CSIS

Center for Strategic and International Studies
1800 K Street N.W.
Washington, DC 20006
(202) 775-3270
Updates from: CSIS.ORG, "Homeland Defense"
Comments to: Acordesman@aol.com

DEFENDING AMERICA

REDEFINING THE CONCEPTUAL BORDERS OF HOMELAND DEFENSE

HOMELAND DEFENSE: COPING WITH THE THREAT OF INDIRECT, COVERT, TERRORIST, AND EXTREMIST ATTACKS WITH WEAPONS OF MASS DESTRUCTION

EXECUTIVE SUMMARY

Final Draft

Anthony H. Cordesman
Arleigh A. Burke Chair in Strategy

FEBRUARY 14, 2001

The following report is the final draft of a book on Homeland Defense being prepared as part of the CSIS Homeland Defense project. A substantially revised version will be published as a Praeger book later in 2001.

Acknowledgements

The author would like to thank Preston Golson and Aviva Roller for their assistance in researching and editing this report

Executive Summary

The US faces growing potential threats from state actors, their proxies, or independent extremists and terrorists. While various analysts have tended to exaggerate the immediate threat, or the current threat posted by given actors, this does not mean that the threat is not real or that the nation does not need to improve its defense and response capabilities. The US must plan to defend against such threats not only to defend its own homeland, but to protect its ability to deploy forces overseas and its allies.

The practical problem is to decide how to be deal with highly uncertain emerging threats in a world where the US has limited resources, and many other priorities. The US cannot bet the lives and well-being of its citizens on today's threats and probabilities. 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. US involvement in the world, the strength of US conventional and nuclear forces, and vulnerability at home are a dangerous combination, and unless the US acts to improve both deterrence and defense, the risk of major asymmetric and terrorist attacks involving CBRN weapons is likely to grow.

Finding the right mix of defense and response is extremely difficult, however, and it is far easier to call for dramatic action than to determine what actions will really succeed and be cost-effective, and then execute them. It is 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.

Correcting the Strategic Gaps in the US Approach to Homeland Defense

At the same time, there is still much to be done. There are basic conceptual and strategic gaps in the way the US is approaching the problem. The most serious gap is the one between the Department of Defense's growing focus on the threats posed by asymmetric warfare, and by states and well organized non-state actors, and the focus of civil Departments on lower levels of foreign and domestic terrorism. At the same time, defining "Homeland Defense" in terms of defense and response against attacks inside the US understates the importance of looking at the link between theater threats and conflicts and attacks on the US, and the threats to our allies and military forces.

An effective approach to Homeland defense also means that all defenders and responders must understand that the range of threats is sufficiently great so that the US cannot plan to deal with one attack, one time. Attacks may be coupled to ongoing theater conflicts. If missile threats against the US are serious enough to deploy NMD, then defense must consider the threat of mixes of missile and covert attacks and response must consider the risk that a missile attack will penetrate any NMD defense. Multiple attacks are possible, as are sequential attacks.

The US must also prepare to deal with the "morning after." The first major covert or terrorist WMD attack on the US or its major allies may change the strategic environment fundamentally. The US must begin to both think and act in response to such risks, but a world in which actually attacks occur will be one in which the precedent is real and the US defense and response to the first attack will set the precedent to a world in which many similar threats may occur in the future.

The US must broaden the way in which it deals with "Homeland defense" to address all of the tools it has at hand. Approaches to improving Homeland defense that arbitrarily exclude US offensive and deterrent capabilities, the ability to defend by identifying and striking at hostile foreign governments and terrorists ignore an important part of Homeland defense. So do

definitions that understate or ignore the broad spectrum of US counterproliferation efforts, including arms control.

Finally, putting a new emphasis on Homeland defense is not a reason for creating a new form of isolationism. Cooperation with our allies and friendly governments can be critical in defending and deterring against asymmetric attacks by foreign states and counterterrorism. Such actions cannot defend against domestic terrorists and extremists, but they can have a major impact in reducing what may well be the most serious source of potential attacks with nuclear and effective biological weapons.

