships with foreign and inter-
national agencies. The SARS Laboratory Network established 
by the World Health Organization played a critical role in 
identifying and controlling the cause of SARS.
• We need proactive communication. Our response to the 2001 
anthrax attacks was characterized by severe communication 
problems. Former New York City Mayor Rudolph Giuliani 
provides the model of a highly skilled risk communicator.
• We need vigilance. Alert clinicians, alert laboratories, alert 
veterinarians, and alert research scientists are essential for 
recognizing and responding to these threats.

Mr. Patrick Libbey
The United States has almost 2,800 local public health agencies.

• They range in size and setting from the Los Angeles County 
Health Department, which serves a population of ten million 
persons, to the health departments found in small townships 
in the Northeast, some of which serve fewer than 1,000 res-
idents.
• Besides size and setting, local public health agencies also differ in their preparedness needs. Different communities face different threats.
• All emergencies are local – at least at first. First responders will depend initially on whatever resources already exist in the affected community. We need to maximize those assets.

From the perspective of public health, three stages characterize any biological event:
• Determining that an event has occurred.
• Responding to it.
• Engaging in long-term consequence management after the event.

Challenges confront us at each of these stages.
• It could take some time to determine that a biological event has occurred. Without a “smoking gun,” we must rely on syndrome surveillance, communication with clinicians, and environmental monitoring.
• These detection systems are tools towards a larger end, not an end in themselves. Although our ability to detect biohazards has improved in recent years, we may be falsely assuming that we have a corresponding capacity to respond.
• Local health authorities are working with the Departments of Justice, DHS, and the CDC to develop the new field of forensic epidemiology, which bring together representatives from the law enforcement, justice, and public health communities.
• Responding effectively requires planning, relationships, and appropriate risk communication at the community level. Messages to different communities must not be inconsistent. Exploiting established contacts with communities is essential. We must overcome gaps in our information management technology.
• A major legal challenge is that this country’s isolation and quarantine laws have developed over time on a case-by-case basis.
• Consequence management can entail a lengthy process of coping with the long-term effects of a public health emergency. The World Trade Center site still poses environmental
threats. After any incident, we must monitor both the environment and those who received treatment.

Biological events are different.
• They are not specific in terms of time or place.
• Successful containment will require rapidly detecting an event and responding effectively to it. The local public health agencies play a key role in detecting an event early, stopping its spread, and providing a foundation upon which to build external assistance.
• We need to do a better job at establishing a baseline for our public health assets at the federal, state, and local levels.
• Fortunately, the better we prepare for intentionally untoward events, the better we can respond to natural disasters as well.

Dr. Charles Gallaway

The range of serious biological threats is increasing.
• We no longer face a known list of biological threats against which we can concentrate our defense efforts. Novel threat agents are constantly emerging.
• Given the unlimited number of possible pathogens, the advantage at present lies with the perpetrator.

The scientific challenge today is to develop capabilities that can work against unknown pathogens.
• We need real-time bioagent detectors to provide actionable information. We are approaching the limits of wet chemistry, so we need to look more at using biomass or terahertz spectroscopy. Micro arrays, which might entail placing some kind of bodily fluid on a microchip, could enhance our capabilities for timely medical surveillance.
• We also need better medical countermeasures for us to respond more effectively after an attack. We cannot develop a vaccine against every possible threatening biological agent. Instead, we should develop means to enhance our innate immunity, perhaps by blocking the pathways through which pathogens can enter our bodies. We also need to treat people more effec-
tively after the fact. Developing these new countermeasures will require a lot of time and money.

The policy community needs to improve how we approve new medicines.

- The decision by the Food and Drug Administration to adopt a two-animal rule for licensing new medical products for human use has helped a lot.
- We need to imagine other novel regulatory approaches that can avoid the very lengthy and very expensive animal testing processes altogether.
- For example, improvements in computational power might allow us to conduct some virtual trials with computer simulations of the human body.

We also must better integrate our civilian and military efforts in this area.

- We need a directive instructing us to use a common set of assays. Otherwise, we risk confusion during a crisis, when civilian and military researchers might hesitate to accept the other side’s findings at face value.
- The Department of Defense and the civilian response community also use completely different means to develop situational awareness. We need a common operational picture.

The technical community is making progress in helping policy makers cope with the challenges of post-incident consequence management.

- We are researching the effects of time, weather, and other environmental factors on biological agents.
- We also are gaining a better understanding of their toxicity and the limits to our ability to detect them.
- The extraordinary high costs of environmental cleanup mean that policy makers will need to adopt less than absolute standards regarding the amount of permissible level of residual biological agent for large geographic areas.
MODERATOR

Ambassador Stephen W. Bosworth, Dean, The Fletcher School, Tufts University

SPEAKERS

Dr. David M. Abshire, President, Center for the Study of the Presidency, and former United States Ambassador to NATO

Ambassador John R. Dinger, Deputy Coordinator for Counter Terrorism, Department of State

Oscar Rocha, President, The Joaquin Amaro Foundation for Strategic Studies, Mexico City, Mexico

E.C. Whiteside, Head, Weapons of Mass Destruction Center, NATO

SUMMARY

Dr. David M. Abshire
Leadership and strategic thinking are important for developing a homeland security strategy. Enlisting the nation’s scientific establishment in the war on terror is vital for success.
• During World War II, President Roosevelt and Vannevar Bush organized the science and research communities for the war effort, and their contribution was vital to ensuring success.

