



Homeland Defense A Strategic Approach

Joseph J. Collins
Michael Horowitz

December 2000

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

About CSIS

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

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

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

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

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

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

Final Draft: Homeland Defense: A Strategic Approach

--- Joseph J. Collins and Michael Horowitz ---

As of: December 11, 2000 PM

Embargoed until 12:01 AM, December 14, 2000

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

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

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

Introduction

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

America will become increasingly vulnerable to hostile attack on our homeland, and our military superiority will not protect us....States, terrorists, and other disaffected groups will acquire weapons of mass

destruction, and some will use them. Americans will likely die on American soil, possibly in large numbers.¹

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

To many, homeland defense appears to be a new requirement, but the perception of homeland defense as a new mission strips it of an important part of its context. Homeland defense --- the defense of United States territory, critical infrastructure, and the population from direct attack by terrorists or foreign enemies operating on our soil --- was, is, and will always be the most essential function of our government. Indeed, nearly every statement of our national strategy has had the protection of our homeland and its critical infrastructure at the top of its list of vital interests.³ Guarding the homeland has also been a constant activity of the government, using everything from the Strategic Air Command to the Coast Guard’s cutter fleet to the border patrol to state and local police forces.

What is changing, however, is not only the level and type of threat, but also how we accomplish homeland defense. During the Cold War, major threats to the U.S. homeland came primarily from hostile foreign powers and, in particular, the Soviet Union. Attacks on the homeland by these powers were prevented primarily through the deterrent effects of strategic nuclear weapons with an able assist from the forward-deployed forces. Air defense was handled by the North American Air Defense Command. Civil defense was part of the total effort, but except for the period of the mid-50s to early 60s, it was a distinctly small and arguably ineffective part of it.

Today, the shape of homeland defense has been influenced by three factors: the uniquely dominant power position of the United States, the technological development of certain states hostile to the United States, and the onset of the information age, which has empowered individuals and non-state actors.

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

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

³ William S. Cohen, “Chapter 1: The Defense Strategy,” *Department of Defense: Annual Report to the President and Congress*, 2000, www.dtic.mil/execsec/adr2000/chap1.html (Accessed November 2000). Executive Office of the President. *A National Security Strategy for a New Century* (Washington, D.C.: The White House, 1999), pp. 1, 2, 4.; Graham Allison and Robert Blackwill. *America’s National Interests: A Report from the Commission On America’s National Interests* (Cambridge, MA: The Commission, 1998), pp. 5, 19-21.

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

A second factor is the technological development of many nations that pose a potential threat to the United States. Many rogue states --- a short-hand expression for about a half dozen states hostile to U.S. interests, including Iran, Iraq, and North Korea --- are entering the latter stages of the industrial age and gaining the ability to develop chemical, biological, nuclear, and missile technology. At the same time, for both strategic and economic reasons, Russia, China, and North Korea have compounded the proliferation problem. The efforts of these three countries --- whether economically or politically motivated --- may not be specifically directed against the United States, but nevertheless pose heightened risks to U.S. interests.

While missile systems --- unlike terrorists --- leave behind a very risky "return address," they are still a factor in the homeland defense equation. National missile defense has been an issue for nearly 35 years, but today it has a new sense of urgency and a different focus. In the latter half of the Cold War, the focus of missile defense efforts was protection against potentially massive Soviet attacks. Today, for most analysts, the focus is on protection from accidental attacks from great powers or small attacks from Iran, Iraq, or North Korea.

Information technology and globalization provide a third factor. The onset of the information age --- marked by the development of the personal computer and the expansion of the Internet --- has decreased the power of states and other mass hierarchical organizations and increased the capabilities of markets, individuals, small groups, and networks. Individuals and non-governmental organizations (NGOs), --- the logical, issue-oriented extension of empowered individuals --- have become important subsidiary actors in international relations. Economic and even social relations have become subject to globalization, a force outside the control of even the most powerful states.⁴

These factors present us with a set of threats that are steadily becoming more serious. In an era of global communications and expanding trade and travel, states or small groups of terrorists --- of foreign or domestic vintage --- can directly attack the United States homeland. The knowledge that tells them how to do this is often free to all on the Internet. The resulting attacks can be by conventional means (gun, knife, or bomb), or they can exploit the growing body of knowledge about CBRN --- chemical, biological, radiological, or nuclear --- weapons or information and the vulnerability of

⁴ Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Anchor Books, 2000), pp. ; and Thomas L. Friedman, "Parsing the Protests," *The New York Times*, April 14, 2000, p. A 31.

telecommunication systems.⁵ As noted above, a small number of states also represent a potential ballistic or cruise missile threat to the U.S. homeland.

Terrorists in some ways pose a tougher threat than small nations with missile capabilities. Aided by rogue states, today's terrorists may --- without leaving a "return address" --- be able to inflict mass casualties, defined here as at least 1,000 casualties (killed, wounded, or sickened). In the future, small groups of terrorists may well be able to make devastating use of CBRN weapons without the help of rogue states.

At the same time terrorists, insurgents, and criminals have often formed strong links for mutual benefit. These links are particularly salient in the area of narcotics traffic. As in the case of Columbia --- strong bands of narco-terrorists can easily rival the power of many small and medium sized states. Moreover, the effects of narcotics traffic on the United States is significant in and of itself. It is estimated that over 50,000 Americans die every year from the effects of narcotics.⁶ Of course, the narcotics threat is different than other threats to the homeland in that there is a considerable domestic demand for narcotics.

Enemies of the United States, opponents of its Armed Forces, or those in opposition to U.S.-based multinational corporations can also choose cyber crime, cyber vandalism or cyber attacks against US public or private interests, turning our reliance on information systems into a strategic vulnerability.⁷ Cyber vulnerability is magnified by the fact that 95 percent of all U.S. military traffic moves over civilian telecommunications and computer systems. A terrorist can combat our military forces, disrupt a military operation, or hurt our economy by hindering our vulnerable civilian telecommunications systems.

Some terrorists are already practicing: In 1999, there were over 22,000 attacks against unclassified military computer systems, a threefold increase over the amount reported in

⁵ This report will use CBRN for accuracy. It clearly denotes the classes of weapons under discussion. CBRN weapons do not always achieve mass destruction. The less precise Weapons of Mass Destruction (WMD) couples an ambiguous set of weapons with the effects that these weapons may or may not achieve. Moreover, conventional ordnance may well achieve mass destruction under certain circumstances.

⁶ Presentation by Dr. William Olson to the Policy Integration Group of the CSIS homeland defense project, June 28, 2000. Because of time and space limitations, this report will not examine the serious, on-going narcotics threat to the United States. Our omission is not meant to suggest that international narcotics traffic is not a serious threat to the U.S. homeland, only a unique one. CSIS has previously addressed this threat in a number of reports, including the one cited in the note immediately above this one.

⁷ Frank Cilluffo and Bruce Berkowitz, eds., *Cybercrime, Cyberterrorism, and Cyberwarfare: Averting an Electronic Waterloo, A Report of the Global Organized Crime Project*, (Washington, DC: Center for Strategic and International Studies, 1998), pp. 1-72.

the previous year. A few experts believe that number to have reached a few hundred thousand per year.⁸ Some estimates suggest only 10 percent of penetrations are detected.

While information attacks in and of themselves do not pose a threat of mass destruction, they can wreak havoc on many levels. After discussing a serious act of cyber vandalism, Dick Clarke, the National Coordinator for Security, Infrastructure Protection, and Counterterrorism, reminded a CSIS-sponsored, Capitol Hill audience:

This is the low end of the cyber terrorism spectrum. It moves up through extortion, fraud, and industrial espionage. At the far end of the spectrum is war by computer attack. When the NATO alliance bombed Serbia last year, they hit mainly infrastructure. In the United States, the telecommunications, transportation, and electric power infrastructure depend on computer controlled networks. Each of these networks can be penetrated by a determined adversary. There is a unique challenge here. For the first time in our history, the Armed Forces cannot defend us from the foreign threat. They cannot surround the power grid....Therefore, we are asking the private sector to defend not only itself, but the country as well.⁹

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

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

⁸ Jim Wolf, “Hacking of Pentagon Computers Persists; Pace Undiminished This Year, Complicating Security Efforts,” *The Washington Post*, August 23, 2000, p. A23..; and comments by Richard Clarke at a lecture for MIT Alumni Association, October 10, 2000.

⁹ Richard Clark, “Homeland Defense: Proceedings of the April 5th Senior Advisory Group Meeting and Participants List,” 2000, webu6102.ntx.net/homeland/reports/sag040500.html (Accessed November 2000).

retaliation after attacks on our homeland increasingly difficult. A delay in identifying such attacks could be very costly.

The following matrix of threats shows the varying intensity and probabilities of homeland defense threats. It also shows the variety of front-line defenders who must be trained and whose activities must be coordinated.

Matrix of Threats to the Homeland

	<u>Threat</u>	<u>Potential for Mass Destruction</u>	<u>Attack Probability</u>	<u>First-Line of Defense</u>
Missile Attack	Foreign, Rogue State	Significant in Mid- to Long-term	Very Low	Military
Major Cyber Attack*	Foreign or Domestic	Negligible; but high for disruption	Significant	Information Technicians.
CBRN *** Terrorism	Foreign or Domestic	Significant in Mid- to Long-term**	Low	Local Officials

Notes:

* For example, a directed cyber attack against a major telecommunications facility, the stock market, or a government agency.

**In near-term, could be significant if terrorists received state assistance.

***Biological or nuclear-related events pose greatest threat of mass destruction.

Terrorists may also achieve mass destruction with conventional explosives, especially if used against sensitive infrastructure targets, such as chemical plants or nuclear reactors.

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

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

part of that process, but ultimately, we are the ones who are responsible for dealing with the people.¹⁰

Legal authority to act in non-traditional areas of homeland defense presents another dilemma. In routine operations, the National Command Authority has sufficient legal authority to use the Armed Forces at home. For example, *posse comitatus*, the law that prohibits most military personnel from engaging in law enforcement, is sufficiently flexible to permit exceptions for riots, civil disturbances, and even support for counter-narcotics programs. An expert on military law told a CSIS Working Group:

The Posse Comitatus Act has never been an absolute prohibition on the military's involvement in maintaining domestic order. Even when originally enacted it was recognized that there were certain exceptions to its scope....There are few areas of domestic law enforcement activity where the military is precluded from participating in times of national emergency or disaster. Through proper, legal declarations of Presidential emergency authority and/or through the use of National Guard assets in state status, it is increasingly likely the military will play a significant enforcement role in response to domestic terrorism and other disasters for the foreseeable future.¹¹

There are, however, more complex, unresolved legal issues concerning homeland defense. Since meeting contemporary threats may involve extensive information gathering at home, homeland defense tasks will be especially sensitive to a nation that jealously guards its civil rights. The specter of massive federal involvement in terrorist incidents has been the subject of a few major motion pictures but no significant political debate.¹² In one of his valedictory speeches, Secretary of Defense William Cohen highlighted the sensitivity of homeland defense issues and said: "I believe that we as a democratic society have yet to come to grips with the tension that exists between constitutional protection of the right to privacy [and] the demand that we made . . . to protect us."¹³

The issue of legal authority during mass destruction incidents in urban areas is especially problematic. In the case of such an unlikely but not impossible scenario, it is not even

¹⁰ Governor Christine Whitman, as recorded in "Homeland Defense: Proceedings of the April 5th Senior Advisory Group Meeting," 2000, webu6102.ntx.net/homeland/reports/sag040500.html (Accessed November 2000).

¹¹ Craig Trebilcock, "Posse Comitatus: Has the Posse Outlived its Purpose," April 2000, www.csis.org/homeland/reports/trebilcock.pdf (Accessed November 2000).

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

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

clear what the legal questions are, never mind what the answers to them might be. Expanding homeland defense roles for the Department of Defense may make sense; it will also set off alarms. Policy architects will have to balance individual rights with the need to protect society under difficult and potentially unique circumstances.

In summary, homeland defense can be viewed as the defense of the most vital of all of our traditional interests. It also comprises a new set of priority defense activities to meet novel threats that have in common the potential for direct impact on the United States. These threats have appeared in the form of missile proliferation in hostile states, the emergence of CBRN terrorism, and a variety of threats to the nation's critical information and economic infrastructure. Each of these threats is in many ways unique. New national strategies will have to deal with a wide range of both new and old challenges. Given the diversity of these threats, it is unlikely that there will ever be "unified field theory" of homeland defense. However, it will be possible to assess our progress in meeting potential threats and make some general recommendations that will unite the policy objectives or ends with the means needed to begin to solve this complex set of problems. That is the primary aim of this essay, but before we arrive at that destination, we must examine all of the threats in some detail, as well as the programs that we have already initiated to deal with them.