Focusing Less on Who's In Charge and More on What They Should Be in Charge of

Each president needs to create the kind of central authority that will ensure the coordination of all federal defense and response activity, develop a common strategy, coordinate program and future year plans and review budget. The precise form this authority takes – and whether it should be a cabinet or confirmed position or be placed under the President – is less important than it suited the style and needs of a given President.

At the same time, the US government needs to be less focused on chains or command and be more objective about the need to accept uncertainty and carry out the necessary research, development, and improved planning to reduce that uncertainty. Far too many studies of Homeland defense worry about the issues of "who's in charge" in the federal government, rather than the details of what senior officials should be in charge off. In many cases, there seems to be an assumption that creating the right organization chart and set of federal responsibilities can create a mix of federal authority, capabilities, and liaison efforts with state and local governments that can deal with the problem.

One does not have to be a believer in chaos theory to realize that such an approach is almost certainly wrong. No federal approach to a highly uncertain range of threats, particularly ones with consequences as devastating as attacks with nuclear and biological weapons, can hope

to develop a system that will be truly ready to deal with such threats and attacks when they actually emerge. The US government cannot and should not pay the money today to try to deal with the worst case threats that may emerge in the future, and it cannot require state, local, and private entities to assume to more than limited additional burdens.

There are many areas where basic research and planning activity is needed to resolve grave uncertainties, and others where special interest pleading threatens to waste vast amounts of public money on the wrong priorities or measures which may either be ineffective or easy to counter. There have been far more attempts to define broad strategies or issue broad directives than come to grips with the need for detailed planning, adequate programs, and program budgets, and meaningful ways to review and coordinate annual budgets and programs.

Many proposed and ongoing programs probably cannot meet the most basic tests of intellectual validity and federal responsibility. There is no long term plan, program, or program budget. There is no supporting analysis of the balance of offense and defense, the countermeasures that could defeat a given program and the cost to defeat it. There is nothing approaching an adequate ongoing national threat analysis of domestic and foreign threats, no net assessment of the overall balance of defense and offense, and no net technical assessment of the trends in offensive and defensive capability.

There is a sharp decoupling of planning to deal with major asymmetric threats that can involve states, their proxies, and more sophisticated terrorist and extremist groups in nuclear and major biological attacks from the lower-level forms of conventional, chemical, radiological, and biological attacks that are the “worst cases” today’s terrorists seem to pose, and which form the focus of most of today’s efforts to improve defense and response. These problems are compounded by major legal issues that limit key aspects of intelligence and law enforcement activities, and by efforts to improve response that are often linked to other goals like improving health services or emergency response capabilities.

Effective planning and action cannot be based itself on vague calls for improved

strategy, exercising and training based on today's threat analyses and techniques, or altering organization charts at the top. It will take years of effort to create a coordinated and effective plan for federal, state, and local action. In most cases, it is the willingness and ability to address detailed issues and to make hands on efforts to create and implement a wide range of cost-effective programs that will determine the success of the US effort in Homeland Defense and not the effort to find a few major recommendations. The devil really does lie the details, and "bumper sticker" or one-issue approaches to policy, are a recommendation for disaster.

Effective research and development efforts are needed in virtually every key area of defense and response activity, and indeed to improve the ability to use political, economic, and military actions outside the US to deter and defend foreign asymmetric and terrorist attacks. At the same time, effective research and development efforts require certain key tools that are sadly lacking in many, if not most, such programs.

There must be a comprehensive and regularly updated net technical assessment of the trends in defensive and offensive technology to establish priorities and the probable cost-effectiveness of given programs. Basic advances are needed in estimating and modeling the CBRN threat to determine what R&D activities are most needed. Each R&D program requires a clear analysis of how the end result would be deployed and the procurement and life cycle costs of deploying effective national programs. There must be a firm end to using special pleading about the merits of a program against today's threat, and the lack of program by program justification based on analysis of the trends in offense and defense, countermeasures to the proposed or ongoing R&D activity, and the cost to defeat a deployed system.

