

CSIS

**Center for Strategic and International Studies
1800 K Street N.W.
Washington, DC 20006
(202) 775-3270
Web: Acordesman@aol.com**

**DEFENDING AMERICA
REDEFINING THE CONCEPTUAL BORDERS
OF HOMELAND DEFENSE**

**Counterproliferation, Counterterrorism,
And Homeland Defense:**

A Threat Analysis

Executive Summary

Rough Draft for Comment

**Anthony H. Cordesman
Senior Fellow for Strategic Assessment**

NOVEMBER, 2000

Introduction

The following report is a rough initial draft section of a full report on Homeland Defense being prepared as part of the CSIS Homeland Defense project. It is a rough working draft, and reflects solely the views of the author and not of the CSIS team working on the project. It is being circulated for comment and reaction and will be substantially modified and updated before being included in the final report.

Homeland Defense: The Threat of Indirect, Covert, Terrorist, and Extremist Attacks with Weapons of Mass Destruction

There is a wide spectrum of potential threats to the American homeland that do not involve the threat of overt attacks by states using long-range missiles or conventional military forces. Such threats range from the acts of individual extremists to state-sponsored asymmetric warfare. They can include covert attacks by state actors, state use of proxies, and independent terrorist groups. They can include attacks by foreign individuals and residents of the US whose motives can range from religion to efforts at extortion. Motives can include well-defined political and strategic goals, religion and political ideology, crime and sabotage, or acts by the psychologically disturbed.

These threats are currently limited in scope and frequency. No pattern of actual attacks on US territory has yet emerged that provides a clear basis for predicting how serious any given form of attack will be in the future, what means of attack will be used, or how lethal new forms of attack will be if they are successful.

As a result, there is a major ongoing debate over the range of threats that need to be considered, the seriousness of such threats, and how the US government should react. A GAO report on terrorism summarizes the various views within the US government regarding these uncertainties as follows:¹

...there are three schools of thought on the terrorist threat: (1) some believe the threat and likelihood of terrorist attack is very low and does not pose a serious risk; (2) others believe the threat and likelihood of terrorist attack is high and could seriously disrupt the U.S. national and economic security; and (3) still others believe assessments of the threat and vulnerability to terrorist attack need to be accompanied by risk assessments to rationally guide the allocation of resources and attention. The expert further stated that such risk assessments would include analyses of vulnerability and susceptibility to terrorist attack and the severity of potential damage. According to U.S. intelligence agencies, conventional explosives continue to be the weapon of choice for terrorists. Although the probability of their use may increase over time, chemical and biological materials are less likely terrorist weapons because they are more difficult to weaponize and the results are unpredictable. Agency officials also noted that terrorist's use of nuclear weapons is the least likely scenario, although the consequences could be disastrous.

It is difficult to predict how these threats will evolve in the future. Potential attackers have good reason to fear American military power, and most are unlikely to launch such attacks without considering the risks. At the same time, America's very strengths create an incentive to

attack it using asymmetric forms of warfare. The US homeland is vulnerable. Waging asymmetric warfare against the US offers both the greatest chance of success and the least risk of retaliation, and some key technologies are evolving in ways that aid the attacker. For example, biological warfare and information warfare will inevitably make the potential threat from both foreign and domestic attackers more serious over time.

It is equally difficult to predict whether attackers will emerge with both the capability and willingness to use weapons of mass destruction. It is not difficult to predict that such attacks are possible. Attacks involving very large amounts of high explosives or chemical, biological, radiological, and nuclear (CBRN) attacks have long been technically feasible, and the “globalization” of chemical and biological technologies and production facilities is making some weapons easier to develop or acquire. Nuclear proliferation continues and the levels of control over weapons, fissile material, and radioactive material are uncertain. Attacks using such weapons can involve a wide range of different levels of casualties, but they can involve attacks that could kill well over 10,000 to 100,000 Americans, with economic, physical, psychological, and political effects that are radically different from any covert, terrorist, or extremist attacks that have occurred to date.

These risks help explain why the US has steadily refined its policy toward terrorism and the risk of such attacks since the Vice President's Task Force on Terrorism issued a report in 1985 which highlighted the need for improved, centralized interagency coordination of the significant federal assets to respond to terrorist incidents. The US response to potential threats from covert attacks by state actors, their proxies, or independent extremists and terrorists has changed even more since the mid-1990s.

The National Defense Authorization Act for Fiscal Year 1994, Public Law No.103-160, Section 1703 (50 USC 1522) mandated the coordination and integration of all Department of Defense chemical and biological (CB) defense programs. As part of this coordination and integration, the Secretary of Defense was directed to submit an assessment and a description of plans to improve readiness to survive, fight, and win in a nuclear, biological and chemical (NBC)

contaminated environment.

The bombing of the federal building in Oklahoma City led to the issuance of Presidential Decision Directive 39 (PDD-39) in June 1995. PDD-39 built on the previous directive and contained three key elements of a national strategy for combating terrorism: (1) reduce vulnerabilities to terrorist attacks and prevent and deter terrorist acts before they occur; (2) respond to terrorist acts that do occur – crisis management – and apprehend and punish terrorists; and (3) manage the consequences of terrorist acts, including providing emergency relief and restoring capabilities to protect public health and safety and essential government services. This directive also further elaborates on agencies' roles and responsibilities and some specific measures to be taken regarding each element of the strategy.²

These policies have since been further developed by two key Presidential Decision Directives, PDD-62 and PDD-63, which were issued in 1998. PDD-62 reaffirmed the basic principles of PDD-39, but clarified and reinforced the specific missions of the US agencies charged with defeating and defending against terrorism, and created a new and more systematic federal approach to fighting the emerging threat posed by weapons of mass destruction (WMD). This includes programs to deter terrorist incidents involving chemical, biological, radiological, and nuclear weapons, and to manage the consequences if such incidents should occur. PDD-63 called for a national effort to assure the security of critical infrastructure. It covers both critical infrastructure protection and cyber crime, and the security of both government and private sector infrastructure to ensure national security, national economic security, and public health and safety.

New legislation has also shaped US policy. “The Defense Against Weapons of Mass Destruction Act,” contained in the National Defense Authorization Act for Fiscal Year 1997 (title XIV of P.L. 104-201, Sept. 23, 1996), established the Nunn-Lugar-Domenici Domestic Preparedness Program. This act made the Department of Defense the lead federal agency for implementing the program, and is to work in cooperation with the FBI, the Department of Energy, the Environmental Protection Agency, the Department of Health and Human Services,

and the Federal Emergency Management Agency.³ Equally important, major new funds have been spent on federal programs to deal with these threats, and federal spending increased by at least 43% between FY1998 and FY2001.