Threats

Missile Proliferation:

Weapons of mass destruction delivered by intercontinental ballistic missiles pose a substantial danger to the United States homeland. A rapid diffusion of technological know-how in the last decade has sped the evolution of ballistic missile programs in rogue states, while China and Russia have continued to deploy and refine their existing ballistic missile arsenals. Nuclear and missile proliferation on the subcontinent is another regrettable aspect of this problem.

Ballistic missile development technology and skills are becoming commonplace. In the 1991 Gulf War Saddam Hussein's SCUD missiles were erratic and even structurally unstable, but in the last decade many rogue states --- such as North Korea, Iran and Iraq -- have increased the pace and scope of their missile development programs. In 1993, North Korea tested the NoDong medium range ballistic missile. The NoDong has also found its way to Iran (Shahab) and Pakistan (Ghauri). India tested a medium range ballistic missile, the Agni, and is developing a longer-range missile. While this state of the art is a great worry for those concerned with theater missile defense, a more direct concern to the issue of homeland defense involves ICBM proliferation.

In 1995, a widely read National Intelligence Estimate (NIE) predicted that in the next fifteen years, the United States was not likely to face the threat of an ICBM from any state other than Russia or China. Missile defense advocates criticized the report, arguing

that it severely underestimated the threat and pace of ballistic missile proliferation.¹⁴ An independent panel formed by the CIA then countered that the ballistic missile threat was not even as severe as the 1995 NIE had indicated.¹⁵ Subsequent Congressional concerns led to the formation of the Rumsfeld Commission, led by former Secretary of Defense Donald Rumsfeld. The Commission, made up of experts on defense and ballistic missiles from throughout the policy community, conducted a complete examination of concerns surrounding ballistic missile proliferation.¹⁶

In July 1998, the results of the Rumsfeld Commission changed the tenor of the debate over ballistic missile proliferation. It concluded that the threat of ballistic missile proliferation had been severely underestimated by previous studies. It did not predict with certainty that a rogue state would develop an ICBM within the next few years. It did argue that the diffusion of missile development tools, cooperation in the developing world over missile development, and the risk of missile exports from countries such as Russia and China, made the risk of new ICBM powers developing in the next decade far from remote.

Several predications made by Rumsfeld have been borne out by subsequent events. First, the current non-proliferation regime is in trouble. With the United States rejection of the Comprehensive Test Ban Treaty (CTBT), nuclear developments in India and Pakistan, conflicts over the future of arms control between the United States and Russia, and other events, non-proliferation regimes are being tested as never before.

Second, the widespread diffusion of missile know-how has made the continued restriction of ICBMs to the major powers increasingly unlikely. A 1999 NIE acknowledged that rogue states were unlikely to follow “traditional” models of ICBM development. Emerging missile powers will likely have shorter testing programs, need fewer missiles for their operational mission, and have less stringent reliability and accuracy requirements. Therefore, the lead-time between medium and long-range missile development, and between initial flight tests and deployment will be much shorter for emerging powers.¹⁷

¹⁴ National Intelligence Estimate, “Emerging Missile Threats to North America During the Next 15 Years: PS/NIE 95-19,” November 1995, www.fas.org/spp/starwars/offdocs/nie9519.htm, (Accessed October 2000).

¹⁵ Independent Panel's report on NIE 95-19, "Emerging Missile Threats to North America During the Next 15 Years." December 23, 1996, www.fas.org/irp/threat/missile/oca961908.htm, (Accessed October 2000).

¹⁶ Rumsfeld Commission, “Report of the Commission to Assess the Ballistic Missile Threat to the United States,” July 15, 1998, 209.207.236.112/irp/threat/missile/rumsfeld/toc.htm, (Accessed October 2000).

¹⁷ Robert D. Walpole, “The Ballistic Missile Threat to the United States,” *Federal News Service*, (February 9, 2000): nexis.

In August 1998, as if to underscore the findings of the Rumsfeld Report, North Korea launched a multi-stage, solid fuel rocket called the TapeoDong 1. While the third stage failed to function, it demonstrated that North Korea is close to developing an operational ICBM, faster than even the Rumsfeld Commission had predicted.¹⁸ The TapeoDong, a three stage ballistic missile, demonstrated that missile programs starting from a SCUD infrastructure could advance beyond short or medium ranges, something previously not thought possible. This launch was a huge aid to those advocating the expeditious employment of missile defenses. Since the TapeoDong 1 launch, most experts consider that the burden of proof in the debate over national missile defense is on the critics of missile defense.

Missile technology exports are another factor confounding the analysis of emerging powers' missile programs. Exports of missile parts or technology can both decrease the lead-time for an ICBM program and increase the accuracy of missiles developed in that program. North Korea, or more importantly Russia or China, could severely decrease the amount of time before a rogue state acquires an intercontinental missile. While Russia agreed in 1999 to sharply limit their exports of ballistic missile components and China has apparently warmed to some international arms control agreements, they continue to export missile parts. Even if Russia and the China do not export a complete missile system, they can export key components that drastically increase the capabilities of a given missile development program. Also, the risk that Russia and China will export complete missiles must be considered; the impact would be so great that the risk, even if low, must be taken seriously.¹⁹ North Korea continues to export ballistic missiles and contravene international non-proliferation norms. For example, Libyan may well have acquired a NoDong prototype this summer. Cooperative missile development combined with key component purchases from Russia and/or China is the most likely scenario for multiple ICBM threats to the United States homeland in the short-term. Unfortunately, such a scenario cannot be ruled out with any certainty.

Most importantly, the development of missile networks poses a challenge to efforts aimed at restricting the flow of missile technology. While the first generation of missile networks, ones including Brazil and Argentina, collapsed by the early 1990s, a new generation of missile development cooperation has emerged. There is a clear line of missile development that goes from China to North Korea to Iran, Pakistan, and others. States that currently import ballistic missiles, such as Iraq and Syria (which recently

¹⁸ Robert D. Walpole, "North Korea's TD-1 Launch and Some Implications on the Ballistic Missile Threat to the United States." (paper presented at CSIS, Washington, D.C., December 8, 1998), p. 1.

¹⁹ George J. Tenet, "The Worldwide Threat in 2000: Global Realities of our National Security," *Federal News Service*, (March 22, 2000): nexis.

demonstrated a SCUD-D capability) could also increase the probability of ICBM proliferation if they begin to export their own missile expertise.²⁰

States engaged in ballistic missile proliferation can diffuse both technology and knowledge crucial to a successful missile program. The proliferation of expertise may even be more important than the hardware. Years can be taken off the timeline for long-range missile development if key scientists trained in missile development can be purchased or ‘traded’ among developing missile powers.²¹

A key point to consider is that even if current negotiations with North Korea end in an agreement to halt missile development and missile exports, the genie may already be out of the bottle with regards to missile proliferation. North Korean sales of the NoDong and purported sales of the technology necessary for the TapeoDong mean that it is just a matter of time before another country duplicates its success. Exports of parts or missiles from Russia or China could also fill a technological need in a rogue state.

In extremis, the danger of a ballistic missile attack on the United States or its allies cannot be dismissed as hyperbole.²² Rogue states have a high level of motivation to acquire long range ballistic missiles. In a war, United States air dominance will naturally lead hostile developing countries towards missiles as a way to counteract our advantage in the air. States may perceive the acquisition of long-range missiles, especially those that could threaten the United States, as a key hedge against the coercive power of U.S. air assets. The main motivation for the ballistic missile development programs of rogue states, as far as the intelligence community has been able to discern, involves increasing their ability to threaten and coerce the United States. It is also possible, and perhaps more likely, that the owner of such a missile could use it to coerce other nations in its own region. The ability of a rogue state to threaten the United States or one of its allies with a missile attack could well be part of a sophisticated enemy anti-access strategy.²³

While some have argued that states are much more likely to threaten the United States with non-ICBM means, such as cruise missiles, or more conventional terrorism, the implication of that statement is not an argument against acknowledging the ballistic

²⁰ Rumsfeld Commission, “Report of the Commission to Assess the Ballistic Missile Threat to the United States,” July 15, 1998, 209.207.236.112/irp/threat/missile/rumsfeld/toc.htm, (Accessed October 2000).

²¹ George J. Tenet, “The Worldwide Threat in 2000: Global Realities of our National Security,” *Federal News Service*, (March 22, 2000): nexis.

²² For an example of such a view, see The Coalition to Reduce Nuclear Dangers, “Pushing the Limits: The Decision on National Missile Defense,” July 2000, www.clw.org/coalition/libbmd.htm, (Accessed October 2000).

²³ George J. Tenet, “The Worldwide Threat in 2000: Global Realities of our National Security,” *Federal News Service*, (March 22, 2000): nexis.

missile proliferation threat.²⁴ While non-strategic missiles are a grave theater defense issue, it is difficult to maneuver short-range cruise and short-range ballistic missiles into a position where they could strike the US homeland. This may well change in the future, creating another potential vulnerability for the United States.

Some critics of missile defense have hyped the very real advantages that a covertly placed, terrorist device would have over a missile with a “return address.” However, the chances that the United States could intercept a ballistic missile fired by a developing power might well be substantially lower than finding and thwarting the use of one on its soil. It is possible that an adversary might calculate that a missile attack would have a higher probability of success than a CBRN terrorist attack.

It is important not to overstate the risk of a ballistic missile attack on the United States. A key lesson of the Rumsfeld Report is that enormous gaps in the intelligence community make accurate analyses of developing missile programs exceedingly difficult. However, it is important to acknowledge that such a threat does exist, even if it cannot be quantified, and even if its timeframe and location cannot be specifically denoted.

The enormous impact of an ICBM strike on the United States, especially if it involved a biological or nuclear warhead, also makes worst-case scenario planning a necessity. Thousands could die in a single strike. The United States would probably be forced to retaliate, leading to further escalation or even a large-scale war. Conversely, a weaker U.S. leader might be forced to back down in a regional crisis. If regional bullies can deter or disrupt U.S. military operations, faith in U.S. leadership could be greatly diminished.

Clearly, the United States must have multi-layered systems for both theater and national missile defenses. Putting our collective heads in the sand only makes that type of attack more likely to occur.²⁵ Building an effective defense is our best insurance that no power could ever credibly threaten us with a missile attack.

The Threat of CBRN Terrorism:

Terrorism is defined by the State Department as: ... premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine

²⁴ Joseph Cirincione, “Assessing the Assessment: The 1999 National Intelligence Estimate of the Ballistic Missile Threat.” *The Nonproliferation Review*, Spring: 125-137. Also see George J. Tenet. “The Worldwide Threat in 2000: Global Realities of our National Security,” *Federal News Service*, (March 22, 2000): nexis.

²⁵ George J. Tenet, “The Worldwide Threat in 2000: Global Realities of our National Security,” *Federal News Service*, (March 22, 2000): nexis. Also see Robert D. Walpole, “The Ballistic Missile Threat to the United States,” *Federal News Service*, (February 9, 2000): nexis.

agents, usually intended to influence an audience.²⁶ CBRN terrorism is simply an act of terrorism where a chemical, biological, radiological, or nuclear device is used or those elements are brought into play by other means, such as a conventional attack on a nuclear power plant. CBRN terrorism may or may not produce mass destruction. A terrorist use of conventional explosives may also produce mass destruction.

Americans are no strangers to terrorism. Indeed, as figure x [andreas small spreadsheet] shows, over 700 Americans have died at the hands of terrorists in the past two decades. Contemporary terrorism, however, is changing. While the number of terrorist attacks each year waxes and wanes, terrorism has become more lethal. The State Department's detailed records show that worldwide there have been 50% more casualties from terrorism in the 1990s than there was in the preceding decade.²⁷

Today, terrorism against the United States may occur inside the homeland, as well as abroad. American embassies and isolated, overseas military installations will remain vulnerable. At home, not only landmark buildings and government installations, but crops and agricultural facilities may be the target. The terrorists attacking U.S. interests may be foreign or domestic. Terrorist funding today is less likely to come from organized states, although state funded terrorism remains a key factor in the Arab-Israeli dispute.²⁸

Networks of terrorists, as opposed to larger, more hierarchical organizations are now the norm. Their objectives may be more deadly, and their political content may be more difficult to understand. Modern terrorists --- including those that struck our forces in Khobar towers and the U.S.S. Cole --- do not always "take credit" for their work, complicating responses. They will also have access to advanced technologies that could both increase their power and improve their ability to communicate with one another in a secure fashion.²⁹

²⁶ Office of the Coordinator for Counter Terrorism in the Office of the Secretary of State, "Patterns of Global Terrorism: 1999-Department of State Publication 10687," April 2000, www.state.gov/www/global/terrorism/1999report/patterns.pdf, (Accessed November 2000). The DOD definition is similar, but does not limit attacks to non-combatant targets and notes that the goals of terrorists are usually political, religious, or ideological in nature. Office of the Joint Chiefs of Staff. *DOD Directory of Military and Associated Terms- Joint Chiefs of Staff Publication 1-02* (Washington, D.C.: Office of the Joint Chiefs of Staff, June 1998), p. 452-53.