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

There is a wide range of individual areas where the US must improve its strategy and plans for Homeland defense against CBRN attacks. 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.

- *The threat involves asymmetric warfare as well as terrorism, and response must also deal with threats such as the failure of a national missile defense system to intercept more orthodox methods of attack.* An adequate Homeland defense program cannot be based on defending and responding to terrorism, extremism, or the kind of limited CBRN attacks that now seem most probable. States, their proxies, and more sophisticated non-state groups may attack as well. Advances in biotechnology may give individuals or smaller groups far more lethal weapons in the future.

- *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 and program development – particularly one that is 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 many of 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 indicated 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.
- The 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 of 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, while most terrorism can be dealt with as “business as usual.”
    - Defense/response may have to be given high priority relative to normal legal procedures and civil rights. This, however, requires both a clear and present danger as a justification, and clear safeguards to minimize any interference with civil liberties.
    - 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 will use, it is almost certain that some of these “true believers” will eventually 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, and that the overwhelming majority of “true

believers" will prove to be wrong.

Federal programs will be 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 with rigid lines of responsibility, chains of command, and standardized equipment for defense and response. 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.

Resource constraints can be particularly critical when 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.

The US may or may not get strategic warning that the risk of such attacks has increased, and of the form they will take. If it does not, it may benefit from the fact the first such attacks come against its allies or other nations. It is far from clear that the intelligence and analytic tools

exist to warn that a possibility is becoming a probability and then a certainty in time to react, and with sufficient clarity to make the US react. As a result, the US must (a) be prepared to see increasing "possibility" and not just increasing "probability" as strategic warning, and (b) recognize that it needs contingency plans to change its defense and response plans and programs the moment an attack is successful or a pattern of attack because probable.

The US cannot afford to focus on dealing with one successful attack or mix of attacks. It must consider the risk of an emerging pattern of asymmetric warfare and highly lethal terrorism, and plan for the "morning after." A mentality that treats any catastrophic attack as a strategic defeat, and that does not prepare for immediate action to deal with follow-on attacks, is a recipe for strategic disaster and an incentive for further attack. US response plans must explicitly recognize these risks and the need to assure the nation, our allies, and our enemies that we will not be paralyzed or panic even if a nuclear or major biological attack succeeds.

There are major problems in threat analysis 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 US must fundamentally reexamine its assessments of the effects of chemical, biological, radiological, and nuclear weapons in the event of various types of asymmetric and terrorist attacks*. Far to often, the US is attempting address the evolving threat and consequence of each type of CBRN attack using dated research and modeling designed for the needs of the Cold War, or which has been developed to deal with selected generic threats rather than conduct a zero-based examination of the current and potential future consequences of CBRN attacks. The modeling of nuclear and major biological attacks that underpins federal planning seems particularly weak, and particularly in dealing with (a) the impact of attacks in specific major urban areas, (b) fallout and ecological effects from a nuclear attack, and (c) biological attacks involving multiple agents, infectious agents, and tailored or genetically enhanced weapons. It is unclear that any major effort is underway to give local, state, and regional responders the ability to model or simulate a range of attacks that apply to specific areas and cities in ways that support improved defense and response planning. The efforts of the Defense Threat Reduction Agency (DTRA) are a major first step towards such efforts, but are now acutely limited in terms of resources, scale, and comprehensiveness.