• At the Center for the Study of the Presidency, we have worked with Secretary Ridge and representatives from the scientific establishment to develop strategies for marshalling the nation’s scientific and technological capabilities to further our homeland security efforts.

We also need to utilize our European alliances by including them within our strategy.

• Leadership is power, especially the power to communicate. We should utilize NATO and especially the North Atlantic Council meetings, since they offer an opportunity to communicate with twenty-five members, forty-six if Partnership for Peace members are included.

• The alliance can be effective. Working with our European partners in the mid-1980s, we were able to convince Libyan leader Muammar Qaddafi to cease supporting terrorism within Europe. It is also flexible. In the 1980s, through informal meetings, we were able to change several countries’ policies on missile deployments and modernization.

• Today there is insufficient collaboration between the EU, NATO and our missions, and all parties are culpable.

• The European scientific establishment can also make vital contributions to fighting international terrorism, and we should work to ensure their involvement. A reinvigorated North Atlantic Council could also help funnel defense investment to support the GWOT and away from heritage Cold War investments.

Public diplomacy should figure more prominently in our strategy.

• Changing perceptions represent core power. Lieutenant General David Petraeus, who is leading U.S. efforts to train Iraqi security forces, observed that we will lose if we do not change minds.
• We should devote more resources and attention to understanding how we can utilize global communications to build goodwill towards America.

• Congress is far ahead of the White House in emphasizing public diplomacy. I served on the Advisory Group on Public Diplomacy for the Arab and Muslim World, which was established by the State Department at the request of the House Appropriations Committee in June 2003, and in our report we reviewed the state of America’s standing in the world and proposed how to fix its failing public diplomacy.13 I have spoken with National Security Advisor Condoleezza Rice and her deputy Steven Hadley,14 and I believe the White House will devote more attention to public diplomacy after the elections.

Ambassador John R. Dinger

The U.S. government’s counter-terrorism strategy encompasses all regions.

• The Middle East obviously factors extensively in our counter-terrorism efforts. Within the region the State Department is actively involved in counter-terrorism assignments outside of Iraq and Afghanistan.

• In East Asia, there were the horrific bombings in Bali in October 2002 and Jakarta in August 2003, and in the Philippines three Americans were kidnapped in May 2001.

• In Africa, we had the embassy attacks in Nairobi and Dar es Salaam in August 1998, and the bombing of the Paradise Hotel in Mombassa, Kenya in November 2002.

• Europe witnessed the horrific train bombing in Madrid in March 2004. In South America, the Revolutionary Armed Forces of Colombia continues to hold three hostages, and in November 2003 launched a grenade attack on a Bogotá restaurant.


14 Dr. Rice has since become Secretary of State, and Mr. Hadley has replaced her as the National Security Advisor.
The success or failure of our global campaign against terrorism hinges on other nations being willing and able to fight terrorism. This fundamental principle underpins all of our counterterrorism efforts.

- Outside of Afghanistan and Iraq, local forces, with American support, have contributed significantly to the capture and killing of al-Qaeda’s leadership and lower-level operatives, including Khalid Sheikh Mohammed in Pakistan and Hambali, the head of Jemaah Islamiyah, in Thailand.

- While the United States will use all elements of its power to fight terrorists, including direct and unilateral military strikes, the key effort must focus on building the capability of foreign governments to fight terrorism on their soil and in their own interests.

- We must also eliminate foreign support for terrorism while also building goodwill towards America. Local governments must encourage their populations to reject terrorism, while America must employ its public and private resources to lift our international standing in public opinion. Government programs such as the Millennium Challenge Account are important, as are private efforts by prominent and popular Americans.

There are a number of tools that we are employing to build local capacity in fighting terrorism.

- The State Department is providing counter-terrorism training to local law enforcement.

- We are providing an advanced name-check capability to help countries better control and monitor movement across their borders.

- We have sent financial assessment teams to advise and assist other nations in blocking terrorist financial transactions.

- Often, however, the best way of boosting local capacity is through on-the-job training in pursuing terrorists.

**Mr. Oscar Rocha**

For a number of reasons, Mexico lacks an energetic homeland security strategy focused on countering international terrorism.
• We do not feel threatened, although Mexico may be targeted by international terrorists. Yet we cannot allow the luxury of waiting for a terrorist attack before developing a homeland security policy. Thus, homeland security represents a policy challenge between the Mexican national security establishment and the broader public and political system.