At the same time, there is no way for federal, state, and local governments to predict what attackers will actually take the risk of launching attacks on the US, or to predict the kind of event or crisis that could suddenly change their willingness to use any given means and level of attack. There are no clear boundaries that separate one form of attack from another, or that allow the US government to predict where and how it will have to attack to defend against an attack or to respond to one.

While it is tempting for governments to plan for the kind of cleanly defined single incident with which governments can best cope, there is no reason to assume that an attacker must follow such rules. Multiple attacks can greatly complicate defense and response and use different means of attack. A single attack can use a variety of weapons ranging from a mix of biological agents to a mix of chemical and information warfare. One attacker can piggyback on the attack of another, and attacks on the US homeland can be linked to attacks on Americans overseas or our allies. The very threat of an attack can be used to try to deter the US from attacking or exercising its diplomatic or military power, or it can be used to try to force a domestic political agenda on federal, state, or local governments.

Equally important, homeland defense must respond to a constantly changing threat. Many of the actions necessary to defend the American homeland will take years – sometimes well over a decade – to fully implement. In many cases, research and development is required, and the end result must then be transformed into deployed and effective capabilities at the federal, state, and local level. Such action can only be cost-effective, however, if it has a reasonable life cycle or period of effectiveness.

As a result, the US must make decisions now to shape programs that will affect its capabilities as much as a quarter of a century in the future. It must do so knowing that it cannot predict what new threats will or will not emerge, and that grave uncertainties exist

regarding the emergence of new methods of attack and defense, and the balance of technology between them. The world can evolve in radically different directions, and is almost certain to do so. The level of foreign threats can vary sharply by region, and the level of domestic threats can change strikingly. Santayana's warning that those who cannot remember the past are condemned to repeat it is as valid as ever, but those who ignore the uncertainty of future change may well face far more serious problems.

These uncertainties have polarized part of the debate over the threat posed by weapons of mass destruction and attacks producing mass casualties. There are those who believe passionately that such attacks on the US homeland are inevitable. There are those who believe the threat is unreal, and that it is an exaggeration that has grown out the search for new threats following the end of the Cold War. There are debates over how the threat should be categorized and prioritized, what response measures are needed, if any, and what kinds of attack are most likely. So far, these debates have provided many insights as to what may happen, but no basis for resolving the many uncertainties involved.

General Recommendations

The US faces real and growing potential threats from state actors, their proxies, or independent extremists and terrorists. While US agencies and analysts have tendency to exaggerate the immediate threat, or the threat posted by given actors, there are many potentially hostile foreign and domestic sources of such threats, and some key threats like biological weapons involve rapidly changing technologies that will pose a steadily growing threat to the America homeland.

It is also clear from the preceding analysis that the federal government is making progress in many areas, and laying the groundwork for improved cooperation with states, localities, the private sector, and the public. Indeed by the standards of many governments that face far more clear threats than the US, the US has already made significant progress in beginning to address these issues. In many cases, the US is already well ahead of its friends and allies.

At the same time, there is much to be done. Many detailed recommendations have already been discussed in the analysis of the threat, and federal activities and spending by agency, and the recommendations of various commissions. In many cases, it is the willingness and ability to address these detailed issues and recommendations that will determine the success of the US effort in Homeland Defense and not the effort to find a few major recommendations. The issue simply does not lend itself to vague calls for improved strategy or games with control, coordination, and organization chart. The devil really is in the details, and “bumper sticker” or one issue approaches to policy are a recommendation for disaster.

There are, however, a number of general recommendations that could help refine and improve the US effort.

Planning for Both Higher-Probability, Lower-Consequence and Low Probability/Catastrophic Events

The US must come firmly to grips with the fact it does not exist at the end of history and has not forged a kinder and gentler world:

- *Unchecked vulnerability is an unacceptable danger for “the world’s only superpower.”* Nature may abhor a vacuum, but enemies do not, and the evolution of more effective homeland defense is almost certainly essential to deterrence. At the same time, the very term “homeland defense” can be misleading. There are no boundaries that separate US counterproliferation and counterterrorist activity in defense of the American homeland from defense of its allies, military forces, and citizens overseas.
- *Deterrence, counterproliferation, counterterrorism, and law enforcement must be closely linked in dealing with these new threats, and it is clear that US must rethink many of its current security concepts.* Even the strongest advocates of homeland defense must recognize that a better offense may often be more effective than improved defense. Improving the offensive threat of retaliation overseas may often be the best way of defending both US interests overseas and US territory. A given investment in strengthening our allies may often be a better defense against proliferation and terrorism than investing in domestic counterterrorism programs. Hard trade-offs may have to be made between investments in the intelligence needed to intimidate and deter foreign states and terrorist groups, and the law enforcement capabilities needed to intercept attackers once they enter the US.
- *The US cannot afford to rely on rethinking the offense as a substitute for improved defense, anymore that it can use defense as a substitute for deterrence, offense, and retaliation:* The US cannot prepare itself for the new threats posed by asymmetric warfare, foreign proliferation and terrorism, and domestic violence using new means like chemical, biological, and information warfare without much stronger programs to prevent such attacks in the US and to respond to them if they succeed. The world of the 21st Century will not be a repetition of the mutual assured destruction of the Cold War. Radical states, regimes acting under extreme pressure, terrorists, and American citizens can turn threats like chemical, biological, and nuclear weapons

into grim realities in ways the US will never be able to deter with complete confidence.

- *The US must act now if it is to prepare for the future.* Developing an effective program means thinking at least 25 years into the future. It will take at least a decade for federal, state, and local authorities to develop the organization they need to deal with these threats. There are massive organizational problems that federal, state, and local authorities must solve in order to cooperate efficiently. The role of the federal government must be redefined in ways that are both compatible with a free society and which can preserve one when it is under attack and when attacks are successful. It will take years of exercises, tests, and training to determine what courses of action can be made to work and are most effective. Investing in such a process of change means that it must be flexible and modular enough to react to the fact no one can predict the nature of future attacks, but any meaningful improvement in capability will be so expensive that it can only be justified if it can cope with uncertainty.
- *The US must decide whether it will begin now to fund effective defenses against attacks on a scale far different from any form of covert or serious attack than it has planned to deal with since the end of its efforts to provide civil defense against nuclear attack.* Marginal changes in federal, state, and local efforts, and in the relationships between federal, state, and local agencies, can do much to cope with the threat posed by attacks using large amounts of high explosives, chemical weapons, and low-lethality biological and radiological attacks. While the level varies by state and locality, attacks involving 1,000 to 10,000 casualties do not require radical changes in response capabilities. Nuclear and high lethality biological attacks can, however, easily produce casualties in excess of 10,000-100,000 Americans. To date, most studies and exercises indicate that existing programs and capabilities would not be adequate to deal with such attacks, and they would require far more decisive federal action and intervention than is currently feasible. There are those who argue strongly that no such threat currently exists and those who argue with equal force that they are inevitable. The present reaction of the federal government seems to be to try to improve near-term response capabilities to deal with lower levels of attack while conducting research and development into the higher levels of attack, but the policies involved remain unclear and the actions of federal agencies reflect very different perceptions of these threats.
- *The US must take a new approach to research and development and technology:* There are many areas of new technologies which must be moved off the drawing board, tested, deployed, and modified if the US is to have defensive tools that begin to match its offensive capabilities. At the same time, the US needs careful net assessments of the trends in the threat and how these impact on new approaches to defense and response. Effective planning means that the US cannot afford to mix the myth of technology with the reality. The past track record of US efforts to create and use new technologies in its defense is one of amazing eventual success. At the same time, it is one of almost universal evidence that even the best technologists cannot be trusted to create successful and deployable tools with anything like the promised effectiveness at the promised cost and time.