- *There is little real analysis of the impact of multiple attacks, sequential attacks, and the longer-term consequences of attacks. The focus is often almost exclusively on deterring, defending, or responding to the first attack.* The US focus on terrorism, rather than asymmetric warfare, has left a major gap in the planning and analysis of Homeland defense between relatively limited terrorist use of CBRN weapons and the far more drastic threat from ballistic missile attacks. Ironically, there is almost no practical response planning for a missile attack, or any other kind of easily attributable biological or nuclear attack, although the US is considering spending tens of billions of dollars on a missile defense system that is almost certain to remain imperfect or "leak." As a result, most "worst cases" fall fatally short of being real worst cases. There is far too little analysis of the longer-term physical, psychological, economic, political, and strategic impacts of a major successful attack, or of contingencies involving multiple and sequential attacks. Truly new methods of long-term attack like agricultural or ecological attacks receive limited attention

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 simply 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 current 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 transparency and 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.*

- *Regions, state, local governments, and private entities cannot prepare in a closed environment, and there is little opportunity for feedback from outside the federal government. Equally, there is little practical way to determine the best trade-offs between federal, regional, state, and local efforts.* There cannot be an effective national partnership in dealing with Homeland defense, or basis for popular support, without a high degree of transparency as to federal efforts and ongoing discussion and debate over what needs to be done. The federal government lacks every conceivable element of the capability to plan and impose effective Homeland defense on state and local governments and the private sector. It needs constant feedback and commentary, and federal officials need to be exposed to constant challenge from state and local officials and experts, as well as analysts outside the federal government.

- *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.

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

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 serve as the focus for the defense effort, or that it can be prioritized 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 in creating standard lines of authority and responsibility. 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 acceptance of the fact 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.

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 deals with issues that are also 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 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.

- *The US must develop future year plans and coordinated program budgets.* It must develop five-year plans for on going programs, and long term RDT&E plans that include deployment plans and cost and supporting net threat assessments, for each federal department and agency. It must coordinate them at the White House level, where it will also be necessary to carry out review of relevant annual budget submissions to ensure the continued execution of federal efforts.

- *Carry out net technical assessments of the changing CBRN threat and of the technological options to improve defense and response capabilities.* Examine both the threat and federal RCT&E efforts in ways that support coordinated efforts to use technology to improve Homeland defense and response, which ensure the uncertainties in threat effects are reduced, that RDT&E efforts are tied to practical deployment plans, and risk assessments examine the cost to defeat new programs and RDT&E efforts.

- *Immediately undertake efforts that are not-resource-intensive, such as contingency planning on legal, psychosocial, and even military issues.* This planing should extend to worst case scenarios involving asymmetric state attacks, nuclear attacks, and major biological attacks, and involving the use of mixes of agents, multiple attacks, attacks against multiple cities or targets, and sequential and copy-cat attacks.

Unless this level of transparency and improve planning and programming 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.

Managing Research and Development, Rather Than Treating Asymmetric Attacks, Terrorism, and the CBRN Threat as an Excuse for 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.

- *RDT&E is not a magic bullet that should be exempt from adequate planning, programming, and program, threat validation.* Federal research and development efforts have a poor to dismal record of effective management. It is time to reverse this situation.

- *Threat analysis needs to be improved by joint efforts within the intelligence and federal RDT&E communities to create annual national threat assessments that evaluate the overall trends in threat technology and methods of attack, and to provide RDT&E planners with better, and technologically oriented threat forecasts*. This should probably take the form of an annual NIE with outside support from a task force composed of cleared RDT&E experts. It should explicitly consider the risk of asymmetric state, as well as terrorist and extremist attacks, and the linkage between the growing risk of biological attacks, the problems created by changes in the pattern of natural disease, and changes in biotechnology. Two key goals behind such an effort will be to educate the intelligence community in the impact of changes in technology, and how to improve strategic warning.

- *The US must develop and conduct ongoing annual net threat assessments of the foreign and domestic threat of CBRN attacks and terrorism.* Threat assessments are not adequate to establish the balance of evolving trends in offensive and defensive technology, and the formulation, prioritization, and execution of successful RDT&E programs.

- *RDT&E program planning and justification needs fundamental improvement at the individual program level.* As has been discussed earlier, programs should not be justified or executed without regularly update plans that examine how the technology would be deployed, the systems and training required, procurement and life cycle cost, and the required test and evaluation program and measures of effectiveness. Programs should only be carried out after examination of the probable and possible trends in the threat, the availability of countermeasures to defeat them, and the cost to defeat them. Where possible there should be independent assessments of the probability of success and the validity of the cost analysis and test and evaluation program.