• Mexican President Vicente Fox’s timid response to 9/11 represented a policy failure, because he failed to articulate the importance of counter-terrorism cooperation to the Mexican people.

• The Iraq war was not seen as part of the GWOT, given the shifting rationales for it and the failure to find WMD. Mexico was a member of the Security Council prior to the war, and the overriding issue for Mexico was whether we should cooperate with the United States on Iraq, not whether we should enhance bilateral counter-terrorism cooperation.

Yet Mexico is threatened by international terrorism.

• As it becomes harder to operate in the United States, al-Qaeda may find it easier to operate and conduct attacks in adjacent territories. For example, many Americans vacation in Mexico, and they could be targeted in an attack.

• An attack could disrupt bilateral trade as well as negatively impact the symbiotic economic relationships existing between towns on opposite sides of the border. Also, many Mexicans reside legally and illegally in the United States, and they could find themselves unwelcome if an attack occurred. Terrorism could therefore disrupt both political and economic relationships.

• Currently, counter-terrorism cooperation is fragile. It exists inside government agencies, but there has been very little effort to articulate the reasons for it to the Mexican public.

We need to think in terms of a North American perimeter, given the movement of goods and people across America’s borders with Mexico and Canada. But there are three obstacles to better U.S.-Mexican cooperation on counter-terrorism, and they involve bias, sovereignty and drugs.
• Bias originates from divergent threat perceptions and how organizations deal with the latter. For instance, from the Mexican point of view, the next al-Qaeda attack will probably resemble the Madrid or Oklahoma City attack rather than 9/11. Yet U.S. efforts to make airline travel safer do not match our own threat perceptions and priorities for cooperation, and Mexico needs to be careful how it allocates money given its limited resources.

• Sovereignty is the cornerstone of Mexican identity, and Mexicans need to feel in control of their destiny. Given the history of “asymmetrical cooperation,” there remains a lack of trust of U.S. intentions when it proposes a policy that affects the bilateral relationship. In past cooperative efforts, for instance in counter-narcotics, Mexico felt like a junior member of the partnership.

• There remains lingering bitterness over past counter-narcotics cooperation. Many American counter-drug policies essentially failed, succeeding only in turning Mexican territory into a battleground. And Mexico is still bitter over its unhappy experience with the drug certification process.¹⁵

• There is a Mexican homeland security strategy, but it is focused upon making law enforcement more efficient and impeding the flow of drug money, which fuels corruption.

To establish effective bilateral security cooperation, Mexican security interests must be incorporated into the discussions and adopted policies.

• The agenda must be jointly developed, and doing so would garner Mexico’s proactive cooperation.

• Counter-terrorism cooperation must also be considered as one aspect of the bilateral agenda. We need to move forward on the broader relationship as well.

¹⁵ Under sections 489 and 490 of the Foreign Assistance Act of 1961, the President must submit to Congress by November 1 a list of “major illicit drug producing countries” and “major drug transit countries,” also know as the “Majors List”. In September 2004, Mexico was included in the “Majors List” for fiscal year 2005.
• Bilateral counter-terrorism efforts must also have the political backing of the Mexican public to ensure a higher level of commitment from Mexican politicians. The Mexican political class must build popular support for cooperative efforts.
• Building trust would ensure a more robust level of security cooperation. Confidence-building measures, such as bilateral cooperation on WMD detection and consequence mitigation within Mexico, would build trust because Mexican authorities lack these capabilities. Some form of Mexican participation in NORAD would also help to solidify trust. A true sign of friendship and trust would be the granting of export licenses for the sale to Mexico of highly desired defense items.

Mr. E.C. Whiteside

Transatlantic cooperation is essential for defending our common values and overcoming our common threats and challenges. NATO strongly condemns terrorism, and its members will fight it together as long as necessary.
• Defense against terrorism may involve the use of military forces by the North Atlantic Council to deter, disrupt, defend and protect against actual or threatened terrorist attacks, including actions against terrorists themselves and those who harbor them.
• A recent NATO study indicates the growth in terrorism over the last thirty years. Recently, two NATO countries, Turkey and Spain, have been attacked by terrorists.
• The risks of terrorists acquiring WMD are real, and NATO has an important role in supporting the global dimension of combating threats to homeland security.

The Alliance is engaged in a number of initiatives in the fight against terrorism
• Operation Active Endeavor was launched in autumn 2001 with the clear objective of interdicting terrorist movement in the Mediterranean. Efforts are underway to secure contributions from countries that participate in NATO’s Mediterranean Dialogue.
• NATO has improved intelligence sharing through the new Terrorist Threat Intelligence Unit, and it has provided assistance, such as the NATO Airborne Early Warning and Control Aircraft, in protecting selected major events.

• At the 2004 Istanbul Summit, NATO Heads of State and Government agreed to assist Iraq with the training of its security forces. Rather than combat aims, the mission is focused on providing training, equipment and technical assistance.