The development of such a complex approach to threat assessment, based on a frank admission of the vast uncertainties involved, goes against the basic grain of the American character, and forces far more demanding criteria for program justification than are normally required. The US cannot, however, deal effectively with threats posed by state actors, their proxies, or independent extremists and terrorists unless it adopts such an approach.

Even if the US adopts such an approach, however, it will still have to concentrate its limited resources on making marginal improvements in current capabilities to deal with current

threats, while adopting a research and development-driven approach to dealing with more serious and emerging threats. As a result, any US program is likely to have marginal impact, and require constant evolution for at least the next half decade.

Planning for Both Terrorism and Asymmetric Warfare

No one can predict that the US homeland will be subject to major asymmetric attacks using weapons of mass destruction. At the same time, this study has indicate that there is a clear incentive for such attacks and that there are states that could emerge as potential attackers. There is no firm way to assign priorities to the need to fill the gap between “terrorism” and the concern with overt threats like ballistic missiles, but the following factors must be considered:

- Low level terrorist attacks are indeed more probable, and in fact are constantly occurring at the cyber and false alarm level. Seen over a 25 year period, however, the probability of some sophisticated form of major asymmetric attack is high. This probability not only affects the US, but its allies.
- The US faces a “non-Gaussian” reality in trying to predict and characterize the nature of such threats. There is no “standard distribution curve” of past events that can be used to predict the future.
- The cumulative probability over time of a low to moderate probability event actually be the highest priority for planning is much higher than the probability the most probable events will actually be the highest priority for planning.
- The US cannot deal with the problem by adding analytic and technological elegance to the classic American solution to all critical problems: “Simple, quick, and wrong.”
 - Crisis/war driven intentions and escalation extremely difficult to predict.
 - History is irrational and is often made out of worst cases. Intelligent, prudent, “business as usual” intentions usually means crisis never occurs in the first place.
 - Asymmetric values and perceptions are very real, but extremely difficult to assess and transform into meaningful predictions of future hostile action against the American homeland.

In reacting to the higher levels of threat posed by asymmetric warfare, the US must consider the following factors:

- The problems of warning, defense and response differ sharply by level of attack and threat.
- The rules change for all responders as attacks escalate from conventional low-level terrorism (“crooks and crazies”) to major levels of damage and casualties:
- A true national emergency involving a nuclear and/or major biological attack will force the Department

of Defense into a critical and probably lead role.

- Law enforcement must operate in state of national emergency, rather than on a business as usual basis. The issue of having to retask law enforcement to operate in an undeclared state of war becomes a very real prospect.
- Public health and emergency services will be saturated and face realities they can only half-anticipate.
- Possible threats can emerge to the basic structure of America's commerce, economic infrastructure, continuity of government.
- Any a nuclear and/or major biological attack on the American Homeland well be linked to a serious theater-driven crisis or war. If so, the threat will not be directed at US per se, but at US as extension of regional/theater/foreign nation objectives.
- Allied targets, US forces and businesses overseas, and critical economic facilities can be targeted, not just US.
- Multiple and sequential attacks become more likely, as are mixes of methods of attack.
- The availability of sophisticated biological and nuclear weapons more likely.
- The possibility of simultaneous attacks on information systems and critical infrastructure will offer asymmetric attackers a low cost adjunct to virtually all forms of asymmetric and theater warfare.

Within this context, it is important to consider both what asymmetric threats and terrorism have in common, and some of the critical differences. The common areas include:

- All threats relate to a wide range of different national security activities as well as a wide range of domestic defense and response efforts.
- All efforts to improve Homeland defense compete for limited resources and federal emergency management capabilities.
- All US response risks "squeezing the balloon:" Defending in one area while failing in the others pushes attackers to attack the less defended area.
- There are many common problems in law enforcement.
- There are many common problems in public health and emergency services.
- Effective defense and response depends on an accurate assessment of the relative vulnerability of commerce, economic infrastructure, continuity of government.
- Terrorist or asymmetric use of weapons of mass destruction create the risk of attacks with effects so costly that response may prove unaffordable, and where it is unclear that technology and systems are available for effective response.

At the same time, there are critical basic differences between the impact of most

forms of terrorism and state sponsored or proxy asymmetric warfare:

- All attacks are not created equal. Limited CBR attacks at the terrorist and extremist level are fundamentally different from nuclear and highly lethal nuclear and biological attacks.
- Covert and proxy attacks by foreign governments are acts of war. Truly sophisticated terrorists will not operate under the limits currently assumed in most studies.
- Such attacks sharply raise the probability of “cocktails” of different agents, mixes of CBRN and cyber attacks, and the use of such attacks to supplement theater conflicts. NMD + CBRN + CIP is then credible.
- The current and perhaps any affordable response effort will collapse at finite and limited levels, forcing federal/state/local governments and the private sector to improvise radically.
- Bioattacks with immune or genetically engineered strains that have unpredictable delays, persistence, symptoms, ability to defeat treatment and vaccines, and lethality become a real possibility.
- Sophisticated attackers will respond to US defensive measures by (a) shifting their methods of attack to strike at the least defended areas, and (b) developing countermeasures to exploit the weaknesses in any defense.
- This makes “cost to defeat” and net technical assessment of all defensive programs and options critical.
- There does not seem to be any current prospect of dramatic changes in the ability to build a nuclear bomb in the basement and in domestic/foreign terrorist ability to acquire nuclear weapons.
- The situation with biological technology *may* be radically different. Bioattacks with immune or genetically engineered strains that have unpredictable delays, persistence, symptoms, ability to defeat treatment and vaccines, and lethality then become a real possibility.
- There are major and natural differences in priority between Defense and Law Enforcement/Responder communities. Each focuses on business as usual.
 - Responders/defenders do not focus on levels attack so different from their experience that they are regarded as “mission impossible.”
 - The linkage to foreign threats and wars is largely ignored outside the Department of Defense and national security community.
- Intelligence and law enforcement efforts are now decoupled in ways that pose serious legal barriers to effective action in dealing with asymmetric warfare and the threat of nuclear and major biological attacks.
- Asymmetric warfare can push US rapidly towards Presidential state of emergency, most terrorism is business as usual.
 - Defense/response may have to be given priority relative to normal legal procedures and civil rights.
 - Federal, regional, and state efforts to cope with the breakdown/collapse of local defense and

response efforts must have a much higher priority.