²⁷ L. Paul Bremer III, *Countering the Changing Threat of International Terrorism: Report of the National Commission on Terrorism* (Washington, D.C.: The Commission, July 13, 2000), pp. 2, 5.

²⁸ *Ibid.*, p. 3.

²⁹ *Ibid.*, p. 6

More importantly, terrorists in the future are likely to want to create mass casualties and to have an improved capacity to do just that. A number of incidents suggest a disturbing trend in both domestic and international terrorism. In the World Trade Center bombing in 1993, where 6 died and over 1,000 people were injured, and in the destruction of the Murrah Building in Oklahoma City in 1995, where 168 died, and hundreds were injured, we have already seen potent attempts at achieving mass casualties.

The case of the Japanese cult Aum Shinrikyo was also telling. This cult unsuccessfully attempted to spread anthrax spores but was later partially successful in using nerve gas in the Tokyo subway system. While their technology failed and (thankfully) only 12 people were killed in the subway incident, 5,000 went to hospitals, reminding us that the threat of mass casualties in the future may well be compounded by the effect of mass panic.³⁰

There are numerous types of CBRN weapons that --- alone or in conjunction with conventional explosives --- may create havoc or even mass destruction.³¹

There is also some evidence of a growing interest by terrorists in using chemical, biological, radiological, and nuclear (CBRN) devices. In 1999, the Center for Nonproliferation Studies recorded 175 terrorist-related incidents (including hoaxes) that involved weapons of mass destruction (WMD), a number that represents 25 percent of the total WMD incidents since 1900.³² Since the dissolution of the Soviet Union there have been numerous cases where groups of various pedigrees have attempted to obtain nuclear devices, or fissionable or other radioactive materials. Iraq alone has never accounted for 19,000 liters of botulinum toxin, 8,500 liters of anthrax, and 2,200 litres of aflatoxin. A high NSC staff official said recently: "Terrorist groups, including Osama bin Laden are attempting ... to get chemical weapons and even experimenting with nuclear materials."³³ Many analysts consider the use of CBRN devices in a terrorist incident a matter of when, not if.

It is important to note here the underlying causes of this problem. First, the nature of terrorism is changing. In 1994 former CIA Director R. James Woolsey's said that,

³⁰ For a very complete analysis of lessons learned from Aum Shinrikyo, especially the relative difficulty of successful biological weapons terrorism, see Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (The Gilmore Commission), *First Annual Report: I. Assessing the Threat*, December 15, 2000, pp. 46-51.

³¹ For a basic list with characteristics, see Anthony Cordesman, *Defending America: Redefining the Conceptual Borders of Homeland Defense – Risks and Effects of Indirect, Covert, Terrorist, and Extremist Attacks with WMD* (Draft), Sept. 1, 2000, Table Five, pp. 11-15, at www.csis.org/homeland/reports/EffectsterWMD.pdf.

³² Cameron, Gavin et al, "1999 WMD Terrorism Chronology: Incidents Involving Sub-National Actors and Chemical, Biological, Radiological, and Nuclear Materials." *The Nonproliferation Review*, Summer 2000: 2-3.

³³ Richard Clarke in an interview with Lesley Stahl, *60 Minutes*. October 22, 2000.

“Today’s terrorists don’t want a seat at the table, they want to destroy the table and everyone sitting at it.”³⁴ CSIS scholar, Walter Laquer described the evolution of fanatic terrorists in this manner:

Once upon a time terrorism was “propaganda by deed,” and the terrorists’ intention was to create as much noise as possible, not to cause the greatest number of fatalities. But this, quite often, is no longer true. The element of propaganda has receded or even disappeared altogether, and the intention now is to wreak as much havoc as possible.³⁵

Laquer notes that these new types of terrorists may have nationalist-religious roots, apocalyptic visionary roots, or sociopathic roots. None of these motives are new, but they appear to be more commonplace. Moreover, all of these groups have easy access to information about CBRN weapons. This knowledge, freely floating in cyberspace, has been reinforced by the presence in rogue states of scientists trained in the West, as well as disaffected experts who have left the former Soviet Union to seek more rewarding careers in states interested in CBRN and missile proliferation. The aging Russian nuclear weapons arsenal and the detritus of its huge chemical and biological weapons programs are additional concerns.

Other reasons for an increasing risk of CBRN terrorism have previously been mentioned. As the sole superpower with an active internationalist foreign policy, the United States at home and abroad has become the focus of the angst and bitterness of rogue states and non-state actors. Effectively combating a superpower requires the selection of asymmetrical means used against targets of opportunity. Foreign and domestic critics who perceive themselves as disenfranchised by globalization may also focus their anger on the United States. Disaffected American fascists, anarchists, or even garden variety lunatics may see globalization as the cause of their plight and seek revenge by way of CBRN terrorism. While state sponsorship of terrorism may be waning, terrorist movements still thrive as independent non-state actors, empowered by an Internet that enables them to communicate well and brings them much of the information that they need to employ high lethality devices.

Thankfully, there are numerous obstacles to and disincentives for the terrorist use of CBRN weapons. First, obtaining CBRN materials is still difficult. Second, it is difficult to store and transport most CBRN materials. Third, these weapons are --- compared to conventional explosives --- relatively difficult to weaponize or disperse. Compounding this problem, the effectiveness of chemical and biological weapons are highly dependent

³⁴ James Woosley, “Hearing of the House National Security Committee: Threats to National Security,” *Federal News Service*, (February 13, 1997): nexis.

³⁵ Walter Laqueur, “The New Faces of Terrorism,” *The Washington Quarterly*, (Autumn 1998: 171-172. For an opposing view see Ehud Sprinzak, “The Great Superterrorism Scare,” *Foreign Policy* (Fall 1998): 110-124.

on wind and other weather conditions. This makes them less reliable and complicates planning. Fourth, the negative image of CBRN weapons or materials adds to domestic and international surveillance associated with them. Fifth, given taboos associated with CBRN weapons, using them --- even if they did not achieve mass destruction --- would likely bring a stronger response from authorities than the use of conventional explosives. In short, there are many reasons why even a maniacal terrorist would stick with conventional explosives or firearms.

The Gilmore Commission's detailed study of Aum Shinrikyo's well-funded attempt to disperse anthrax and use sarin gas in the Tokyo subway system concluded that:

Aum's experience suggests --- however counter-intuitively or contrary to popular belief --- the significant technological difficulties faced by any nonstate entity in attempting to weaponize and disseminate chemical and biological weapons effectively. Although the Aum experience represents only a single point of reference, it provides a striking refutation of the claim about the ease with which some weapons can be fabricated and made operational.³⁶

Aum's efforts, however, offer no solace for the future. Aum's people did not have adequate scientific supervision and may have been sabotaged from the inside. In the future, the potential use of biological agents --- anthrax, plague, mycotoxins, etc. --- is particularly troubling and may well become a more attractive option for a hostile state or terrorist bent on mass destruction. Ounce for ounce, the lethality of these agents is many times that of chemical agents or nuclear weapons. Pounds or possibly ounces of biological agent can do a job that would require tons of a chemical agent.

- In one study, 30 kilograms of anthrax spores applied in a densely populated area at maximum effectiveness created 500 times the number of deaths that could have been produced by 300 kilograms of deadly sarin nerve gas.
- A 12.5 kiloton (thousand tons of TNT equivalent) nuclear device --- close to the potency of the bomb dropped on Hiroshima --- employed in the same area would likely have produced 20 percent fewer deaths than well-dispersed anthrax under relatively ideal climactic conditions.³⁷
- Another study suggested that the lethality of 250 pounds of anthrax, spread efficiently over the Washington D.C. metropolitan area, could cause up to 3 million deaths,

³⁶ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *First Annual Report: I. Assessing the Threat*, December 15, 2000, p. 48.

³⁷ Anthony Cordesman, *The Risks and Effects of Indirect, Covert, Terrorist, and Extremist Attacks with Weapons of Mass Destruction: Challenges for Defense and Response*, September 1, 2000, webu6102.ntx.net/homeland/reports/EffectsTerrWMD.pdf (Accessed November 2000).

significantly more than would likely result from a 1 megaton (a million tons of TNT equivalent) hydrogen bomb.³⁸

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

Many recent studies have pointed out the difficulties that terrorists would incur if they wanted to use biological agents. However, several factors make the use of biological agents by terrorists a substantial danger in the future. First, in the near term, non-state actors may be helped by rogue states, removing technological obstacles to the efficient use of any kind of CBRN weapons. Second, proliferation in the developing world or the insecurity of the Russian or Iraqi CBRN arsenal may provide a ready source of agent to terrorists. Third, future advances in genetics may make it easier to create more potent and more easily useable agents. Fourth, technological barriers to the effective dispersal of biological agents are disappearing and knowledge of these advances will inevitably spread.³⁹ Finally, our medical and public health systems do not have the capacity to handle a large-scale, CBRN terrorist attack. In the future, terrorists using biological weapons are likely to have a much greater capacity for mass destruction.

Today, terrorists using CBRN weapons pose a significant threat of mass disruption. Tomorrow, they are likely to have a much greater capacity for mass destruction. The time to take preventive action is now.

The Cyber Threat:

The threat of cyber-attacks on US government or private interests, as well as other kinds of attacks on critical infrastructure nodes are increasingly dangerous. Dr. Ruth David and Randy Larsen of ANSER Corporation said:

[D]ue to our increasing dependence on information technology, America is even more vulnerable than most countries to cyber attacks. We all witnessed what two junior college dropouts can do when they launched the “I Love You” virus on the Internet. In April 1998, a few dozen government employees assumed the role of the enemy in an exercise called ELIGIBLE RECEIVER. They quickly demonstrated their ability to shut down America’s power grid and seriously disrupt U.S. forces in the Pacific. Imagine what damage a 21st century adversary could inflict with a team of computer engineers trained in America’s best universities.⁴⁰

³⁸ Tara O’Toole, “Biological Weapons: National Security Threat and Public Health Emergency,” a presentation at CSIS, August 22, 2000.

³⁹ Randall J. Larson and Ruth A. David, “Homeland Defense: Assumptions First, Strategy Second,” *Strategic Review*, (Fall 2000): 6-8.

⁴⁰ *Ibid.*, p. 6.

Threats to U.S. critical infrastructure are a danger to the vitality of the United States economy, as well as to national security. As one recent account of cyber-threats reported, “the technical lifeblood of modern society [is found in our] dams, power grids, air traffic control systems, telephone networks and banking. If those infrastructure sectors are the nation’s lifeblood, digital commerce provides the vessels through which it flows.”⁴¹ Thus, it is important not only to protect the physical structures of critical infrastructures, but the information nodes that allow them to function properly.

There are four basic concerns:

- First, a terrorist could attack critical economic or telecommunications infrastructure, such as sabotaging a dam or bombing an electricity plant.
- Second, and perhaps more disconcerting, a competent computer scientist equipped only with a Pentium III and a modem located anywhere in the world could wreak havoc on U.S. computer systems, causing power failures in hospitals, information network shutdowns, or other problems.
- Third, the CIA and FBI have identified several nations currently developing cyber warfare capabilities, though no nation has yet deployed them in a ‘combat’ situation.⁴² Our Armed Forces place tremendous emphasis on their information systems and have great vulnerabilities in this area, as well as awesome counterattack capabilities.
- Fourth, several attacks could occur in tandem, baffling authorities as a growing cycle of violence cripples the response capabilities of the United States government.

Imagine a cyber attack on the public health system that shuts off the power at critical medical facilities, just as a covertly released biological weapon begins to infect large numbers of the people. Imagine several different infrastructure nodes shutting off at once, such as a power plant in Seattle, a dam in Colorado, air traffic control at Chicago-O’Hare, and other nodes. Would the incidents be labeled as an act of terrorism or seen as a set of unfortunate coincidences? Even if recognized as a cyber-assault, could that assault be traced back to a perpetrator? The potential impact of any of these scenarios is almost incalculable. As Caleb A. Pringle reports, “the likelihood of an electronic Pearl Harbor is real. It is unlikely to happen tomorrow but needs to be prepared for today.”⁴³

⁴¹ Paul Shukovsky, “High-Tech Group Keeps Eye Out For Cyber-Threats,” *Seattle Post-Intelligencer*, January 20, 1998, sec. B, p. 1.