• In Afghanistan, NATO took control of ISAF in August 2003, and there are now approximately 7,000 soldiers, sailors and airman from thirty-five NATO and non-NATO nations supporting the mission. Provincial reconstruction teams have been set up in a number of cities, and ISAF efforts were vital in ensuring the success of the recent Afghan elections.

NATO has undertaken a number of measures, such as the establishment of five CBRN defense initiatives in 2002, to counter the threat posed by WMD proliferation.

• The deployable NBC analytic laboratory can investigate and collect samples of possible NBC contamination. It is ready to go anywhere, anytime. The NBC Joint Assessment Team assesses the impact of an NBC event and advises NATO Commanders on the means of mitigating its effects.

• The NATO Chem-Bio Defense Stockpile has identified national stockpiles that can be shared in a crisis and rapidly moved into theater. The Disease Surveillance System collects information on unusual disease outbreaks, and it will alert NATO commanders of a biological outbreak. Through it we are also developing interoperability standards for disease surveillance.

• The Virtual Center for Excellence for NBC Weapons Defense has expanded and strengthened NBC defense training, and it provides NBC education to senior-level officials. Each of these five capabilities has been brought together in a multinational CBRN defense battalion.

• The alliance has also decided to acquire theater missile defenses to protect NATO-deployed troops, and we are working
closely with Russia, which has excellent missile defense technology, to examine opportunities for interoperability.
SUMMARY

Our conference panels are examining in detail the important homeland security challenges facing the United States – including critical infrastructure protection, bioterrorism, maritime, aviation, and border security, and emerging technologies – so I will focus on the broader strategic context and the President’s path to victory in the GWOT. The United States has three important strategic objectives in the GWOT: Defeating terrorists and their networks, both at home and abroad; working with partners to isolate terrorists and outlaw regimes while promoting democracy; and transforming the federal government to fight terrorism more effectively for the long haul. President Bush has laid out a clear path to ultimate victory in the GWOT:

- Defend the peace by taking the fight to the enemy throughout the world;
- Protect the peace by working with our allies to confront terrorism while securing the American homeland;
- Extend the peace by supporting the rise of democracy as an alternative to hatred and terror.
The administration’s policy differs from previous U.S. approaches towards the terrorist threat. The terrorists no longer attack us with relative impunity, as they did with the 1993 World Trade Center bombing, the 1996 attack on the Khobar Towers, the 1998 bombings of our embassies in Kenya and Tanzania, and the 2000 attack on the USS Cole.

- We now effectively marshal all instruments of U.S. national power – military, diplomatic, intelligence, economic, and law enforcement.
- We are on the offensive abroad in a campaign of direct and continuous action aimed at disrupting, degrading, and ultimately defeating the terrorists and their networks.
- We are preempting acts of terror before they emerge, and defeating the enemy overseas so that we do not face them at our shores.

We and our foreign allies have achieved numerous successes in the GWOT on a number of fronts. We have killed or taken into custody three-quarters of the senior al-Qaeda leaders, operational managers, and key facilitators that we have been tracking since 9/11. These measures have weakened their leadership and diminished their capability. We have reduced terrorists’ funds by freezing their assets, denying them access to the international financial system, protecting legitimate charities from terrorists’ abuse, and preventing the movement of monies through alternative financial networks. We continue to contract the space in which terrorists can operate and transit freely.

- Afghanistan and Iraq no longer provide a haven or other assistance to terrorists. Instead, the newly liberated fifty million people of Afghanistan and Iraq are fighting alongside Coalition forces against their former terrorist oppressors. The citizens of these two countries, including their women, now
enjoy basic civil rights such as education, healthcare, and the opportunity to participate in democratic elections.

- The governments of Pakistan and Saudi Arabia also have become important partners in the GWOT during the last few years. Pakistan’s security, military intelligence, and law enforcement forces have cooperated with the United States to disrupt terrorism both within and outside their borders. Today, the leadership and people of Saudi Arabia realize that al-Qaeda is as much their enemy as ours. The Saudi government has aggressively attacked al-Qaeda’s network in the Kingdom and have captured or killed over 600 individuals involved in its financial, logistics, and planning infrastructure.

- Libya and the A.Q. Khan network no longer present a WMD proliferation threat. Three years ago, Libya, a long-time supporter of terror, was spending millions of dollars to acquire chemical and nuclear weapons. Today, Libya has abandoned these programs. The A.Q. Khan network, which was selling nuclear plans and equipment to Libya and other problem countries, also ceased operation.

We are taking unprecedented measures to protect the American people at home. The enemy exploits our open society, hides among us, and tries to attack us from within. We have judiciously used the new tools provided by the Patriot Act to break up terrorist cells in Oregon, Northern Virginia, New York, and elsewhere. We have seized millions of dollars here at home that could have helped fund terrorist activities. We have taken other steps to disrupt potential terrorist activities in the United States.