- The risk of attacks with effects so costly in damage and casualties that response may prove unaffordable is much higher, and there is a very real uncertainty that the technology and response systems are now available for effective response.

Reacting to the Uncertain Nature of the Threat

There are many “true believers” who feel that a given threat will or will not materialize in a given form. Given the inherently uncertain nature of predictions as to who will be a threat, the means of attack they will use, and the effectiveness of the means of attack they use, it is almost certain that some of these “true believers” will prove to be right. The problem is that there is no sufficient evidence to say which threats are most important, or to predict the means of attack and level of effectiveness.

Federal programs are being forced to deal with an extremely broad spectrum of potential threats that individually have low probability, but where there is high probability that some of these threats will emerge as threats to the American homeland. As a result, each agency and department tends to treat the threat in terms of its own mission and institutional bias, and this problem cannot be resolved by central direction. Having the National Security Council, a “terrorism” czar, or an interagency forum agree on a given threat or threats will not affect the laws of probability. Uncertainty is simply uncertainty.

There is also an inherent danger in attempting to create a truly coherent program. When a truly high degree of uncertainty exists regarding the need for specific forms of federal action, enforcing a high degree of coherence from the center may actually interfere with the efficient use of resources. In many cases, individual agencies will achieve a higher capability to deal with uncertainty if they suboptimize around those marginal steps each can take to improve their existing capabilities to deal with a wide range of threats. This is particularly true in a sharply resource-constrained environment where many potentially desirable actions will remain unfunded until a much clearer pattern of threats emerges.

This is also true because the threats at issue involve a wide spectrum of extremely lethal

biological weapons and nuclear weapons. Large amounts of high explosive, chemical weapons, and less lethal biological weapons can produce truly tragic consequences. However, the level of deterrence, defense, and response pales in terms of cost in comparison with the ability to deter, defend, and respond to the kind of attacks that could involve casualties far in excess of 10,000 Americans and billions of dollars worth of damage.

There are three further problems involved in such threat analyses that badly need to be dealt with in further US efforts to plan and execute effective programs:

- *Most of the lethality and effects data for chemical, biological, radiological, and nuclear weapons involve major uncertainties that badly need to be resolved, and the federal government is just beginning to develop effective models and simulations of such effects.* There is no lack of effects data or models per se, simply an immense lack of credibility and parametric modeling of uncertainty in a form that goes from dramatizing the problem to being useful in developing specific lessons for federal, state, and local responses. These problems have also been compounded by a natural tendency to build models to justify given policy recommendations or programs. To be blunt, agencies in the federal government, FCRCs, contractors, and NGOs are far better at using analysis to market given policies and programs than to perform analysis per se. There is a striking lack of intellectual rigor and analytic integrity in many of today's efforts that must be remedied if the US is to prioritize federal actions and funding.
- *Programs shaped around today's threats, or some prioritization based on current assessments, will not solve any of the key problems in planning and programming.* Democracies do not suddenly develop solutions they can then keep secret from their enemies. US programs take time to implement and must be publicly funded and implemented in an open society. As a result, potential attackers can adopt new methods of attack and respond to any remaining gaps in US capability. This makes it absolutely essential to explicitly analyze the cost of defeating any given federal program over time, and the probable impact improving any US capability will have in driving attackers to use other means.
- *New methods of analysis must be developed that examine the present and future balance of offensive, defensive, and response capabilities. They must be supported by adequate net technological assessments, and analysis of countermeasures and costs to defeat all ongoing and proposed federal activities.* It is difficult enough to analyze current or near-term risks, but such analysis simply is not adequate. Effective US programs can take a decade or more to fully implement, and the technology shaping current threats is constantly changing. This is not simply a matter of basic advances like biotechnology, it is a matter of the steadily growing dissemination of the technology equipment needed to produce and deliver large amounts of high explosive, chemical weapons, and biological weapons. Much of the description of potential threats does not explicitly analyze the potential growth or changes in threat technology even when it proposes the adoption of new deterrent, defensive, and response technologies over a period of many years. There is a lack of technological net assessment that is a key not only to identifying and prioritizing effective programs, but to managing them so they counter technology growth.

The Lack of “Transparency” in Federal Programs

There is nothing unique about the lack of transparency in federal programs to deal with the threats posed by state actors, their proxies, and foreign and domestic extremists, and the use of high explosives, chemical, biological, radiological, and nuclear weapons. The US budget, and agency program and budget descriptions often fail to describe their budgets, the nature of their programs, and measures of effectiveness in any detail. Aside from the Department of Defense, there are virtually no future year spending projections, and the Department of Defense classifies the breakouts of its future year spending projections that provide any useful description of how money is to be spent.

Far too much of the federal literature on “terrorism,” however, is threat-driven. It does not describe and justify the program, it describes the threat. There is no description of exactly what program activities are involved, or of past, current, and projected costs. There are no measures of effectiveness, or total spending and procurement are confused with such measure. As a result, it becomes extremely difficult to understand what the federal government is doing and why it should do it. Many of the descriptions that agencies do provide raise real questions about the extent to which given agencies have simply reshaped existing activities to take account of the fact the Congress is providing new incremental funding, and counter-terrorism has become fashionable.

These problems are compounded in part by the fact that OMB is required to report to the Congress, but there is no central agency charged with creating a plan, program, and budget. At the same time, they are compounded by a host of jurisdictional problems with the Congress, and the lack of a single committee or joint committee structure that could provide a cohesive degree of overview. As a result, there is a large pool of federal reporting on individual problems and issues, but little effort to appraise the overall program.

There are those who would argue that part of the reason for the lack of transparency is security. There are certainly areas like intelligence where detailed program descriptions could compromise security. There are other areas where too detailed a description of US

investigative and response capabilities could aid an attacker in planning an attack. In broad terms, however, there is little reason to classify most of the information needed to allow outside analysts to fully understand the nature of federal efforts, and there are good reasons to require federal agencies to provide such data.

To put it bluntly, far too many federal activities seem to have limited substantive value, raise major uncertainties, reflect the reshaping of existing programs to obtain incremental funding, or raise questions about duplication. Furthermore, there is a tendency to imply short-term solutions can be found to long-term problems, or fund minor palliatives simply for sake of seeming to act. Few, if any, programs provide any picture of what it will cost to fully implement the activities agencies are now beginning. None seem to provide meaningful measures of effectiveness, or any analysis of the current and future costs of “defeating” the capabilities being funded.