⁴² Michael Kirland. “Nations gird for possible cyber-war.” *United Press International*, February 25, 1999, nexis.

⁴³ Caleb A. Pringle, “Terrorist Organizations’ Use of Information Age Capabilities,” *Defense & Foreign Affairs Strategic Policy* (January 1999): 9-15.

The argument that the threat is overblown, since nothing horrendously bad has happened thus far, is myopic. In truth, while there has not been a cyber version of the Pearl Harbor attack, but there have been many lesser attacks. Multiple attacks on private operators and the spread of viruses such as Melissa and the "I LOVE YOU" virus, which actually infected computers at several federal agencies, are but a few examples of this problem.⁴⁴ Since the creation of the CERT at Carnegie Mellon, funded by the Department of Defense, the center has dealt with more than 15,000 incidents of cyber-security problems, or about 35 calls a day, every day.⁴⁵ Moreover, advances in computer and other information technology occur on an almost daily basis. It is also possible that with the changing of the guard at the top of many terrorist organizations, a new generation of terrorists more familiar with information technology and computers will come to the forefront.

The control of many critical infrastructure nodes by private operators substantially increases the degree of difficulty in ensuring protection. Many private operators, fearing excessive regulations, dislike the prospect of government intervention into private business matters. Americans do not want the government to have access to their filing cabinets or internal means of communication. However, these private operators, in areas such as energy, finance, transportation, and telecommunications, are the backbone of the American economy. An attack on privately held infrastructure, especially one that disabled the ability of that corporation to restore services quickly, could be devastating. With 95 percent of DOD's telecommunications moving over civilian unclassified lines and increasingly more of its combat support services "outsourced" to civilian firms, America's first line of defense may well be corporate information officers or security personnel.

Current regulations also hamper effective private responses to information terrorism. Companies are instructed to design their systems in a fashion that prevents terrorism, a form of passive defense. Active defense, that would seek the source of an infrastructure breach in order to counter-attack, is not authorized for firms in the private sector. Attacks on private infrastructure (and the public sector) are likely to increase. Therefore, without increased public-private cooperation in the area of critical infrastructure protection, both the ability to defend critical infrastructure nodes and the ability to restore the functioning of those nodes in the event of a crisis will be severely undermined.⁴⁶

⁴⁴ Joel C. Willemsen, "Computer Security; Critical Federal Operations and Assets Remain at Risk- GAO Testimony: GAO/T-AIMD-00-314," September 11, 2000, <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai00314t.pdf&directory=/diskb/wais/data/gao> (Accessed December 2000).

⁴⁵ Richard Pethia, "Hearing of the Technology Subcommittee of the House Science Committee Subject: The Melissa Virus," *Federal News Service* (April 15, 1999): nexis.

⁴⁶ Roger C. Molander, "Protecting the Information Infrastructure: A National and International Perspective," *Federal News Service* (July 26, 2000): nexis.

The global networking of computers and information systems makes isolating and protecting key information nodes increasingly difficult. In a world where rapid communications between organizations is crucial to economic and policy interactions, taking all critical infrastructure nodes 'off-line' is not a feasible solution.

Further, the same developments that have increasingly made DOD and other federal agency computer systems interoperable create windows of opportunities for cyber-terrorists. A 1995 DOD self-test of computer security included 38,000 attacks, 65 percent of which were successful and 63 percent of which went undetected. While security at the federal level has improved when compared with 1995 statistics, the ability of potential cyber-terrorists to infiltrate government information systems has improved as well. A recent GAO report prepared for the House Government Management, Information, and Technology Subcommittee noted that on computer security "overall, the government earned an average grade of 'D-.' More than one-quarter of the 24 major federal agencies received a failing 'F.'" It is cold comfort that the Pentagon received a relatively high grade of D+!⁴⁷

The enormous consequences of a coordinated, multi-faceted attack on federal information systems and private operators through cyber or more traditional means (such as explosives, for example)⁴⁸ mandate a continued examination and improvement of homeland defense capabilities. While the cyber threat is most likely one of mass disruption and not mass destruction, attacks on critical infrastructure may also move into that latter category, especially if delivered in tandem with more traditional attacks. Given the problem of attribution --- discovering and identifying perpetrators --- cyber-attacks could be the weapon of choice for the next generation of terrorists. An ounce of prevention might prevent a ton of damage.

Conclusions on threats to homeland security

While Homeland defense is not a new mission, the end of the Cold War, the emergence of the U.S. as the sole superpower, and the onset of the information age have spawned a set of new or at least novel threats. These threats have appeared in the form of missile proliferation in hostile states, the emergence of CBRN terrorism, and a variety of threats to the nation's critical information and economic infrastructure.

⁴⁷ Joel C. Willemsen, "Computer Security; Critical Federal Operations and Assets Remain at Risk- GAO Testimony: GAO/T-AIMD-00-314," September 11, 2000, <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai00314t.pdf&directory=/diskb/wais/data/gao> (Accessed December 2000).

⁴⁸ Adding to the dangers of a terrorist attack are the increasing capabilities of terrorists with regard to conventional weapons. The information age has made the rapid dissemination of effective terrorist tactics, including actual conventional weapons plans, extremely easy. Gavin Cameron, "WMD Terrorism in the United States: The Threat and Possible Countermeasures," *The Nonproliferation Review* (Spring 2000): 162-179.

Each of these threats is complex and in many ways unique. None of them replace old threats. New national strategies will have to deal with a wide range of foreign threats, as well as these apparently new threats to the homeland. As noted above, planning for homeland defense will require a wide range of actors, including state and local governments and elements of the private sector.

All of these threats are highly unpredictable. Indeed, the threat of mass destruction inherent in a missile attack or CBRN terrorism --- especially in the mid- to long-term future --- is such that, if one or the other occurred, it could literally change the course of U.S. history. The effects of either of these attacks on contemporary foreign and domestic policy would be profound.

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

The material that follows will suggest that in the latter half of the 1990s the nation has made significant progress on many issues of homeland defense, but that it still must dramatically improve policy, programs, and organization for homeland defense to ensure security in the future.

The U.S. Response to New Threats to the U.S. Homeland

Meeting the Missile Threat

Missile defense will remain a heated issue well into the next decade. Advocates of missile defenses have viewed missile defenses as a way to protect the U.S. homeland, U.S. troops, and U.S. allies from dangerous missile threats, first from the Soviet Union, and more recently from states such as Iran, Iraq, and North Korea, and potentially China. Critics have feared that missile defense deployment would be destabilizing and create incentives for short-term preemption by targeted states that fear losing their second-strike capabilities. Others were and are still concerned that missile defenses will cause an offensive arms race with Russia and China. The fate of the 1972 ABM Treaty also remains a concern for Russia watchers and traditional arms control advocates. In all, clashing perspectives over the desirability and effectiveness of missile defense has made the issue one of our premier political footballs.

Decades past, the impetus for missile defense was held back by the Strategic Arms Limitation Talks (SALT I) agreement signed by the United States and the Soviet Union in 1972. SALT I included a separate agreement known as the Anti-Ballistic Missile Treaty (ABM), which severely limited the missile defenses for each side. Under the treaty, each side was only allowed a single site from which to launch defensive missiles, and the number of interceptors were limited to 100 per country.

For the next decade, the ABM regime was not seriously challenged although there were concerns over significant Soviet treaty violations.⁴⁹ In 1983, the push for missile defense accelerated once again. President Reagan, seeking a way out of the mutually assured destruction (MAD), sought to shield the United States from missile attacks. He envisioned a space-based system that would shoot down incoming ballistic missile warheads, thus ensuring American security and ending the tyranny of mutually assured destruction. His proposal, the Strategic Defense Initiative (SDI) was derisively labelled 'Star Wars' by its opponents. It sparked a decade long political battle in which billions of dollars were spent on research and development of defensive systems.

With the drawing down of the Cold War, Reagan's successor, George Bush, reformed the missile defense development effort. Bush's missile defense program was titled Global Protection Against Limited Strikes (GPALS). The theory behind GPALS was that upon detection of a launch, space-based interceptors would shoot down the ICBM.

The Persian Gulf War in 1991 significantly changed the missile defense equation. In response to the threat posed to U.S. troops, Saudi Arabia, and Israel by Saddam Hussein's SCUD missiles, modified Patriot anti-aircraft batteries were sent to the Middle East. Originally designed as an air defense system, the modified PAC-2 system became famous through videos and other footage that apparently showed SCUDs being shot down by American interceptors.

After the Gulf War, Theodore Postol from the Massachusetts Institute of Technology (MIT) alleged that the Patriot had not even hit a single target; SCUD failures, he proposed, were primarily due to faulty internal mechanisms, not missile defenses.⁵⁰ While some of his allegations were verified, the focus of missile defense development expanded from merely NMD to both NMD and theater missile defense (TMD).

When the Clinton Administration took office, it drastically reduced the funding available for NMD research, preferring to focus on TMD development. Clinton's actions cut short burgeoning NMD development. According to one analyst, the U.S. could have

⁴⁹ Chief among concerns over Soviet treaty was their construction in the 1980s of a prohibited radar complex at Krasnoyarsk in Siberia. On the related issue of treaty futures, some US lawyers have creatively argued that the ABM Treaty passed out of existence with the passing of the Soviet Union. Woolsey 6-2000 National Review

⁵⁰ Theodore Postol, "Postol/Lewis Review of Army's Study on Patriot Effectiveness," September 8, 1992, www.fas.org/spp/starwars/docops/pl920908.htm, (Accessed October 2000).

deployed an NMD system with ground-based radars and interceptors in 1996, but the Clinton administration slashed funding for the program.⁵¹

In line with its policy of cultivating strong relations with Russia, the Clinton administration feared alienating reformers and provoking nationalists and communists with the specter of NMD deployment. Russia remained opposed to any revisions of the treaty. Since the Clinton Administration viewed the treaty as essential to stable relations, it initially opposed giving a high priority to NMD development.

A combination of other factors, however, once again changed the politics behind missile defense. As described above, the tenor of the missile defense debate changed with the release of the Rumsfeld Report and the TapeoDong I launch by North Korea. Following the congressional uproar that ensued in the wake of the TapeoDong launch, thought to confirm the findings of the Rumsfeld Report that there was an increasing risk of a medium term ICBM threat from rogue states, the priority of NMD development was upgraded. Defense Secretary Cohen announced in January 1999 that the administration was changing its focus from research and development (with the ability to deploy three years after a decision to proceed was made) to deployment by 2005, if technologically feasible. Those policy changes became public law when Clinton signed the Republican-supported National Missile Defense Act, which mandated that the President authorize the deployment of a NMD system as soon as it is technically feasible.⁵²

The change in focus on missile defense deployment brought about a revision in the Clinton Administration policy concerning the ABM Treaty. While still insisting that the ABM treaty was critical to national security, Secretary Cohen explicitly recognized that if an effective NMD were to be deployed, some modification of the ABM treaty would be a necessity. Public recognition of the treaty's six-month withdrawal notice became an issue as the Clinton Administration began negotiations with Russia on amending the ABM treaty.⁵³

⁵¹ William R. Graham, "National Missile Defense: Test Failures and Technology Development," *Federal News Service* (September 8, 2000): nexis.

⁵² William Cohen and Lester Lyles, "Ballistic Missile Defense: A Special Defense Department Briefing." *Federal News Service* (January 20, 1999): nexis.; National Missile Defense Act of 1999, Public Law 106-38.

⁵³ William Cohen and Lester Lyles, "Ballistic Missile Defense: A Special Defense Department Briefing." *Federal News Service* (January 20, 1999): nexis. Two substantive changes to the ABM treaty have already been negotiated, an expansion to include the other former nuclear states of the Soviet Union (besides Russia- which was considered the successor state to the Soviet Union), and a demarcation between TMD and NMD. Neither has been submitted to the United States Senate for its consent and approval. See Dan Goure, *Charting a Path for U.S. Missile Defense: Technical and Policy Issues* (New York: The CSIS Press, 2000), p. 3.