We must sustain our vigilance even as the events of 9/11 grow more distant and we achieve additional successes in disrupting terrorist plots.

- The terrorist threat will continue to evolve.
- The terrorists will seek to combine operational and technological innovation in order to surprise us.
The evil terrorist enemy mercilessly encourages the killing of innocents. We have witnessed their cowardly acts in Bali, Istanbul, Riyadh, Madrid, Egypt, Baghdad, and Beslan.

The enemy only has to get it right once; we must get it right every day.

Our ultimate objective is to create an international environment that is inhospitable to the terrorists and their supporters. We will triumph only when the conditions that promote hatred, despair, and destructive visions, conditions that terrorists seek to exploit, are supplanted by the hopes and aspirations of freedom.

Our efforts to promote freedom and hope have shown the most successes in Afghanistan and Iraq. These countries are in the process of building stable democracies.

Indonesia is another country under terrorist assault whose people have achieved increased freedom recently. The world’s fourth-largest country and the nation with the largest Muslim population, Indonesia recently held democratic elections that resulted in a peaceful transition of power.

We need foreign allies and partners to succeed in this endeavor. Sixty-four countries are assisting CENTCOM at its Tampa headquarters. All NATO members have allies in Afghanistan, Iraq, or both.

The federal government is undergoing a sweeping transformation to enhance its ability to defeat terrorism and support democracy. We are creating an enduring institutional platform that will allow us to fight terrorism on a protracted basis. These changes include a new government architecture and greater long-term investment in anti-terror programs.

The new Department of Homeland Security will lead a unified national effort to defend against terrorist attacks in the United States. Its funding has nearly tripled since 2001. Federal support for state and local government programs to counter terrorism has increased significantly since 9/11.

The new Homeland Security Council is coordinating policy across the multiple departments and agencies involved in the homeland security mission. The new U.S. Northern Com-
emand provides an integrated approach towards homeland defense and coordinates DOD support to federal, state, and local civilian authorities.

- We now have a multilayered approach to aviation security that goes from curb to cockpit.
- We have increased border security by adding 1,000 agents along the southwest border and by deploying US-VISIT, a biometric exit-and-entry system, around the country.
- The new Terrorist Screening Center is consolidating our terror watch lists and ensuring that investigators, screeners, and agents at the federal, state and local level all have access to the same information.
- We have increased port and cargo security by funding thirteen Coast Guard maritime safety and security teams, by implementing the Maritime Transportation Security Act, and by using the DHS National Targeting Center to screen data on all cargo entering the United States before it arrives. The Container Security Initiative is placing a growing number of Customs employees at major international ports to screen inbound containers to the United States.
- The $5.6 billion made available to Project BioShield will provide new tools to improve medical countermeasures to protect our citizens against a chemical, biological, radiological, or nuclear attack.

Finally, the President is leading the way on intelligence reform. He has already initiated several significant changes to improve collection and analysis, bridge the foreign and domestic intelligence divide, and enhance the sharing of information.

- The President recently signed Executive Orders that give the Director of Central Intelligence many of the enhanced managerial powers over the intelligence community that will eventually fall to the proposed National Intelligence Director.
- The establishment of a National Intelligence Director and a National Counterterrorism Center will better position us to fight the GWOT over the long term. This restructuring will allow us to apply more quickly and flexibly U.S. intel-
ligence capabilities against our terrorist enemies and other threats.

- We need to encourage innovation outside the government to mobilize additional resources for the GWOT. In particular, we need to foster intellectual and human capital on terrorism and counterterrorism issues. Promoting area studies and linguistic programs, similar to those developed to study the Soviet Union during the Cold War, would enhance our knowledge base and increase the pool of recruits available for government work over the long term.
Session 7

Emerging Technologies for Homeland Security/Defense
Governmental and Industry Perspectives

MODERATOR
Dr. Dale Klein, Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs

SPEAKERS
Shana Dale, Chief of Staff and General Counsel, Office of Science and Technology Policy
Paul M. Longsworth, Deputy Administrator for Defense Nuclear Nonproliferation, National Nuclear Security Administration, Department of Energy
Dr. Hugo B. Poza, Vice President for Homeland Security, the Raytheon Company
John Stammreich, Vice President Homeland Security, Phantom Works, the Boeing Company

SUMMARY
Ms. Shana Dale
The OSTP provides scientific and technical expertise to the President and to White House senior officials. The OMB and OSTP jointly produce a budget guidance memo on a yearly basis. This
helps to guide the different federal agencies on their R&D submissions. The OSTP coordinates the science and technology activities of the federal agencies through the NSTC, a Cabinet-level council to the President.

- OSTP is involved in the following committees of the NSTC: Environment and Natural Resources, Science, Technology, and Homeland and National Security.

- The National Strategy for Homeland Security guides the federal government in terms of homeland security-related work. This document has objectives that guide and apply across critical mission areas. There are four themes that cut across all of these mission areas, including the importance of science and technology.