- *While there are sharp limits to how much coordination can be forced on a wide range of federal activities, the federal effort would almost certainly benefit from a requirement for a comprehensive annual report similar to the one the Secretary of Defense provides on the national security activities of the Department of Defense, and for including both a net assessment of the threats and US capabilities, and the future year budget implications of given federal activities as well as a description of the current budget request.*
- *Regardless of how the issue of Congressional jurisdiction is resolved, there is also a clear case for requiring the federal government to submit an annual budget justification document, and future year budget plan, that covers all related federal activities at the same time the President submits the federal budget. Such a document could be both unclassified and classified. It would thus ensure that the Executive Branch had to coordinate its programs fully as part of the budget process. It would ensure that whoever is in charge in the federal government had real review authority, and control of money is generally better than a title. It would ensure that all elements of Congress reviewed a common plan, which may be far more important than creating a single new committee. It would also allow full public review and state and local access to the overall federal plan. It is easy to talk about “reinventing government;” it would be nice to actually provide some degree of functional transparency in a critical new mission area.*

Focusing on Priorities, Programs, and Trade-offs: Creating Effective Planning, Programming, and Budgeting

The US would face serious resource allocation problems even if CBRN threats were less uncertain and ambiguous. The threat posed by covert, terrorist, or extremist use of weapons of mass destruction is only one of the new threats the US must react to. Homeland defense includes direct threats such as missile attack, and other evolving threats like information warfare. There

are other transnational threats like narcotics, organized crime, and illegal immigration that pose a serious threat to American society even if they are not military or paramilitary in character. At the same time, the US faces major problems in funding its existing future year defense program, and its civil discretionary and entitlements budget. Money is, and will remain, a critical factor, and will force hard trade-offs on all government action.

This report focuses on the threats to the American homeland posed by state actors, the use of proxies, terrorist and extremist attacks by foreign groups or individuals, and terrorist and extremist attacks by residents of the US using conventional weapons and weapons of mass destruction. Separate reports focus on the threat posed by direct attacks by foreign states using weapons like ballistic missiles, and the threat of information and economic warfare.

This focus is not intended to imply that the emerging threats to the American homeland can be neatly compartmented, or do not interact. The spectrum of threats foreign governments can pose includes all of these methods of attack. Well-organized foreign and domestic terrorist/extremist groups have the *potential* to pose a wide range of high explosive, chemical, biological, and information warfare threats. There are no rules that say foreign governments and foreign and domestic terrorist/extremist groups cannot cooperate or piggyback on each other's activities. In broad terms, however, the threats to the American homeland posed by state actors, the use of proxies, terrorist and extremist attacks by foreign groups or individuals, and terrorist and extremist attacks by residents of the US using conventional weapons and weapons of mass destruction require a different mix of responses. These responses can only be discussed in terms of practical alternatives if it is narrowed down to the point where each of the major relevant homeland defense options can be analyzed in depth.

As is the case with national missile defense, this report also deals with issues that are highly politicized. Preparing to deal with the spectrum of threats posed by foreign states and terrorists using weapons of mass destruction is currently fashionable and "politically correct." This has had major benefits in many ways. The President and high level officials have set forth clear policies for dealing with many aspects of the problem. The Congress has passed dramatic

new legislation, and major changes are well underway to improve federal, state, and local preparation to deal with the threat. There is new money available to federal agencies at a time when severe budget constraints exist on virtually every form of government spending.

Unfortunately, however, the very popularity of the issue of terrorism and weapons of mass destruction also means that there has been a rush to react to potential threats without developing a common definition of the combined threat posed by covert attacks by state actors, state use of proxies, terrorist and extremist attacks by foreign groups or individuals, and terrorist and extremist attacks by residents of the US. There is still insufficient definition of the different kinds of **threats** that different kinds of weapons of mass destruction pose and how these relate to threats using conventional explosives. In many cases, departments and agencies are defining the nature and intensity of the threat to meet their own internal needs and perceptions, or are acting on assumptions that imply a far better ability to predict the future than can possibly exist.

As yet, there is only limited coordination in many federal, state, and local efforts except at the organization chart level. Departments and agencies struggle for resources and influence, and there are good reasons for the resulting “feeding frenzy.” Even if one ignores all federal funding for critical infrastructure protection, the funding for counterterrorism has risen from \$6.5 billion in FY1998 to \$8.3 billion in FY2001, and the funding for new efforts like dealing with the threat posed by weapons of mass destruction have risen from approximately \$645 million in FY1998 to \$1.6 billion in FY2001.

Under these conditions, old programs are being recast to suit new policy priorities and rhetoric, while agencies compete to create new programs and assume lead responsibility. In some ways, homeland defense has replaced the Strategic Defense Initiative as the “next best thing.” As the GAO and CBO have pointed out, the sharp rise in spending has not yet led to tight central management of the homeland defense effort, although there is a growing and steadily more effective effort to develop balanced and coordinated capabilities. There also has been little success in estimating the mid and long term budget implications of program growth and new responsibilities at the federal level, much less the state and local level. Many RDT&E efforts

have been started without clear deployment and life cycle implementation plans, and there are few meaningful measures of effectiveness for federal spending.

The sharp limits on how much money and human resources can be allocated to this aspect of homeland defense will, however, soon force the US to be much more selective in choosing the programs it can continue to expand or sustain. Even today, the government needs to make every effort to coordinate its efforts and prioritize them. Regardless of partisan rhetoric, it is clear that US is not yet prepared to pay for its existing military forces and capabilities. Furthermore, there are other major transnational problems like drugs, immigration, and cybercrime. There are many unrelated shortfalls in law enforcement and emergency response capabilities. For example, the US faces a major crisis in medical spending even without considering the impact of responding to chemical, nuclear, and biological attacks, and is sharply reducing the size of its emergency medical facilities and hospital intensive treatment capabilities.

It is only possible to ignore these realities at the start of a homeland defense program, at a time when planning is largely threat driven and the cost of new activities is relatively limited. As long as current outlays are limited, it is all too easy to find a credible potential threat, issue warnings, make a speech, issue an executive order, or pass a law. Any competent analyst, contractor, research firm, NGO or advisory group can find a new way to focus on potential threats and the potential merit of uncosted and poorly defined solutions. The end result is starting far more activities than can be finished, failing to consider the future trade-offs that must be made to deploy effective capabilities, duplicating other efforts, or refashioning existing programs under new labels.