The Clinton administration proposal for missile defense has been labeled the first level capability or the C1 capability. It established a set of one hundred interceptors, most likely deployed in Alaska, backed up by a single engagement radar in Alaska, as well as a smaller number of upgraded early warning radars in England, and Greenland.⁵⁴

More than a year has passed since the Clinton Administration changed its approach to reflect a higher priority on National Missile Defense. While theater missile defense programs such as THAAD have since demonstrated technical competence after years of failure, Clinton's proposed NMD system, has never had a successful full-scale test. The Ground Based Interceptor (GBI), defined as the centerpiece of Clinton's system, did have a successful intercept test in November 1999. Also, the battle management system was successfully integrated in a January 2000 test. However, the January 2000 test failed to successfully intercept the target, and a July 2000 test also failed. In the July test, a computer problem caused the kill vehicle to fail to separate from the booster rocket. There have also been many accusations of mismanagement by the two defense contractors involved, Boeing and Raytheon, making it even more difficult to understand the current technical problems.⁵⁵

Missile defense analysts, most prophetically in the Welch Commission Report, have warned that the current missile defense development program risked a "rush to failure." Its testing schedule was far more rapid than a normal weapons development schedule, and it was chronically under funded. Moreover, the inherent difficulty of the GBI task --- attempting to hit a ballistic missile warhead in the downward half of its flight with another missile warhead --- made the attempt to design a deployable system by 2005 overly ambitious. Safe development of new technologies frequently takes a long time, with several full-scale development tests. Not a single full-scale test has yet occurred for NMD. A lack of adequate funding has forced defense contractors to conduct systems tests with outdated equipment, decreasing the 'reality' level of almost every test.⁵⁶

In the wake of the July 2000 test failure, in August 2000 President Clinton decided to delay the decision to begin construction of a National Missile Defense. The decision on the type and timing of missile defense deployment will therefore reside with the next administration.⁵⁷

⁵⁴ Dan Goure, *Charting a Path for U.S. Missile Defense: Technical and Policy Issues* (New York: The CSIS Press, 2000), p. 3.

⁵⁵ Bradley Graham. 1999. "Anti-Ballistic Missile Has 2nd Hit." *The Washington Post*. August 3: A6.; Goure, 6/00: 2.; Bill Gertz. 2000. "Cohen calls failure of missile test minor." *The Washington Times*. July 11: A1.; Roberto Suro. 2000 "2005 Missile Defense Inception is at Risk." *The Washington Post*: August 9: A4.

⁵⁶ "Report of the Panel on Reducing Risk in Ballistic Missile Defense Flight Test Programs," February 27, 1998 www.fas.org/spp/starwars/program/welch/welch-1.htm (accessed October 2000).

⁵⁷ Eric Schmitt, "Clinton's Missile Defense: The Overview; President decides to put off work on Missile Shield," *The New York Times*, September 2, 2000, sec. A, p. 1.

Many other conceptual difficulties in the Clinton missile defense plan also made it unlikely to succeed. First, the deployment of the key radar in Alaska made the system able to intercept, at best, missiles coming from only one place, East Asia. In a threat environment where Iran and Iraq are key concerns, the utility of such a system would be severely limited. Second, the limited number of interceptors in the Clinton proposal made it highly susceptible to being overwhelmed. An adversary with many ballistic missiles could easily overwhelm the number of available interceptors. Third, while there is a vigorous debate over the possibility of countermeasures on the ballistic missile of rogue states, the risk of countermeasures certainly mandates designing a missile defense interceptor that can distinguish between the warhead and other objects.

Key in the Clinton administration's plans is a space-based infrared system (SBIRS). However, SBIRS Low will not be in orbit until 2006, with a full-scale system not in place until 2010, leaving the missile defense system dangerously susceptible. As Dan Gouré argued,

The sensor problem is the most significant weakness in the current proposed NMD architecture. . . [F]uture threats will deploy penetration aids to defeat simple sensors. An effective NMD system needs maximum exploitation of information. It requires global coverage and a high-resolution discrimination capability. This means both more and better ground-based radars and, inevitably, the use of space-based sensors. An NMD system cannot be effective and still adhere to existing limitations and compliance standards."⁵⁸

Fourth, ABM treaty constraints inherently limit the proposed NMD system. Some would argue that some defenses are better than no defenses. However, given the risk of global resistance to a NMD and the importance of having a higher degree of confidence, it is important to consider the impact of the ABM treaty on the ability of the United States to deploy effective defenses. The current architecture, bound by ABM constraints, will not be effective.⁵⁹

Fifth, the current proposed NMD architecture, even if it is able to intercept ICBMs, offers no capabilities against cruise missiles or shorter-range ballistic missiles. One likely reaction of states of concern to a NMD would be to reconsider the mechanisms by which they threaten the U.S. Such a delivery shift makes it imperative that the NMD can effectively defeat all types of missile threats.

Therefore, while the current decision to delay the deployment of NMD makes it unlikely that a workable system will be in place before the target date of 2005, it may have

⁵⁸ Dan Gouré, *Charting a Path for U.S. Missile Defense: Technical and Policy Issues* (New York: The CSIS Press, 2000), p. 10

⁵⁹ *Ibid.*, p. 9.

prevented the deployment of a limited system that would have had a high probability of failure. Further research and development on the most cost effective and comprehensive form of missile defense that can be technologically feasible in the short to medium term is clearly an essential element of any homeland defense initiative.

Meeting the Threat of CBRN Terrorism

Before the latest wave of terrorism, the U.S. government saw the potential for CBRN-related problems in former Soviet Union and began to work with the local authorities to help them destroy the Soviet arsenal. Through the Nunn-Lugar Threat Reduction Act of 1993, the U.S. to date has helped destroy 407 ballistic missiles, 365 ballistic missile silos, 67 bombers, 17 strategic missile submarines, 144 submarine launched ballistic missiles (SLBM), 256 SLBM launchers, as well as deactivating 5,014 nuclear warheads. This is less than a third of the total slated for deactivation or destruction under Nunn-Lugar, one of our most important threat prevention policies. The U.S. and FSU are also initiating measures to begin the demilitarization of the Soviet chemical arsenal.⁶⁰

After the devastating attack on New York's World Trade Center in 1993, the sarin attack in the Tokyo subway system, and the terrorist attack on the Murrah building in Oklahoma City, both of which took place in 1995, the federal government accelerated its effort to combat terrorism. In June 1995, the President signed Presidential Decision Directive 39 (PDD 39) which designated the FBI as the lead federal organization for crisis management, which includes efforts to prevent or stop an attack, arrest terrorists, and gather evidence for criminal prosecution. It also designated the Federal Emergency Management Agency (FEMA) as the federal lead for consequence management of mass casualty terrorist attacks. Consequence management refers to measures to protect public health and safety, restore government services, and provide emergency relief. It would include medical assistance, and population evacuation.

While FEMA gets high marks for disaster relief, most observers have found it very slow and uncomfortable with this new post-attack role. One senior official, after noting some recent progress, said: "FEMA has preferred a reactive ... rather than a proactive (i.e., do planning or even prepositioning in advance) approach to consequence management. ...Recent events including the TOPOFF exercise , have underscored the deficiencies of this approach." Another expert dismissed FEMA's view of its principal function as only "being a cash machine for natural disasters."⁶¹ DOD and DOJ have taken up much of the slack for FEMA's hesitancy. Overseas, by design, the State Department had the federal lead on both of these functions.

In a related area, since 1994, the CIA and FBI have jointly run a National Counterintelligence Center, as well as a joint counterterrorism effort. In the near future,

⁶⁰ Statistics as of October 17, 2000, as provided by the DOD's Threat Reduction Agency.

⁶¹ Experts made these remarks to Joseph Collins of CSIS in October 2000, and asked to remain anonymous.

there will soon be a National Counterintelligence chief to coordinate national efforts and run an interagency council with high level defense, intelligence and law enforcement presence.⁶²

To help coordinate these burgeoning, multi-agency efforts, the President signed PDD 62 in 1998 which established --- resident on the National Security Council Staff--- a National Coordinator for Security, Critical Infrastructure, and Counterterrorism. The National Coordinator is Richard Clarke. He and his staff of about a dozen people coordinate these policies at the highest levels and oversee three Interagency Senior Management Groups, one for WMD Preparedness, another for Counterterrorism, and a final one for Critical Infrastructure Protection. These 3 senior groups have over a dozen subgroups to tackle individual issues in their purview. In addition to managing the interagency process, the National Coordinator advises on budget issues and prepares the annual Security Preparedness Report.

In supporting legislation in 1966, the Congress passed the Defense Against WMD Act (commonly known as the Nunn-Lugar-Domenici Act, hereafter the NLD Act) which put the Department of Defense in the lead to train and advise federal, state, and local agencies regarding emergency response to CBRN terrorism or related issues. DOD sponsored teams have conducted training in 120 cities. The responsibility for this program is in the process of being transferred from DOD to the Department of Justice (DOJ), but at the start of the FY 2001, this issue was still unresolved.

To date, since the publication of PDD 39, the GAO estimates that these efforts and associated federal programs have trained over 130,000 state and local emergency responders, which sadly is less than 3 percent of the total.⁶³ One standout effort in this area came from DOJ's takeover of the former Army Chemical Corps facilities at Fort McClellan, Alabama. With significant contractor support, DOJ turned the old Army facility into the Center for Domestic Preparedness (CDP), the only facility in the nation where civilian responders can train in a live-agent environment.⁶⁴

⁶² James Kitfield, "Covert Counterattack," *The National Journal* (September 16, 2000): nexis.

⁶³ Richard Davis, "Combating Terrorism: Federal Agencies' Efforts to Implement National Policy and Strategy- GAO Reports: GAO/NSIAD-97-254," September 2000, www.gao.gov. (Accessed November 2000). An unofficial estimate of the total emergency responder community was prepared by US government experts. It totaled 9 million people. Even if a much more restrictive definition were used and the population was 5 million responders, US efforts have still not exceeded the 3 percent standard.

⁶⁴ Joseph Collins, "Training America's Emergency Responders: A Report on the Dept. of Justice's Center for Domestic Preparedness and the U.S. Public Health Service's Noble Training Center, Ft. McClellan, Anniston, Alabama," July 2000, webu6102.ntx.net/homeland/reports/FirstResponders.html, (Accessed November 2000).

The CDP's Washington-based parent, the DOJ's Office for State and Local Domestic Preparedness Support (OSLDPS) has also done yeoman service in helping state and local emergency responders to acquire equipment, conduct CBRN-related training, acquire technical assistance, and fund major exercises. OSLDPS is currently supervising an effort to help the states develop domestic preparedness strategies to help guide their training and equipment acquisition in the future.

In all, however, the effort to train emergency responders is in its infancy. Not only have few been trained, but emergency responders also need a single doctrinal focal point for manuals and training programs for civilian CBRN terrorism responders. This single point of contact could also be used to manage the exercise "lessons learned" system, noted above.

The NLD Act also tasked the Department of Health and Human Services (DHHS) to stand up medical emergency response teams. Under other legislation, DHHS, through the Veterans Administration, manages stockpiles of medicine and equipment that can be used in response to CBRN terrorist incidents. Approximately "450 tons of antibiotics, antidotes, and medical equipment have been stockpiled in warehouses around the country."⁶⁵ In a similar vein, the U.S. Public Health Service has taken over an unused Army hospital and turned it into a test bed for training hospital staffs to deal with medical effects of CBRN terrorism. The Center for Disease Control in Atlanta also has a very active Bioterrorism Preparedness and Response Program, another adjunct to medical readiness for homeland defense.

The Department of Defense has faced an especially complex challenge on homeland defense issues. On the one hand, it has tremendous assets that can be brought to bear on homeland defense issues, but on the other hand, its mission focus is overseas. It is also normally prohibited by law from certain activities --- like gathering intelligence or law enforcement --- inside the United States. Moreover, the American public jealously guards its civil liberties and clearly wants state and local authorities in the lead, whenever possible. Finding an appropriate role for the military is not only a legal issue, it is also one of public and elite opinion on how our federal system should work, especially in a situation that featured mass destruction.⁶⁶ Finally, the Pentagon is also aware of the potential problems associated with domestic operations of any sort. One analyst wrote

⁶⁵ Richard Clarke, *60 Minutes: Interview with Lesley Stahl*. October 22, 2000.