Efforts have been initiated to defend against biological weapons of mass destruction. The President has initiated the Bio-Surveillance Program Initiative, a $274 million government-wide program to integrate real time information on the health of the nation’s human and agricultural populations.

- The National Bio-Surveillance Integration System, a key element of the Bio-Surveillance Initiative, integrates and fuses data from sensors throughout the country, as well as human health information, agricultural health surveillance, and terrorist threat information.

- Since 2003, Project BioWatch has monitored atmospheric samples around the clock in approximately thirty cities. Further deployment of this project is expected.

- Project BioSense, initiated in Fiscal Year 2003, is an effort by the CDC to enhance the ability to monitor human health


17 President Bush’s Fiscal Year 2005 budget request includes a $274 million Bio-Surveillance Program Initiative designed to protect the nation against bioterrorism and to strengthen the public health infrastructure. The initiative will enhance on-going surveillance programs in areas such as human health, hospital preparedness, state and local preparedness, vaccine research and procurement, animal health, food and agriculture safety and environmental monitoring. (accessible in full at [http://www.dhs.gov/dhspublic/display?theme=43&content=3092&print=true](http://www.dhs.gov/dhspublic/display?theme=43&content=3092&print=true))
events. It also monitors the status of human populations by analyzing ambulatory care sites, laboratory testing orders, and over-the-counter drug sales.

The administration is aggressively pursuing the development and acquisition of medical countermeasures to safeguard citizens in the event of a WMD attack. A comprehensive, end-to-end review of the nation’s bio-defense capabilities culminated in the *National Strategy for Bio Defense in the 21st Century*.\(^\text{18}\) This directive charts a course for the development of countermeasures against CBRN attacks.

- Project BioShield is the effort to spur development and acquisition of medical countermeasures. The WMD Medical Countermeasures Subcommittee is an interagency group that establishes priorities for BioShield funding. The President has committed $5.6 billion over the next ten years to fight anthrax, smallpox, and other diseases. A priority of this program has been the development of a next-generation anthrax vaccine and seventy-five million doses of this vaccine will enter the National Strategic Stockpile in FY 2005.\(^\text{19}\)

Another area set forth in the President’s *National Strategy for Homeland Security* is biometrics technology.

- Biometrics technology has become an important technology for applications such as the positive identification of individuals coming across our border.

- OSTP has created the NSTC Interagency Working Group on Biometrics. This fosters U.S. government collaboration and minimizes duplication on biometrics research, development, testing, and evaluation by developing and implementing interagency coordination plans. It also functions as the govern-

\(^{18}\) Biodefense for the 21st Century is a presidential directive signed in 2004 that provides a comprehensive framework for our nation’s biodefense. Biodefense for the 21st Century builds on past accomplishments, specifies roles and responsibilities, and integrates the programs and efforts of various communities -- national security, medical, public health, intelligence, diplomatic, agricultural and law enforcement -- into a sustained and focused national effort against biological weapons threats. (accessible at [http://www.dhs.gov/interweb/assetlibrary/HSPD10Biodefensefor21stCentury042804.pdf](http://www.dhs.gov/interweb/assetlibrary/HSPD10Biodefensefor21stCentury042804.pdf))

\(^{19}\) The Strategic National Stockpile consists of drugs, vaccines, and medical equipment that is stored at multiple sites throughout the United States.
ment’s clearinghouse for information on biometrics research, technologies, and technical policy issues.

The NSTC working group has been developing international working groups on biometric technologies and developing common U.S. government positions when possible. The group initiated a face recognition challenge where agencies will join forces to achieve the goal of improvements in the performance of face recognition systems. On January 5, 2004, US-VISIT biometric entry procedures were deployed at 116 airports and fourteen seaports.20

- In its first six months of operation, US-VISIT biometric entry procedures identified 559 individuals as being suspicious subjects.
- By 2004/2005 there will be extensive biometrics testing, including 200,000 prototype transportation worker identification credentials issued by DHS.
- The Airport Access Control Program verifies the identification of airport employees. Five airports are evaluating the TSA-registered traveler pilot program to identify frequent travelers who have voluntarily submitted to background checks.
- TSA has a biometric device to evaluate nine biometrics products including fingerprints, hand shape, iris recognition, and face recognition systems.

OSTP has been engaged in developing systems to detect hostile intent by identifying groups or individuals who threaten us.

- Research in this area includes the examination of cultural and sociological factors that may give rise to an environment conducive to terrorism, as well as individual biological and behavioral indicators.
- The National Science Foundation has initiated a new five-year research program in human and social dynamics to stimu-

20 US-VISIT is part of a continuum of security measures through the Department of Homeland Security. It incorporates eligibility determinations made by the Department of Homeland Security and the State Department. When a visa is issued by the Department of State, biometrics such as digital, inkless finger scans and digital photographs allow the Department of Homeland Security to determine whether the person applying for entry to the United States is the same person who was issued the visa (information on US-VISIT is accessible at http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0424.xml).
late break-through knowledge about human action, as well as organizational and cultural issues.