- *Improvements in policy and strategy are no substitute for effective management, programming, budgeting, and measures of the effectiveness. The practical challenge is to use more management information systems and PPB methods to tie the efforts of government together to develop clear priorities, ensure that cost estimates are provided of bringing programs to maturity and sustaining them, tightly manage where the money goes on an ongoing basis, ensure that the risk of countermeasures and cost to defeat is assessed on a continuing basis, find suitable measures of effectiveness, and make suitable iterative trade-offs. In fact, one recommendation of this report is that there be one central point in the federal government charged with developing a budget overview of current programs, an analysis of their future year costs and deployment costs, relevance to the threat, and measures of effectiveness.*

Unless this transparency is ruthlessly forced upon the federal government – both in the executive branch and Congress – no amount of organizational changes, committees, legislation, and directives will create the proper focus. The creation of lead agencies will be a bureaucratic farce, and state and local authorities will be confronted with conflicting demands, and will often have little impact on federal bureaucratic infighting.

Equally important, Congressional oversight and effective outside review and constructive criticism will be impossible. The constant misuse of security classification will create large areas of “black programs” that encourage departmental empire building and a lack of management. Programs with limited relevance will be recast as part of the homeland defense effort, and areas that really need funding will be ignored.

Effective Action Must Be Broad-Based and Sub-Optimize Efficiently

At the same time, there are limits to how much coordination is practical, and how much central direction can be applied. The federal government, individual agencies, and state and local governments will often have to sub-optimize changes to their current programs in those areas where they can do the most in the near term with the least money. While the Clinton Administration is seeking to create a cohesive federal program, and has made progress towards this end, there are no models, analytic methods, or simulations which can hope to integrate all of the elements of homeland defense into some master analysis or set of priorities based upon a common model.

The problem is not specialization and compartmentation per se. It is that it must be the result of central management and oversight, particularly given the severe limits on what any foreseeable combination of allied, federal, state, and local efforts can do. Cost constraints will be tight, trade-offs will be made whether or not they are made openly and explicitly, and the result will be anything but leak-proof. Most importantly, central direction is needed to ensure that the capabilities the US creates evolve to respond to reality and not to established bureaucratic

priorities.

It is also far from clear that threat and risk assessments can be used to create a set of scenarios that focus the defense effort, or which prioritize it around a select and well-defined group of scenarios. Once again, the problem is to determine the range of low probability events the US may have to react to, and what this means for deterrence, offense, defense, and response. While it is most likely that the US will have to react to a series of relatively low level events in the near term, the cumulative probability that the US may have to react to a few much more serious events over the mid to long term may well be equally high. As a result, threat and risk assessments must consider nuclear and highly lethal biological attacks.

Furthermore, there are deep conceptual problems. As has already been discussed in depth, the range of threats simply are not predictable enough for given agencies to attempt more than a constantly evolving and uncertain process of suboptimization. Put differently, departments and agencies must often do what they can to improve their capabilities at the margin, rather than seek to create building blocks in some kind of coherent homeland defense.

Such efforts may not, however, have great impact on US ability to defend against nuclear and highly lethal biological attacks. They may give the impression of defense and response capability, but the end result might not be able to cope with very high levels of attack, which may well force all levels of government to improvise radically with little warning and under intense pressure. Marginal improvements in resources may fail to deal with response requirements or be impossible to allocate efficiently within the time windows required. This is particularly true because there currently seems to be little practical understanding of what a “worst case” or high level attack would really do, and how uncertain its effects now are.

Finally, the present coordination effort often focuses either on “worst cases” or on those federal programs identified as being directly designed to defend or respond to the threat state actors, their proxies, or independent extremists and terrorists pose to the American homeland. This is almost certainly *not* the right way to create the most effective overall program to actually improve homeland defense. Such a program must explicitly consider the offensive,

deterrent, and retaliatory capabilities of US military and intelligence agencies, and the role their activities overseas can play in creating an effective deterrent to foreign attacks on the US.

As a result, the US needs to rethink its approach to develop a program that constantly evolves, and which is based on the dilemma that it must try to manage chaos:

- *Effective homeland defense must be based on responding to the patterns of threats that actually emerge, and to shifts in the most likely contingency requirements.* It is virtually an iron law that any effort will fail that is based upon the current theories of what threats *may* emerge in a given area. Once again, a guiding principle is that there is a timeline of at least a quarter of a century of uncertain risk. No program or analysis made today can possibly be based on the correct priorities. The issue is rather how quickly and effectively programs can anticipate change and react to it.
- *The key to a successful result is that sub-optimization must be deliberate and subject to broad review, and not simply evolve by accident. Whatever the federal government does, it must involve an explicit and well-reasoned balance between:*
 - Offense and defense.
 - Action overseas and in concert with our friends and allies, and measures actually taken in the US.
 - Counterproliferation and counterterrorism.
 - Defense and response.
 - Including threats in the spectrum of threats requiring special action by the federal government as part of homeland defense, and the role played by conventional law enforcement.

Managing Research and Development, Rather Than Treating CBRN As A Wish List and Slush Fund

Research and development programs receive little detailed description and the description that is provided often concentrates on the threat being dealt with, and provides little program detail. No agency provides a meaningful description of its future program, future costs, milestones, or measures of effectiveness. Cooperation with state and local agencies is often ignored, and when it is not, it tends to be discussed in anecdotal terms

There is no evidence that any department or agency has provided a technology net assessment to examine whether its programs will provide defensive capabilities that outpace advances in offensive capability. There is virtually no discussion of the risk posed by

countermeasures or the cost to defeat current and planned programs. There is no discussion of the outyear costs of research and development activity or of estimated deployment schedules, measures of effectiveness, and life cycle costs. Almost without exception, there is no way to be certain to what degree which given programs in given departments or agencies are actually focused on CBRN and other counterterrorism activities, or have simply recast ongoing or desired programs to compete for such funds.

- Federal research and development efforts have a poor to dismal record of effective management. It is time to reverse this situation.

Looking Beyond CBRN: Dealing with All Medical Risks and Costs

The previous analysis indicates that there is a need for a zero-based review of the current data on the lethality of biological weapons, and for a comprehensive net technical assessment of current and future trends in biological offense and defense. Biological warfare defense and response efforts cannot, however, be separated from the need for an effective national health program.

Response measures against biological and nuclear attacks can require truly massive increases in public health efforts and emergency services at a time when the US already faces major problems in funding medical entitlement programs and growing cost constraints are being placed on investments in medical capabilities which normally have high utilization rates. The response capabilities required to deal with large biological and nuclear “incidents” may simply be unaffordable without far more evidence that such attacks are likely, and effective treatment may simply be impossible. One grim result is that “triage” may have to be performed in ways that deliberately leave a very high number of casualties to die.

The risk of attacks on the American homeland that have massive medical consequences requires that homeland defense measures deal with two major interrelated problems in public health policy and spending.

- *The key limiting factor in terms of response capability and expense will be medical treatment. This*

requires nationally distributed capabilities, but it is unclear that they are technically credible and can be made cost effective? It is far from clear that today's defense and response training really prepares anyone for threats other than relatively small and easily characterized events. Much of the non-medical response effort seems to be focused around obtaining equipment and facilities to "get well" from past underfunding or provide equipment for small events. It is unclear that creating standard packages of such equipment, or responding to responder's priorities, really deals with the problem of homeland defense. The question is what kinds of training and equipment really help and what can really be done locally on a nation-wide basis.