It should be obvious that basic research programs require a different level of justification, planning, and programming from R&D efforts that are moving towards deployment. The basic problem, however, is that these improvements either do not now take place as programs mature or often take the form of internally managed efforts that are more designed to sell the program involved than prioritize and manage it.

Looking Beyond CBRN: Dealing with All Medical Risks and Costs, the Need for a Comprehensive Public Information Capability, and the Linkage to Improved Strategic Deterrence and Response Capabilities

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.[1]

- *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.

- *The US should not invest in more stockpiling of vaccines and medicine, improved public health measures, or other major new response efforts without far better planning, programming, and justification than it currently possesses. Similarly, no measures should be taken to suggest or require improvements in federal and military health and medical capabilities, private health care, or medical education without such an effort.* Major improvements may well be needed in all of these areas, but rushing forward in individual areas without coordinated programs can waste federal money and potentially impose massive waste on state, local, and private sector efforts. This is particularly true because many efforts are vulnerable to simple countermeasures (such as using a disease for which there is no stockpile, a mix of diseases, or tailored diseases with new symptoms or effects that make timely response extremely difficult), make the improved facility a target, or prove to be of marginal value in a limited attack or be overwhelmed in a major attack. To put bluntly, the US medical, biosciences, and emergency responses communities have an alarming tendency to demand federal money bed thrown at problems without adequate overall planning and justification, and often with motives that seem to be focused more on other priorities than Homeland defense. Focusing narrowly on the highest priority programs will almost certainly stress available funding

beyond its limits. There is no room for hobbyshops and technical adventures.

- *There are fundamental problems in medical ethics and civil rights that must be addressed at higher levels of attack*. No one really wants to address the fact that quarantines may be necessary in ways that threaten civil rights, and that overwhelming medical and response services with suspected, curable, and fatal cases will require decisions as to who lives, suffers, and/or dies, and who receives limited treatment resources, which can challenge every current practice and aspect of medical ethics. It is fundamentally unrealistic, however, not to explicitly address these issues, and unethical to place the burden without real warning on state, local, and private responders and medical practitioners.

- *A similar problem must be addressed in terms of the psychological impact of attacks, on both a short and long term basis*. There is an unresolved and critically important debate over the extent to which attacks will produce local, regional, and national panic and a host of related psychosomatic problems that may or may not be related to physical problems. Some argue for intensive treatment and care. Others argue that such careful may be unaffordable in terms of resources, and exaggerating the treat may become a self-fulfilling prophecy. Far too often, those whose focus on the psychological dimension ignore the strategic priorities the US may have to minimize the broader national impact of an attack and/or ignore the collateral problem of dealing with the long-term physical problems created by radiation and exposure to disease, toxins, and chemical poisons. This aspect of response needs a major research effort and should not be ignored simply because it is difficult and unfamiliar.

- *Practical real-time information may often be more cost-effective and save more lives than investments in medical services, biosciences, and physical response efforts*. Much of the current response effort is built around comprehensive rescue and treatment. It fails to focus on the need to provide real-time data to all of those in the area under attack, and nearby, as to what to do to minimize exposure. There is no plan to use the national broadcast information system to create a single, reliable source of data or to educate national and local media as to the need to be ready to provide help in the event of warning or execution of an attack. There are no plans to characterize attacks precisely with real time detection and characterization, to communicate specific information about whether to stay (and what physical measures should be taken), whether and how to flee, and whether to seek treatment. At high levels of attack, such measures may be far more effective and affordable than any practical investment in improved medical care and other physical response capabilities.