⁶⁶ Most of these legal prohibitions already admit to exceptions that would allow the President *in extremis* to make a broader use of military forces inside the United States. For example, the famous *Posse Comitatus Act* and supporting directives that bar federal troops (but not National Guardsmen working for the governor) from enforcing laws, has had many exceptions to its rule. It is often cited as an excuse for inaction by policy makers who want to keep the military out of the homeland defense field. See Craig Trebilcock, "Posse Comitatus: Has the Posse Outlived its Purpose," April 2000, www.csis.org/homeland/reports/trebilcock.pdf (Accessed November 2000). Also see Fred C. Ikle, *Defending the U.S. Homeland: Strategic and Legal Issues Issues for DOD and the Armed Services* (Washington, D.C.: CSIS Press, January 1999).

that “incidents associated with incidents on the Mexican border and questions concerning the limited involvement [of DOD personnel] in the Waco fiasco illustrate the risks of these types of missions. For this reason, DOD backed off the term “homeland defense” in favor of the more understated “military support to civil authorities (MSCA).”⁶⁷

Overall, DOD has adapted well to its new challenges. While accustomed to being in the lead on national security issues, DOD has adapted its staff and created new organizations to better support the lead federal agencies in both crisis and consequence management. Its efforts emphasize the following principles:

- Public accountability and strict respect for federalism and civil rights;
- Maintenance of a supporting role to the lead federal agency;
- Emphasis on core competencies, such as mobilization and logistics; and
- Use of the Reserve and National Guard units as “forward deployed” units for domestic consequence management.⁶⁸

To coordinate its efforts to combat the effects of terrorism at home, the Secretary of Defense has appointed an Assistant to the Secretary of Defense for Civil Support (ATSD-CS) to advise him and serve as the Department’s point of contact on all issues regarding departmental support in this area. This solution has worked well, but it is an impermanent one. Future administrations should consider assigning this billet to one of its more than 10, confirmable Assistant Secretaries or perhaps to the confirmable Principal Deputy Under Secretary of Defense for Policy.

To coordinate possible large-scale support, DOD established in 1999, under the auspices of Joint Forces Command, Joint Task Force – Civil Support in Norfolk, Virginia. JTF Civil Support, commanded by a National Guard general officer, would be the DOD point organization in providing support to state Governors, FEMA, and the FBI in a complex emergency, other than a natural disaster. Their specific missions include the rapid delivery of DOD forces in support of the lead federal agency, command and control of nearly all DOD forces in the area, and doctrine and planning integration. A holdover from the past, DOD has another organization the Directorate of Military Support (DOMS) that coordinates support for natural disasters and answers to the Secretary of the Army.

The cutting edge of DOD’s day-to-day capability in the field are the soon-to-be 27, uniformed WMD Civil Support Teams. These 22-person, full-time, National Guard

⁶⁷ John Kreul, “The Threat of Terrorism against the U.S. Homeland: What Role Should the Military Play in the Federal Response?,” *A USA National Security Watch* (May 2, 2000): 2.

⁶⁸ Berkowsky briefing to Cilluffo group.

manned elements will assist state and local officials with their ability to make rapid assessments and initial detection of CBRN events. They can also advise local officials on what other federal or National Guard assets can be used to assist them. By 2002, 97 percent of the U.S. population will live within 3 hours drive of one of these teams.

In addition to the CSTs, the Department of Defense maintains a number of specialized units that are also highly useful in combating CBRN terrorism. The Army has a Technical Escort Unit trained in disposing of and moving CBRN and conventional ordnance. The Marine Corps has a 275-man Chemical/ Biological Incident Response Force (CBIRF) for short notice rescue or decontamination missions. The Army and Navy also maintain special medical research units --- like the U.S. Army Medical Research Institute of Infectious Diseases --- that conduct research on chemical and biological defense issues. The Army, in particular, especially in its reserve components, has many mobile field hospitals, mortuary, transportation, military police and medical supply units that can be called upon to assist the appropriate federal, state, or local authorities. For example, the Air Force reserve components alone have 25 patient decontamination units, nationwide. The Army reserve components have 38 chemical and biological defense units nationwide. Together the DOD, VA, and DHHS also control 45,000 stateside hospital beds, not including the mobile assets in the Army and Air Force reserve. While these multipurpose units receive little publicity, they represent the real strengths that DOD can bring to solving consequence management problems.

The capabilities of our Armed Forces also include the assets of the Coast Guard. While the Coast Guard is part of the Department of Transportation, it contributes mightily to homeland defense by securing our maritime frontiers and supervising security in our ports. Uniformed Coast Guard personnel are also not subject to *posse comitatus* restrictions and regularly interact with law enforcement, customs, and border patrol personnel. In all, the Coast Guard provides a unique set of links among the nation's maritime assets, its military, and its law enforcement and state public safety organizations.

In conclusion, in the area of responding to CBRN terrorism, the federal government has made an excellent, even if complex start. In addition to fine tuning roles and missions, it will be necessary is to create an overarching supervisory structure that will be able to harmonize the efforts of the many organizations working this particular problem. This same glaring need exists in the area of responding to the cyber threat and threats to critical infrastructure.

Response to Cyber challenges and threats to critical infrastructure

Despite the enormous risk to national security posed by cyber-attacks and other threats against critical infrastructure, it is only in the last few years that the United States government has even begun to consider the challenge that lies ahead. Executive Order 13010 in 1997 established the President's Commission on Critical Infrastructure Protection (PCCIP). The PCCIP identified five areas integral to critical infrastructure protection:

- Policy Formulation: Designing strategically sound approaches to critical infrastructure protection;
- Assessing Emerging Threats to both public and private operators;
- Prevention and Mitigation: Creating a culture of security where owners and operators recognize the threat and are willing to commit resources for protection;
- Information Sharing and Analysis, and
- Response, Restoration, and Reconstitution: If deterrence fails, marshalling the resources necessary to ensure a rapid reconstitution of damaged critical infrastructures.

The report of the PCCIP noted severe inadequacies in current levels of critical infrastructure protection, especially in the key infrastructure under the control of private industry. This led to Presidential Decision Directive 63 (PDD 63). Recognizing the existence of interlinked computer systems and an increasing capability to attack those systems, PDD 63 directed federal agencies to jump-start protections against cyber threats, with the goal of total cyber security by 2003.⁶⁹ Just as with PDD 62, the directive put Richard Clarke, the first National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, in charge. He and his staff have been working with the Office of Management and Budget to coordinate national efforts to protect critical infrastructures and increase national awareness of the rising threat.⁷⁰

The National Infrastructure Protection Center (NIPC) was set up under the auspices of the FBI to gather information on cyber threats. The NIPC is made up of representatives from the FBI, DOD, Secret Service, DOE, DOT, private sector, and the intelligence community. It is also designed, in the case of an attack, to coordinate the response of the United States and implement pre-designed recovery and reconstitution plans.⁷¹

The Federal Computer Incident Response Capability (FedCIRC) was also bolstered under PDD 63. An OMB official noted that “FedCIRC ... coordinates the cross-government sharing of information regarding common vulnerabilities and works with the FBI, DOD,

⁶⁹ Kenneth M. Mead, “Computer Security within the U.S. Department of Transportation,” *Federal News Service* (September 27, 2000): nexis.

⁷⁰ John T. Spotila, “Computer Security: Cyber Attacks- War Without Borders,” *Federal News Service* (July 2, 2000): nexis.

⁷¹ Office of the White House Press Secretary, “Fact Sheet: Protecting America’s Critical Infrastructures: PDD 63,” May 22, 1998, www.fas.org/irp/offdocs/pdd-63.htm (Accessed November 2000).

and others to assist agencies in responding to computer security incidents.”⁷² Funding levels have been inadequate, forcing the transition of the FedCIRC function to the General Services Administration.

FedCIRC obviously serves an important function; given the disparate levels of technology between agencies and the common information threats faced by many agencies and private operators, coordinating information to create a database of lessons learned is an essential element of homeland defense. However, FedCIRC only focuses on federal agencies, meaning it is too limited to itself coordinate critical infrastructure threat and response information. To fill the information gap, PDD 63 established the Information Sharing and Analysis Center (ISAC) to be led by the National Coordinator and a range of private and public sector individuals. The purpose of the ISAC is the information gathering, analysis and dissemination focused on government-private cooperation and partnerships.

In the Department of Commerce, a Critical Infrastructure Assurance Office (CIAO) was set up to assist federal agencies in becoming resistant to cyber threats and to facilitate cooperation with the private sector. Private sector operators control the vast majority of critical infrastructure nodes, especially in energy, finance, transportation, and telecommunications. Therefore, any defense initiative that does not include an active partnership with the private sector is doomed to fail.

For a variety of reasons, however, both private and public operators are hesitant to cooperate on infrastructure protection. Some federal operators think cooperation with the private sector presents a no-win double bind. Either the government will not share classified information with private operators, meaning a comprehensive exchange cannot occur and cooperation cannot achieve the greatest possible benefits, or the government will be forced to reveal secrets that could compromise national security.⁷³

Private operators are equally hesitant to cooperate with the federal government. Private corporations fear that if they share their proprietary information with the federal government, the government will either leak that information, endangering their profits, or use information garnered from the private sector to justify new regulatory schemes. The latter concern is particularly acute.⁷⁴

Private sector operators were identified by PDD 63 as possible voluntary partners for infrastructure protection initiatives. The public sector must be able to take advantage of the multiplicity of innovations in cyber security ongoing in the private sector. Similarly,

⁷² John T. Spotila, “Computer Security: Cyber Attacks- War Without Borders,” *Federal News Service* (July 2, 2000): nexis.

⁷³ Roger C. Molander, “Protecting the Information Infrastructure: A National and International Perspective,” *Federal News Service* (July 26, 2000): nexis..

⁷⁴ *Ibid.*, nexis.

the incredible potential resources that can be marshaled by the government make governmental responses to substantive attacks potentially more effective than purely private solutions.⁷⁵

State and local officials will almost always be the first line of defense against cyber threats and attacks on critical infrastructure. Thus, federal cooperation with them will be an essential part of an effective national protection policy. In many cases, only local governments will have the institutional knowledge necessary to develop effective protection plans for critical infrastructure and get those facilities back on line if disaster strikes. PDD 63 directs the federal government to create partnerships that integrate local and state concerns into a national framework. The National Infrastructure Assurance Council (NIAC), comprised of private sector leaders and state and local government representatives was formed expressly to ensure that state and local concerns were heard and understood, so a more effective protective framework could be implemented.⁷⁶

One important regulatory factor addressed by PDD 63 and always in the background of discussions of cyber security is the implication of potential regulations on constitutional rights, especially privacy and search and seizure rights. Agencies are directed under PDD 63 to seek alternatives to direct regulation and design protective systems that preserve individual liberties.⁷⁷ While current regulatory plans do not seem especially intrusive, it is important that continuing efforts to create a secure information environment do not come at the expense of individual rights.

On January 7, 2000, the White House released its National Plan for Information Systems Protection. The program establishes three key objectives; Prepare and Prevent, Detect and Respond, and Build Strong Foundations. The first objective, Prepare and Prevent, focuses on a comprehensive program to identify critical infrastructure assets, develop mechanisms to prevent infrastructure shutdowns in case of attack, and design programs to prevent those attacks from occurring in the first place.

Second, Detect and Respond refers to the active element of homeland defense. The goal of the government is to monitor systems so that attacks can be predicted and quickly and decisively responded to.

⁷⁵ The White House, "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 22, 1998, www.fas.org/irp/offdocs/paper698.htm (accessed November 2000).

⁷⁶ Office of the White House Press Secretary, "Fact Sheet: Protecting America's Critical Infrastructures: PDD 63," May 22, 1998, www.fas.org/irp/offdocs/pdd-63.htm (Accessed November 2000).

⁷⁷ The White House, "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 22, 1998, www.fas.org/irp/offdocs/paper698.htm (accessed November 2000).

Finally, Build Strong Foundations is the catch phrase for the medium to long term research and development to train a generation of information technology specialists, increase popular awareness of information threats, and design programs that will protect privacy and civil liberties while also ensuring successful protection occurs.⁷⁸

In the congressional arena, efforts to improve critical infrastructure protection have foundered in a continuing wave of partisanship. The proposed Cyber Security Information Act of 2000, supported by President Clinton, was last debated in June, and has not even been voted out of committee. The act would have recognized the enormous risks to critical infrastructure from cyber attacks and supported the National Plan for Information Systems Protection.⁷⁹

Some positive actions have unquestionably been taken in the last year. In February 2000, the new OMB policy for information technology acquisition was released. Each agency, when purchasing or developing new information technology equipment, will be required to develop and implement a plan to cyber-safe that technology before the OMB authorizes the release of funds to the agency.⁸⁰ Mechanisms that ensure new technologies are cyber-safe are essential to developing a system of protection. However, the limited charter of the OMB prevents their assumption of a bigger role in critical infrastructure protection. While they can manipulate the distribution of funds to encourage awareness of cyber dangers, it is difficult for the OMB to act in a way that increases the safety of existing infrastructures or coordinates inter-agency actions.