- *There is a significant amount of medical literature – including a recent report by the National Intelligence Council – that indicates that the US is under significant cumulative threat of the outbreak of some disease for which current medical treatment is not adequate. In short, the US may face a serious threat from nature as well as from foreign attackers and domestic extremists.⁴*
- *However, US medical spending has already reached the point where it dominates much of the end use of the entitlements in the federal budget, and where drastic efforts are being made to down-size medical spending. These facts are largely ignored in much of the current discussion of homeland defense, which focuses on threats and then on research and development measures that do not have a deployment cost, and which often involves response efforts so limited in estimated casualties that the list of equipment is "affordable" largely because it is assumed that the existing infrastructure can deal with the casualties and the medical impact is both treatable and involves non-infectious threats. These assumptions, however, are only valid as long as the most serious threats are defined away and the eventual need to pay for facilities and a full spectrum of response measures is ignored.*

Homeland Defense and/or Law Enforcement

The US also faces major problems in defining the point at which federal intervention in some form of homeland defense program is needed, as distinguished from a reliance on normal federal, state, and local law enforcement. Many of the definitions now used for terrorism can include virtually any threat of violence by an individual or small group with a political or ideological agenda, or who is willing to attack civilians. In practice, however, most such threats are dealt with as normal law enforcement activities unless some foreign element is involved. Even in those cases where foreigners are involved, many cases are dealt with through normal law enforcement means.

It does not make sense to change these arrangements without clear cause, and the previous statistics on terrorism in the United States need to be kept in perspective in allocating law enforcement resources. According to the FBI's uniform crime statistics, there were 10 cities in the US with populations of 100,000 or more that had more than 100 murders in the first six months of 1999, and three with over 200 murders. If rapes and assaults are counted, there were

47 cities in the US with populations of 100,000 or more that had more than 1,000 “casualties” in the first six months of 1999, and nine with over 3,000.⁵

There is a reason why it now takes some 40,000 armed men and women to try to secure the greater New York metropolitan area alone. There is also a reason why law enforcement activity cannot be centered around counterterrorism or dealing with low probability covert attacks until there is a far clearer and more dangerous threat than now appears to exist. At the same time, it is inconceivable that the US could develop an effective approach to homeland defense that did not attempt to make use of these resources at every level of law enforcement.

- *The task is to find the right trade-offs between reliance on normal law enforcement and specialized homeland defense activity, and between using existing resources with other primary missions and creating new dedicated homeland defense components.*
- *It may be that the US will require a more decentralized and distributed defense and response effort than the federal government now realizes.* Most forms of federal response, and a great deal of state and regional response, could come too late to fit the critical time windows for biotreatment. And dealing with the prompt effects of nuclear explosions and fall out. Some form of decentralized and distributed local/civil defense may be the only answer. The questions then become prompt attack characterization, instructions to flee or stay, proper guidance to responders, and options for very low-cost distributed defensive aids like masks, medicines, etc.
- *The US needs to rethink civil defense.* It must look beyond asymmetric warfare and terrorism, consider broader national public health priorities, and NMD “leakage” problems. Real-time warning and threat and attack characterization, allow federal, state, and local defenders and responders to cover widest area most cheaply: The effective use of media to warn and advise citizens at risk will often help people avoid the effects of attack. Flee or stay advice will be critical, so will detailed advice on what to do in the office, home, and car a. There must be a real time linkage between defender, responder and media. At the same time, the US should analyze whether there are credible and affordable low cost civil defense options, and examine what can citizens, corporations, local, state, and federal governments might really be able to afford. Options like gas and biological defense masks, home shelters, etc. need examination.
- *At a different level, the US needs to study ecological and agricultural defense.* The risk posed by biotechnology cannot be evaluated solely in terms of threats to human beings.

Rule of Law, Human Rights, Asymmetric Warfare, High Levels of Attack and “New Paradigms”

Homeland defense impacts heavily on legal and human rights issues. Until now, the threats to the US have been limited enough so that the US can afford to shape its response on the basis of strict observance of civil law and human rights. There is also ample emergency authority

for the President, Governors, and local officials to use virtually all of the assets of government to deal with homeland defense emergencies if they arise. Even restrictions on the use of the military, such as the Posse Comitatus Act (18 USC 1385), have so many exceptions that the problem is much more likely to get sufficient warning to act than any practical legal barrier to effective action.

Much of the present discussion of legal and human rights issues, however, ignores what would happen if the threat of the use of biological or nuclear weapons against the US homeland became more tangible and immediate. It also ignores the real world effects of state actors or terrorists/extremists carrying out highly lethal attacks. These effects include the problems in human rights created by the need to deal with mass triage in the face of saturated medical facilities and/or to contain a civil population with force in the event of an attack using a highly infectious agent.

- *US intelligence efforts and law enforcement must both reorganize to deal with the risk of a “paradigm” shift in the willingness and ability to use weapons of mass destruction in unconventional attacks on the US homeland, and be given the proper legislation and regulations.* Many states are now involved in a process of proliferation that will change their capabilities to carry out such attacks. Advances in manufacturing, petrochemicals, and the biological sciences are making it steadily easier for both states and non-state actors to build lethal chemical and biological weapons. The technology and components to develop every aspect of nuclear weapons other than weapons grade uranium and plutonium are becoming steadily more available.
- *At the same time, there is a need for new basic safeguards to the rule of law and human rights.* No change should be made to the protection of civil and individual rights that does not require extraordinary due process and carefully defined levels of threat and potential risk. Virtually all attacks and threats to date have not posed a level of risk that justifies any change in current legal restrictions or protections of civil liberties. Such threats may emerge in the future, but they also may not. The risks posed by weapons of mass destruction and asymmetric warfare must be defined in ways where changes in the role of US intelligence, defense, and response are clearly linked to outside judicial review, and where only the most serious risks involve changes in the way in which government deals with such threats. There must be clear plans for possible states of emergency that do more than enable effective governmental defense and response. The US must define how it will act to protect civil rights and liberties even under worst case defense and response conditions, and provide a clearly defined set of reviewing authorities for any action in a state of emergency,
- *The issue of live or let die triage in the event of an actual attack where casualties saturate response capability poses the greatest single threat to human rights.* It must be addressed to guide local responders and determine whether new diagnostic and detection technology can reduce the medical burden. The US should not wait for the event to come to grips with the critical issue of how triage can be provided in response activities in ways which best protect individual rights as well as allow the most effective use of limited response resources.