• DHS, intelligence agencies, and other agencies are investing in research and technology to detect deception. On July 6, 2004, DHS released a call for proposals for a university-based center of excellence in behavioral and social aspects of terrorism and counterterrorism.

The NSTC Social, Behavioral, and Economic Sciences Subcommittee will soon release its report on combating terrorism and research priorities in the social, behavioral, and economic (SBE) sciences.

• The report emphasizes the SBE science’s role in predicting, preventing, preparing, and recovering from terrorist attacks.

• The report outlines research priorities, such as the development of datasets, the application of decisions science methods to risk communications strategies, the development of biometric and bio-imaging capabilities, the elucidation of the basic neuro-mechanisms of fear and anxiety, the development of robust, valid models of psychobiological and psychosocial mechanisms of distress and resilience, and the development of robust cross-cultural models of social behavior.

On first responder technology, OSTP is working within the federal government to expedite existing technology to the field, to develop standards and engage in research and technology development, and to develop medical emergency preparedness and emergency planning. The current presidential administration is committed to American science and innovation and the pursuit of research and technology to protect the homeland.

Mr. Paul M. Longsworth
The U.S. government has a unique responsibility to stop transnational terrorist threats before they get to our borders. The objectives of the National Nuclear Security Administration (NNSA) are to stop those threats by cooperating with over seventy countries. The NNSA accounts for, secures, and eliminates tools that terrorists would use such as nuclear weapons, fissionable material, and radiological dispersal devices. There are three phases to the program.
• The first phase is to eliminate the materials that terrorists use. These programs are primarily being implemented in Russia, where we secure over 600 metric tons of fissionable material. We are building plants that can process plutonium and eliminate surplus weapons in Russia and in the United States. We are blending down highly enriched uranium and burning it in reactors within the United States.

• The second phase is to detect whether those efforts have failed. We do this by installing radiation detectors at airports, seaports, and land border crossings. We do this through space-based assets, ground-based assets, and airborne assets. Most of our R&D efforts are focused on detecting whether people are trafficking in nuclear material.

• The third phase is conducted at the U.S. border where NNSA is trying to stop threats before they enter the United States. The NNSA is focused on technologies and challenges. Currently, we are spending $200 million a year on new technologies. Many of these get deployed on space-based assets and we build and deliver them to other federal government agencies. We do this for treaty monitoring and improving trafficking detectors that can be used at seaports and land border crossings.

• Better remote sensing technology, such as synthetic aperture radar, is being developed for the purpose of giving a before and after picture of an incident.

• We have developed Palm Pilot and cell phone-based equipment to improve standoff detection for shielded nuclear materials. This provides greater security for inspectors at border crossings.

• There is progress being made in advanced radiation detection technologies. Current detectors for trucks, trains, other vehicles, and cargo containers use a gross count system that indicates whether radiation is present, but does not indicate the isotope. Real time isotope identification methods are being developed primarily through Sandia National Laboratories. They have developed a sodium iodine smart detector that can detect radiation and identify the isotope, thereby eliminating
the need for secondary inspections. These real time isotope identification systems minimize the training for operators and are able to handle high volume and multilane traffic.

- Real time detectors, however, have drawbacks. These include the cost and limited commercial availability of the detectors. The NNSA has been working with commercial vendors to begin building, demonstrating, and marketing real time systems. Sandia has signed an agreement with Thermal Electron to commercialize one of these detectors.

- We are also working to improve hand-held detection equipment.

We are trying to advance our capabilities, but face some challenges in doing so.

- Transshipment is one of the biggest problems. Through the Megaports Initiative, NNSA will equip the twenty largest ports in the world that ship to the U.S. with radiation detectors.\footnote{The Megaports Initiative is a program aimed at thwarting illicit shipments of nuclear and other radioactive material. (information can be found at \url{http://www.nnsa.doe.gov/docs/NA-04-FS01.pdf})} The trans-shipped cargo that comes through the Rotterdam, Netherlands port undergoes a radiation detection screening process. The Rotterdam port is one of the few that is fully equipped and operational.

- NNSA is trying to develop a crane-mounted radiation detection system, although there are challenges related to equipment survival and cost. In terms of equipment survival, the system has to be exceptionally robust and able to withstand application. In addition to this, the cost of putting a detector on every spread bar is also very expensive. In spite of these limiting factors, we think that we have a system that will be in application soon.

There is a need for interagency cooperation. We have extensive cooperation with the Office of the Secretary of Defense and other federal agencies primarily through the National Security Council. The NNSA participates in the Proliferation Strategy Working Group, which discusses programs that are needed to interdict materials overseas and the technology needed to detect them. We also
work closely with the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs, Dr. Dale Klein, on several counterterrorism groups where we share technology and operational experience.