John Gilligan, the Chief Information Officer (CIO) of the United States Department of Energy and co-chair of the inter-agency CIO Committee on Security, Privacy, and Critical Infrastructure Protection, argues that federal agencies have taken great strides in the last year to improve their ability to resist cyber-threats. Specifically, Gilligan argues that in the last year:

The Council has sponsored a web-based repository for sharing security best practices. We have developed sample security policies for use by agencies for intrusion reporting and procuring security products....The Council is also leading efforts to establish a government-wide encryption infrastructure using public key technology that will ensure confidentiality of government information as well as support digital signatures and strong authentication.⁸¹

⁷⁸ The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0 An Invitation to Dialogue* (January 7, 2000), p. xi.

⁷⁹ Cyber Security Information Act of 2000. Bill Tracking Report: H.R. 4246: nexis.

⁸⁰ John T. Spotila, "Computer Security: Cyber Attacks- War Without Borders," *Federal News Service* (July 2, 2000): nexis.

⁸¹ John M. Gilligan, "Computer Security: How Vulnerable are Federal Computers," *Federal News Service* (September 11, 2000): nexis.

In the area of information sharing, the Council has established a web site specifically devoted to distributing lessons learned regarding cyber security. The site includes various agency policies, briefings, and lists of potential security programs. The next step in information cooperation for the Council is establishing a repository of 'best practices' by each agency, allowing agencies to learn from each other how to best combat information insecurities.⁸²

Concurrently with the release of PDD 63, internal and external evaluations began at every federal agency to determine their vulnerability to cyber threats. Initial reviews demonstrated serious shortcomings, and agencies began to change their policies to reflect recognition of growing cyber dangers. The most recent General Accounting Office (GAO) analysis of federal computer security, released in September 2000, demonstrates that all twenty-four federal agencies have significant problems in the area of cyber security. Each agency examined had "significant computer security weaknesses."⁸³ In fact, the federal government as a whole was given a D-, with seven agencies receiving a failing grade. In a series of related corrective measures, the DOD created at U.S. Space Command two standing task forces, one for defense of the computer network and the other for offensive measures.

While it is possible that increasing examples of information security problems reported by the GAO are due to the broader nature of the study than previous evaluations, cyber-security at the federal level is clearly problematic. The GAO found inadequate protections existing at almost every level of the computer security process. Security resource management and planning was frequently insufficient. New initiatives are clearly necessary to coordinate the efforts of various agencies and draw the expertise of the private sphere into the ongoing efforts of public agencies.⁸⁴

A skilled worker shortage also imperils critical infrastructure protection, especially in the public sector. While Silicon Valley has no problem attracting skilled programmers, the growing private sector information market has drained the pool of workers for federal information security. The GAO reported in July that at many federal agencies they

⁸² John M. Gilligan, "Computer Security: How Vulnerable are Federal Computers," *Federal News Service* (September 11, 2000): nexis.

⁸³ Joel C. Willemsen, "Computer Security; Critical Federal Operations and Assets Remain at Risk- GAO Testimony: GAO/T-AIMD-00-314," September 11, 2000, <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai00314t.pdf&directory=/diskb/wais/data/gao> (Accessed December 2000).

⁸⁴ *Ibid*, <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai00314t.pdf&directory=/diskb/wais/data/gao> (Accessed December 2000).

observed, there were not enough qualified workers to develop and implement a plan for infrastructure protection of information assets. In response to this problem, the Congress appropriated 11.2 million dollars in FY 2001 for the National Science Foundation to use as scholarship money for U.S. students pursuing degrees in computer security. In exchange for the scholarship, the recipients upon graduation will go to work for the federal government.

Until each federal agency has the knowledge and ability to assess its own vulnerability and develop an effective plan to safeguard its computer network and the parts of infrastructure that it is responsible for, true self-sufficiency in defense cannot be achieved. Nurturing the institutional knowledge for self-assessment should be a high priority for each agency in the federal government.⁸⁵

Also, the spate of reports and publicity concerning information security could create a false sense of security as federal agencies rush to plug cyber holes in their information infrastructures and private operators begin to cooperate with the federal government. However, as Roger Molander of the RAND Corporation noted in July, it is important recognize that there are still broad areas of unknowns in the infrastructure protection equation, making a single, one size fits all solution unlikely to succeed:

It should be clear from the above discussion that there is no simple "silver bullet" for enhancing U.S. or global critical information infrastructure protection, or even more broadly, information infrastructure-based critical infrastructures such as electric power. It is still quite unclear how vulnerable key sectors are, how widespread the effects of a major strategic attack might be, and how effective various responses to that attack - such as work-arounds and reconstitution - might be. It is also unclear how well an adversary (e.g., a nation-state or major terrorist group) could marshal the necessary knowledge and resources to mount a strategic-level attack, especially without its preparations and probes being detected.⁸⁶

The threat to critical infrastructure assets, especially information assets, in the short to medium-term requires a stronger set of protective measures than the measures that currently exist. Recent plans fail to create a comprehensive system for monitoring and distributing information and will never be able to ensure security as long as federal agencies remained understaffed in the information arena. Additionally, while PDD 63 sets out public-private cooperation as a key goal, both because the private sector is an

⁸⁵ John T. Spotila, "Computer Security: Cyber Attacks- War Without Borders," *Federal News Service* (July 2, 2000): nexis.

⁸⁶ Roger C. Molander, "Protecting the Information Infrastructure: A National and International Perspective," *Federal News Service* (July 26, 2000): nexis.

important repository of cyber security information and because the private sector controls many critical infrastructure nodes, current efforts have failed to jump-start that cooperation. New incentives and plans are necessary to ensure critical infrastructure security.

Programmatic and Budgetary Response.

From 1998 to FY 2001, funding for homeland defense-related activities increased 45 percent. In FY 2001, the OMB reported that the President's budget request contained 12.9 billion dollars, including 8.3 billion dollars for combating terrorism, up 55 percent since FY 1998. The latest budget request also included 1.6 billion dollars for combating WMD, up 240 percent since FY 1998. The FY 01 request also included over 2 billion for critical infrastructure protection, up 78 percent since 1998.⁸⁷

Organizationally, the Department of Defense is slated to receive about 51 percent of these funds, and the Department of State, with its huge bills for embassy security comes second. Law enforcement went from 41 percent of the total in 1998 to 32 percent in FY 2001. CSIS analysts estimate that the main increases in overall federal effort took place in physical security, preparing for and responding to terrorist acts, and in research and development. Not all of these expenditures are strictly concerned with defending the homeland. For example, 79 percent of DOD expenditures on counterterrorism are for protecting U.S. forces and facilities overseas.⁸⁸ Even the programs that are obviously vitally concerned with homeland defense are disconnected and impossible to evaluate. In all, there are many budget lines, few long-term programs, and absolutely no uniformity in how each department accounts for its proposed expenditures. Even the much touted consequence management work of the DOD is hard to analyze. One analyst noted:

DOD's total consequence management effort is now [FY 2001] only \$265 million and is less than 6 percent of its total effort.... The data that DOD provides make it impossible to understand what is really happening...⁸⁹

⁸⁷ Anthony Cordesman, "U.S. Government Efforts to Create a Homeland Defense Capability: A Program and Budget Overview of Federal Spending on Counterterrorism and WMD," July 13, 2000, webu6102.ntx.net/homeland/reports/budgetoverview.pdf (Accessed November 2000).

⁸⁸ Anthony Cordesman, "Department of Defense Programs: Countering Asymmetric, Indirect, Covert, Terrorist, and Extremist Attacks with Weapons of Mass Destruction," November 3, 2000, webu6102.ntx.net/homeland/reports/dodcountasym.pdf (Accessed November 2000).

⁸⁹ *Ibid.*, p. 11.

While OMB has improved the transparency of the budget process, there is only limited coordination, little long-term planning, inadequate programmatic development, and a near total lack of net assessments. Annual budgets are in search of long term programs, which, in turn, are in search of the national plans that would give them objectives and priorities. We have only begun to understand all that we are doing and not doing for homeland defense. We do not have adequate threat estimates, technical assessments, or net assessments to guide our policy-makers. In the words of CSIS's Anthony Cordesman, the current holder of CSIS's Burke Chair of Strategy:

These rapid changes in the way the Federal government deals with terrorism have been accompanied by an even more rapid growth in federal spending, which [in turn] has created major problems in tracking and assessing the Federal effort to deal with terrorism. The reporting on key programs contributing to homeland defense is currently a definitional and statistical nightmare, and is filled with conflicting bureaucratic rivalries and priorities.⁹⁰

We have only begun to understand all that we are doing and not doing for homeland defense. While some other studies have rightly found duplication of effort,⁹¹ this problem stands second to the inadequacy of our efforts. A more detailed, coordinated planning, programming, and budgeting effort throughout the government would clearly be in the national interest.

A Progress Report: Exercise TOPOFF, the Denver Experience

Three congressionally-mandated emergency exercises for top officials, codenamed TOPOFF, provide an excellent example of the difficulties of putting the many U.S. homeland defense programs into action. Planners created a chemical scenario in Portsmouth, New Hampshire, and a radiological scenario in Washington, DC. The third exercise, a Spring 2000 event in Denver was perhaps the most challenging. It involved a CBRN terrorism incident centering on the release of plague bacilli at a performing arts center. Denver was chosen both for its size (a population of about 500,000) and its recent participation in federally-funded training.

The TOPOFF exercise in Denver was able to evaluate the readiness of the nation's public health system and infrastructure to deal with chemical, biological, or radiological terrorist attacks. It allowed the selected participants to deal with the resulting virtual emergency for four-days with no additional information other than the on-going reports of the epidemic's toll and effects. Some key aspects of a real crisis --- actual media play and potential panic among the population, for example --- were unable to be tested during the exercise.

⁹⁰ Ibid., p. 3.

⁹¹ See Amy Smithson and Leslie-Anne Levy, *Ataxia: The Chemical and Biological Terrorism Threat and US Response*, (Washington, DC: Stimson Center, 2000): xiv-xix.

The exercise was particularly valuable because it included a simulation of mass casualties. Six days after simulated dispersion in Denver, there were 3,700 cases of plague and nearly a thousand simulated deaths. Because of the covert nature of the incident and the nature of modern transportation systems, this single-city incident quickly became an international epidemic. Hospitals were overwhelmed, local medical supplies were inadequate, distribution systems for emergency supplies were uncertain, and medical and emergency managers quickly became exhausted. Coordination and communication were somewhat chaotic.

While the exercise was considered a technical success, it did expose a serious number of weaknesses that are emblematic of the defects in our capabilities to deal with CBRN terrorism. A report by the JHU Center for Civilian Biodefense Studies concluded --- based on interviews with senior exercise participants --- that this simulation of a relatively unsophisticated, single-point attack demonstrated that:

...the systems and resources now in place would be hard-pressed to successfully manage a bioweapons attack such as that portrayed in TOPOFF. The exercise was also instructive in illuminating problematic issues of leadership and decision-making; the difficulties of prioritization and distribution of scarce resources; the crisis that contagious epidemics would cause in health care facilities; and the critical need to formulate sound principles of disease containment.⁹²

On the issue of disease containment, JHU analysts noted a special need to improve our thinking about patient isolation, travel advisories, curfews, airport closures, and quarantines. Decisions about all of these issues must solve on-the-scene problems, but their effects must also be weighed against civil rights and personal liberties.

On a related issue, we have yet to develop a well-accepted basis for even predicting the effects of CBRN device usage. There are varying assumptions, data bases, and predictive models that guide crisis management. A senior federal official made this complaint that went beyond the recent TOPOFF exercises:

When an incident occurs, each “team” may show up with its own hazmat/weapons effects modeling equipment. EPA may use one approach, DOD assets another, and first responders an entirely different one. With a variety of potentially competing models, which one will become the basis for determining things like evacuation plans, areas of contamination, estimates of population affected, likely direction of the plume, etc.? Presumably this is the kind of issue that should be worked out well in advance of an actual crisis, rather than waiting for deconfliction on the ground in the midst of chaos.⁹³

⁹² Thomas Inglesby, Rita Grossman, and Tara O’Toole, “A Plague on Your City: Observations from TOPOFF,” *Biodefense Quarterly*, September 2000, p. 9.

⁹³ Correspondence between a high federal government official, a recognized expert in consequence management, and Joseph Collins of CSIS, October 25, 2000.

The TOPOFF exercises and many other aspects of homeland defense covered in this report, all demonstrate that we have miles to go before we are ready to deal with even a simple, single-point incident of CBRN terrorism. In the future, improved and well-publicized preparedness will also prove to be our best deterrent to such tragedies taking place on American soil.