The Need for Central Coordination and Management, and the Creation of Effective Future Year Planning and RDT&E Management Systems

There is broad agreement that some central office is needed to coordinate the federal effort, to ensure proper program and budget review, to coordinate auditing of capability, and to coordinate emergency response capability. There is also broad agreement that such a coordinator needs sufficient rank and authority to speak for the President on these issues, and to ensure that agency budget submissions must include adequate programs and funding. Some have proposed an independent office similar to the Y2K program, some a new form of drug Czar, and some a cabinet level officer.

- *These issues, however, need far more careful study, and the issue is not as much one of who is in charge as one of what they are really in charge of and the planning and management tools they need.* Similar arguments are being made about providing a coordinator to deal with critical infrastructure attacks and all of homeland defense. At the same time, many of the prevention and response skills involved are highly specialized and duplicate the activity needed to respond to many other forms of emergency – accidents, weather, etc. At this point in time, what really seems to be needed is a Presidential Task Force to review the broad need to deal with all of the emerging threats to the American homeland, and to draft recommendations and a PDD for the next President.
- *There are fundamental differences in the response needed at given levels of attack and threat:* Coordinating counterterrorism, civil law enforcement, and response to relatively limited attacks does not involve a state of national emergency, an undeclared war, or involve the kind of defense and response efforts need to deal with major nuclear and biological attacks. It is not clear that an office focused on “peacetime” threats will have the staffing, contingency planning capability, and crisis management capability to deal with the kind of threats posed by asymmetric warfare.
- *Nuclear, large-scale biological attacks, and infectious biological attacks require very different levels of skills.* Regardless of the federal direction of Homeland defense efforts, the technology and effects of the most lethal forms of attack are so different that any effort to manage the response must include different mixes of skills and federal departments and agencies.
- *No change in management or direction can be effective unless it resolves how to integrate the Department of Defense and US intelligence community into a Homeland Defense effort designed to deal with asymmetric threats, state and proxy attacks using nuclear weapons or effective biological weapons.* Scale is a critical issue, as is the potential need to integrate the response to attacks on the US Homeland with US action in theater or regional conflicts.
- *Effective coordination and management means effective review of budgets and future year programs.* No change in leadership or management can be effective that is not based on review authority over the budgets of federal departments and agencies, and the development and review of an integrated future year program that includes a rolling program budget that project expenditures at least five years into the future, and allows mission-orient assessment of the overall federal effort.
- *Similarly, effective coordination and management requires full review of all federal RDT&E efforts, and sufficient net technical capability to make risk assessments and carry out net technical assessments.* Technology offers major potential improvements in Homeland defense, but it must be applied as a system or systems, not a series of uncoordinated increments, and analysis of the cost to deploy technology and

means of defeating it needs far more explicit analysis than it currently receives.

- *Crisis and operations management can be required at radically different levels and involve radically different levels of planning assistance.* Anyone can be called a crisis manager. Actual crisis management is extremely difficult. The moment a crisis escalates from “conventional” terrorism to a major threat, or response to major uses of weapons of mass destruction, an effective operations command or management capability must be in place.

Broader Solutions and New Approaches to National Strategy: Reacting to Asymmetric Warfare

Finally, the US needs to close the current gap between counterterrorism and asymmetric warfare in ways which go beyond narrowly defined defense and response efforts. Homeland defense should not be defined purely in terms of reactions within the US homeland. The US must examine ways it can use its offensive capabilities to deter such attacks, and respond to them in ways that will ensure such attacks are limited in scope or do not occur in the future.

- *There is a need to revise US strategic offensive doctrine to deal with these issues.* The Cold War may be over, but the threat of CBRN attacks is not. Homeland defense should not mean that the US drifts towards a response-oriented approach or a Maginot Line-like emphasis on defense. Major asymmetric attacks must be firmly deterred, preempted or reduced in size, and firmly retaliated to. It must be clear that attacking states, and states that deliberately host terrorist movements, will be the target of US strikes directed at the nation and not simply at the leadership, and the US needs to give its theater and strategic forces this option. As part of this effort, the US must answer the following questions:
- What changes to deterrence, offensive strike capability, and retaliation really matter if states and foreign movements are involved?
- *What can be done to aid defenders in securing US borders and territory?*
- *What can be done in terms of intelligence/technology to rapidly and conclusively identify the attacker?*
- What can be done to accelerate and improve warning time for offensive/counterattack/deterrent purposes?
- When is the threat/attack one that justifies “war?” When does a civil emergency become a de facto conflict?”
- What should the retaliatory doctrine be? How lethal should the escalatory action be? How can the US best halt or punish the attacker? How can it prevent follow-on attacks? Deter future attackers?
- What strategic linkage is needed between Homeland defense and theater defense. What will act best to both defend the US homeland and enhance force protection? Protect our allies? Deter third party adventures and copycats? Cope with multiple, mixed (cocktail), and sequential attacks.
- Responding to the threats posed by asymmetric warfare also means revisions to intelligence, threat assessment efforts, arms control, and counterproliferation efforts. Once again, effective US efforts raise key

issues that go beyond the scope of this study:

- Establishing opportunities and limits for intelligence capability is critical to effective action.
- How much can targeting, precision strike, weapons effects, and BDA really be improved?
- Limiting asymmetric capability and peacetime improvements in threat characterization are critical: Limiting and monitoring technology transfer and RDT&E efforts is the first line of defense.
- What can be done to improve or replace HUMINT? Can data-mining and AI provide a new technological approach?
- The myth that expanding HUMINT efforts will help either needs to be transformed into a reality or dismissed.
- How can cooperation with our allies intelligence services and international law enforcement agencies be used as a first line of defense?
- Detection of efforts to proliferate is not enough. Homeland defense requires US intelligence to improve its capability to characterize the nature of possible attacks as precisely as possible to reduce burden on defender and responder, and help prioritize and define options for offensive/counteroffensive action.
- Nunn-Lugar is extremely cost-effective Homeland defense. It needs to be fully extended to biological weapons.
- Sanctions and arms control and export control regimes like the NPT, MTCR, Australia list, Wassener Convention, Chemical Warfare Convention, etc. may be effective tools. They too are potential tools in creating a more effective approach to Homeland defense.

¹ United States General Accounting Office, GAO Report to Congressional Requesters, “Combating Terrorism, Federal Agencies’ Efforts to Implement National Policy and Strategy,” GAO/NSIAD-97-254, September 1997, p. 15.

² GAO/T-NSIAD-98-164, “Combating Terrorism,” April 23, 1998, P. 3.

³ GAO/T-NSIAD-98-164, “Combating Terrorism,” April 23, 1998, P. 4.

⁴ National Intelligence Council, “The Global Infectious Disease Threat and Its Implications for the United States,” CIA NIE-99-17D, January 2000.
<http://www.cia.gov/cia/publications/nie/report/nie99-17d.htm>.

⁵ FBI, Uniform Crime Reports, January-June 1999, November 21, 1999. Table 4.