- We work with DHS through the Container Security Initiative. The Megaports Security Initiative is part of this effort.
- We provide training to Customs agents on how to identify and respond to threats. We provide training for governments overseas as well.

**Dr. Hugo Poza**

The homeland security business at Raytheon is divided into three areas: information analysis, infrastructure and protection, which we call “Detect;” border and transportation security, or “Protect;” and emergency response, or “Respond.”

- “Detect” focuses on data collection and analysis, and the key challenge is being able to absorb all the available information so that it enables effective decision-making.
- Our products are designed to access data from a variety of sources and IT architectures. They can be used to screen passengers and foreign visitors, and perform background checks. One particular product, *Genesis*, collects data from different sources and yields recommendations to border guards, analysts and other potential users.

In the “Protect” area, the focus is on integrating various data to provide extensive situational awareness and thereby enable intelligence decisions that protect our borders and critical infrastructure.

- The data may include information on weather and terrain conditions, emergency services, conditions at particular facilities, and biometric data, as well as data from infrared and imaging
sensors and advanced communications systems. Our products will also enable modeling and simulation.

- The key task is to coalesce all of the data into one point to facilitate decision-making.
- Our Sensor Terrain Analysis Tool assesses environmental and local conditions in a particular location, and helps in evaluating, for instance, the trustworthiness of border guards at particular crossings in the Ukraine or Uzbekistan.

Communications interoperability and patient tracking represent two key aspects of our emergency response business.

- Since 9/11 the inability of first responders to communicate with each other has remained a major problem. The ACU-1000, developed at Raytheon JPS Communications, links incompatible radio systems. The entire County of Los Angeles could be made interoperable at a cost of $7.5 million.
- Our Emergency Patient Tracking System, currently being used by all thirty-six hospitals in St. Louis, allows hospitals to communicate and exchange information with one another, thereby facilitating a more effective response to a natural or man-made disaster. It can also facilitate the containment of disease outbreaks through tracking incoming patients. For instance, if there were 1,000 lungs cases on one day, while in the past the daily average was twenty, local health authorities could be alerted to investigate the anomaly and undertake necessary measures if needed.
- Many existing products and technologies developed under DOD and U.S. government funding can, in general, be applied to improve our homeland security efforts. Operational adaptation can be achieved with some investment.

Mr. John Stammreich

There is insufficient strategic-level thinking on homeland security issues within the U.S. government.

- We must recognize that we cannot completely eliminate all threats.
- We must balance effectiveness and affordability when setting priorities for homeland security expenditures.
• Policies sometimes have unintended side effects. It may appear logical to put military anti-missile technology on our entire commercial fleet of 17,000 airplanes. But the technology is not well-suited for commercial application, and terrorists might upgrade to a more advanced version of a shoulder-launched missile and effectively overcome the installed defenses. In this instance, the billions spent on anti-missile technology would not make the public any safer.

Network-centric operations can provide the right information, at the right time and to the right people, and are essential for pro-actively deterring and defeating terrorists.

• Network-centric operations consist of a number of tools and capabilities, including automated cognitive knowledge management, interoperability between new and legacy systems, broadband communications, and visualization systems that fuse imagery into usable intelligence. Much of this enabling technology originated within the private sector.

• Network-centric operations will, for instance, allow a security guard to watch 300 to 400 cameras at one time.

• Network-centric operations are being developed in a more evolutionary and iterative development process, bypassing conventional modeling and development procedures.

• Within the commercial sector, companies such as Wal-Mart are using the latest network-centric tools to provide real-time information on the buying habits of their customers and the environmental factors that influence their customers, suppliers and competitors.

• Going forward, network-centric operations will continue to be developed in a collaborative fashion, acquiring capabilities unforeseen by their original creators. The commercial sector will remain influential, as threat correlation capabilities, cognitive management tools, and decision aids will migrate from commercial to public sector software applications.

The impact of network-centric operations on homeland security will be measured by its contributions towards the establishment of effective layered defenses.
A network of sensors is more effective than an individual sensor. Given the diversity of threats that we face, we will never be able to develop, for instance, the perfect biosensor. No single technology will provide a solution. A layered, networked group of sensors would provide greater security.

Automated cognitive information systems capable of sharing and collaborating will make a significant impact on our homeland security capabilities.

New capabilities will arise from a “technological push” rather than from a “requirements pull,” by discovering new uses for existing technologies.

Complementary advances are being made in both the commercial and the DOD network worlds. To achieve the situational and domain awareness required to contain terrorism, we need to take advantage of the dynamism within the network world.
FINAL REPORT

FROM A CONFERENCE ORGANIZED BY
Institute for Foreign Policy Analysis
International Security Studies Program of
The Fletcher School, Tufts University

WITH THE SPONSORSHIP OF
United States Northern Command
Defense Threat Reduction Agency