Conclusions

U.S. homeland defense efforts are like the proverbial glass that is both half full and half empty. Compared to the US posture five years ago in every area --- missile defense, the protection of critical infrastructure, and defense against CBRN terrorism --- there has been measurable progress. Compared to where we need to be, however, much work needs to be done. Not only are programmatic and policy fixes in order, but many aspects of U.S. homeland defense policy need to be reconsidered, and others need a plan to tie them together. This kind of defense planning is hard enough to do when it primarily entails coordinating the responsibilities of five disciplined, uniformed military services, but it is far more complex when it becomes widely interagency on the federal level, and also includes state, local, and private sector concerns.

Among the most important findings of this report are:

- There is a priority need to reevaluate our national missile defense goals, programs, and testing program.
- The most obvious need in the area of homeland defense is for a national plan and a comprehensive, multi-year program. To write and enforce such a plan, however, will require major organizational changes in the federal government and new organizations to spur state-federal dialogue.
- The homeland defense effort must fit into the U.S. system of laws and concept of federalism. At the same time, given the possibility of mass destruction and mass disruption, we need to explore areas where new legal authorities may be necessary.
- It will be increasingly important to assess where policies and programs for homeland defense fit in terms of national priorities. Conceptually, homeland defense tasks do not replace current tasks for deterrence, engagement, presence, and power projection, but they are related. A failure in any of those tasks may well increase risks to the homeland. Likewise, a failure to build appropriate homeland defense capabilities might encourage an attack that could jeopardize a deployment for an overseas operation.
- U.S. homeland defense efforts have been reactive, disjointed, and focused on post facto consequence management. In addition to the critically important issues of crisis and consequence management, we must see homeland defense in terms of preventing, deterring, disrupting, and attributing attacks on the homeland.

- The U.S. intelligence apparatus is geared primarily to assess major, foreign threats in the form of overt attacks on the United States and its allies. While there have been significant improvements in intelligence work on terrorist issues, the U.S. must continue to redirect efforts at gaining, processing, and analyzing intelligence across the entire spectrum of terrorist and cyber threat actions from early planning through execution to attribution of the event.
- In a similar vein, we need to sharpen our knowledge of the effects of the evolving cyber threat and CBRN weapons. The US urgently requires a net technical assessment that looks not only at threats but also at US capabilities to meet them.
- There is a critical need to train more people to prepare for and deal with cyber security and homeland defense issues.
- There is a critical need in the field of cyber security for the government to improve cooperation with the private sector, create incentives for the private sector to better protect its own systems, and improve its own credibility by improving its internal operations.

Recommendations

Missile Defense

The next Administration must develop a new plan for missile defense. The threat assessment needs recalibration, and current missile defense plans may not make sense in terms of the technological possibilities. Future air and cruise missile defenses must also be taken into account. Moreover, the next Administration will also have to improve coordination with our allies, come to some final agreement (or disagreement) with the Russians over the ABM Treaty, and link National Missile Defense (NMD) to an overall approach to arms control and efforts to reshape strategic offensive forces. There has been much useful research and development in the past decade. Now we must develop an architecture that reflects new strategic requirements and encompasses the threat, the infrastructure, and the technology.⁹⁴

CBRN and Cyber Threats: Organize, then Plan

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

⁹⁴ For a detailed outline of a new plan for missile defense, see Daniel Goure, *Defense of the U.S. Homeland against Strategic Attack*, a forthcoming CSIS report.

provisions for consequence management against a foreign missile strike on the territory of the United States.

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

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

Among his or her principal responsibilities, the VP would chair a new National Emergency Planning Council that includes representatives from all departments, agencies, states and territories. This Council would be the senior body for federal and state coordination on matters relating to critical infrastructure protection or response to terrorist incidents. Private sector organizations would be invited to participate on issues related to critical infrastructure protection. The Council would meet twice yearly, once at the principal level (VP, Governors, CEO), once at the subordinate level. The National Coordinator would be the Vice Chair of the Council.

Under this reorganization, there would be no changes to the principal State, DOJ, and FEMA responsibilities for crisis management and consequence management. FBI and CIA counterterrorist coordination efforts would remain unchanged. Neither the National Coordinator nor the Vice President would supervise on-going CT or CI operations. The National Infrastructure Protection Center (NIPC) would remain under FBI auspices, and the Critical Infrastructure Assurance Office (CIAO) would remain at the Department of Commerce.

Some consolidation of offices/functions would take place to support new EPS in the office of the Vice President. The National Defense Preparedness Office (NDPO), a DOJ clearinghouse for domestic preparedness, would be transferred to FEMA. Selected divisions of the Office of State and Local Domestic Preparedness Support, currently in the Office of Justice Programs, would also become a part of FEMA or the Emergency Planning Staff. The EPS and FEMA would also absorb responsibility for running

training programs under the Nunn-Lugar-Domenici Act, that had recently been transferred from Defense to the Department of Justice.

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

The Pentagon would realign offices so that it had one coherent system for civil support to natural disasters and to terrorism, as opposed to the two distinct systems that it has today. The Directorate of Military Support (DOMS) would no longer work for the Secretary of the Army, but instead would be aligned with the Joint Staff and JTF Civil Support. In the next administration, the Assistant to the Secretary of Defense for Civil Support should become a confirmable Assistant or Deputy Under Secretary. When appointed, this official needs to ensure that lines of responsibility within OSD are clarified and that any overlap in ASD RA and ASD SO/LIC functions is corrected.

To foster more effective oversight, a bipartisan congressional Task Force should study ways to improve and simplify the oversight of selected homeland defense tasks. The objective would be for each legislative body to have only one authorization and one appropriations committee for cyber threats, CBRN terrorism, and critical infrastructure protection. The leadership of the House and the Senate should also appoint a minority and majority staff specialist in each of the appropriations and authorization committees to follow all counter-terrorism programs. These staffers can alert Members who are voting on a specific agency's counterterrorism program as to how that program or policy fits into the overall U.S. counterterrorism effort.

Planning for CBRN and Cyber Threats

Among the key, recurring tasks for the VP, the National Coordinator, and the Emergency Planning Staff would be to:

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

- Supervise all aspects of emergency planning and policy development for the federal government.

The Vice President, the National Coordinator, and the EPS should also accomplish the following projects on a priority basis:

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

Early on, the VP and the National Coordinator need to assess our present and future needs against our on-going research efforts and make detailed recommendations to the President and the Congress. While this report has not made a detailed assessment of R&D needs, many experts believe that the USG should foster an acceleration of research in immunology and genetics with the objective of putting improvements in immune responses ahead of the ability to create new and more deadly biological agents.⁹⁵ A net technical assessment is needed on this set of options, as well as on others that include an analysis of potential deployment costs and requirements, countermeasures, and relative costs and benefits.

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

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

As soon as practical, the President should also direct the VP and the DCI to assess our ability to gain, process, analyze, and disseminate intelligence on cyber and terrorism issues. CBRN counterterrorism poses unique challenges to the U.S. Intelligence Community (IC). Terrorist groups are hard to penetrate and less susceptible to technological collection techniques. Continuing to widen the circle of intelligence consumers to include HHS and selected state and local officials will be an important

⁹⁵ Conversation between Joseph Collins, CSIS and Dr. Tara O'Toole of the Johns Hopkins Center for Civilian Biodefense Studies, Washington, D.C., August 22, 2000.

task. It is clear also that FBI and CIA guidelines about recruiting terrorists as informants must be simplified to make it easier to recruit terrorists to provide information.⁹⁶

The VP and the EPS should join with DOD and DOS to review our arms control posture to see if a more effective enforcement regime could put teeth into the prohibitions on the development of biological weapons. Even though the BWC's verification procedures will have serious limits, the BWC is useful because it strengthens the international norm against development of biological weapons and creates an impediment to nations bent on acquiring biological warfare capabilities.⁹⁷

Finally, the VP and the EPS should study other ways to build up our prevention and deterrent capabilities against terrorists and cyber attack. A well-conceived, effective, and well-publicized exercise program that demonstrates our capability to deal with attacks could help to deter hostile states or terrorists from choosing biological or chemical weapons or attacking our critical infrastructure. More directly, strong intelligence as well as robust customs, border patrol, and Coast Guard capabilities will remain the most important steps we can take in any incident prevention process.

In a similar vein, the VP and the National Coordinator should support the continuation of Nunn-Lugar Threat Reduction Act. In the future, to help prevent threats to the West, Nunn-Lugar needs to redouble its efforts to assist the Russian government to destroy chemical stocks and related equipment.

CBRN Terrorism and Cyber Threat Training

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

In the cyber area, in 1999, there were only 10 U.S. citizens who received the highest academic degrees in computer security. Majoring in other aspects of computer science or related disciplines carries much greater financial rewards. Clearly, the federal government will have to establish incentives for people to move into this field and stay in government service. In this regard, CSIS applauds the appropriation in FY 01 of 11 million dollars worth of NSF-administered scholarship money for students who will serve in government cyber security positions.

For CBRN terrorism, the focus should be on training emergency responders, ER personnel, and public health officials. In the past 5 years, we have trained only about 3%

⁹⁶ This issue was first publicized in L. Paul Bremer III, et al., *Countering the Changing Threat of International Terrorism: Report of the National Commission on Terrorism* (Washington, D.C.: The Commission, July 13, 2000), pp. 7-10.

⁹⁷ This issue will be explored in a new paper by Dr. Michael Moodie of the Chemical and Biological Arms Control institute, forthcoming CSIS Press.

of the total number of emergency responders. To assist in training at their level, emergency responders need a single doctrinal focal point for manuals and training programs for civilian CBRN terrorism responders.

To move toward those goals in the near term, the USG should examine such options as:

- Fund the DOJ's Center for Domestic Preparedness at Anniston, Alabama to allow it to achieve full capacity of 10,000 trainees per year. Also, continue to fund the USPHS's Noble Training Facility at the same location. Both of these new institutions are special national assets and should be carefully nurtured and protected.
- Encourage departments who use the CDP to assign all of their graduates to training roles within the local departments.
- Continue to coordinate with the U.S. Army Chemical School at Fort Leonard Wood, Missouri to share training techniques and lessons learned on dealing with chemical and biological devices and defense operations.⁹⁸
- Continue at a minimum the same level of interagency effort at mobile training after the Domestic Preparedness Program goes under DOJ control in FY 2001.
- State Department-sponsored training of host nation personnel is chronically underfunded and should be drastically increased. In other areas, the VP and NCA should do whatever is necessary to assure full funding for protection of US embassies and installations overseas.
- As a separate entity, fully fund the National Defense Preparedness Office clearinghouse for information on WMD preparedness planning and policy.

In the long term, the federal government should:

- Continue to reassess equipment and training needs across the country.
- Determine the steady state number of people that will have to be trained to deal with terrorism and weapons of mass destruction.
- As initial needs are met, gradually abolish mobile training teams and replace them to the greatest extent possible with multilevel institutional training at full capacity

⁹⁸ CSIS questioned whether there was excess capacity at the USA Chemical School at Fort Leonard Wood that could be used to train first responders. An extensive estimate was conducted on-site and Army experts determined that there was very little excess capacity there. See correspondence from the USA Chemical School to CSIS, dated October 4, 2000.

CDP(s), or other fixed training institutions. The focus of this institutional training should be to train local trainers and officials.

- Develop a WMD “training and doctrine center” in Anniston, Alabama or some other suitable facility. This center could also become the hub of the cyber attack and CBRN terrorism lessons learned process. Also, organize a series of conferences, as well as a private Internet site, to facilitate the sharing of ideas and lessons-learned among emergency responders throughout the U.S.
- Study the need and feasibility of establishing a second CDP-type of live agent training facility, probably in the western United States, to allow a greater number of responders to be trained expeditiously in a toxic agent environment.
- Foster greater organizational collaboration between the health sector and emergency management officials. Such collaboration is critical for survival at the local level during an epidemic. FEMA and HHS should develop an equivalent national preparedness program together to foster such collaboration. Linkage at the county and city level is critical and will not happen until the FEMA and HHS are well-connected by a common doctrine guiding bioterrorism preparedness and response at the top level.

Medical Training and Preparedness

In a similar vein, we need to continue to improve the ability of U.S. hospitals, public health services, and health care providers to deal with mass casualties and the effects of chemical and biological weapons. This will entail the examination of the most cost effective approach to equipment and drug stockpiling. All of this will be especially difficult in an environment where a third of all civilian hospitals are already losing money. The USG will have to continue to leverage the public health and VA medical systems to help local hospitals adapt to the threat.⁹⁹

⁹⁹ For more detailed recommendations on CBRN terrorism and the cyber threats, see reports by Arnaud de Borchgrave and Frank Cilluffo, forthcoming CSIS Press.