- *The US must address the issue of deterrence and defensive response against foreign threats, as well as the issue of aiding its allies if they come under such attack.* The US cannot afford to rely purely on internal defense and response. Attacks on the US may well escalate out of theater or regional conflicts and tensions. Foreign movements and governments need to be deterred and the US must have plans to respond to prevent attacks and limit or respond to follow on attacks. This creates new dilemmas in international law in an era of undeclared wars, as well as highlights the gap in US strategic offensive planning between counterterrorism efforts overseas, conventional warfare, and nuclear retaliation. Creating an effective political, economic, and military capability to respond to an asymmetric nuclear or major biological asymmetric or foreign terrorist may again do far more to reduce casualties than any practical investment in improved medical care and other physical response capabilities. At the same time, it raises critical issues about attribution, targeting, collateral damage, international law, and international politics that the US has only begun to address.

It should also be noted in this context that much of the current planning for medical and response treatment focuses on attacks on human beings, and not on attacks on livestock, agriculture, or the ecology. This focus probably is valid in reflecting current probabilities, but it

ignores critical possible vectors of attack and ones where hostile states or terrorists may develop steadily greater expertise and capability. Attacks on agriculture and the ecology offer a subtle form of attack, further compound the problems in attribution and response, and might be conducted as either a long-term form of anonymous attack or quite revenge long after a crisis seems to be over.

Homeland Defense and/or Law Enforcement

The US 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.[2]

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 again needs to establish its ecological and agricultural defense requirements.* The risk posed by biotechnology cannot be evaluated solely in terms of threats to human beings.

The Role of the Intelligence Community and the Need for Improved Intelligence

The previous recommendations have touched upon many aspects of intelligence, the need for improved threat assessment, the need to improve the linkage between intelligence and law enforcement and response, the need to improve intelligence for deterrence and military response, and the need for net assessments in which the intelligence community plays a major role. At the same time, there is a need for caution.

When federal planners deal with uncertainty, they tend to make impossible demands on the intelligence community for strategic warning, detection, characterization, attribution, targeting, and damage assessment. There is an almost ritual tendency to round up the usual

suspects and call for yet another strategic warning study or effort to expand human intelligence. In far too many cases, there is an effort to make impossible demands on intelligence, and/or shift responsibility without providing a net assessment of capabilities and responsibilities, the necessary resources, and/or the tasking necessary to either maintain such efforts or execute painful trade-offs between existing tasking and new tasking. Under these conditions, it is hardly surprising that experienced intelligence officers find it difficult to take such efforts seriously, and are forced to silently accept what they private regard as an irresponsible allocation of responsibility by policymakers.

No one can quarrel with the fact that virtually every commission, study group, and analyst that has examined Homeland defense calls for improved intelligence. There is broad agreement among most of the experts in the field, and they are almost certainly right. There are, however, important warnings that need to be given about each of the efforts to improve intelligence that are recommended by various experts:

- *Delegating "mission impossible" is not a solution.* There will almost certainly be serious shortfalls in warning, defense, detection, characterization, attribution, targeting, and damage assessment regardless of what is done to improve intelligence resources, capabilities, and technology. The US must not repeat the critical mistake it made in its planning for the revolution in military affairs, and place an impossible burden on the intelligence community. It must accept the fact that the fog of war will be a key problem in both asymmetric conflicts and terrorism, and plan accordingly.

- *Political, economic, and military response planning must explicitly be based on the high risk that no improvement in* defense, detection, characterization, attribution, targeting can meet peacetime legal standards in many contingencies, and the US will still have to respond immediately to a critical threat to its strategic interests. Intelligence cannot eliminate risk and uncertainty, and is very unlikely to meet all of the criteria for an idealized approach to international law. This is no excuse for reckless action, or a Homeland defense strategy based on "ready, fire, aim." It also, however, is no excuse for a political, economic, and military response plan based on intelligence and law enforcement's ability to perform "mission impossible."

- *Isolated intelligence efforts are no substitute for the fusion of intelligence, planning, and operations into a single integrated effort.* As is touched upon in more depth shortly, it has been clear since Vietnam that efforts to segregate intelligence, operations, and planning are not practical whenever joint operations are needed and the stakes demand the most quick and effective response possible.

- *Strategic warning can be improved. However, it is as much a problem in decision-making as intelligence, and it can never be relied upon or be a substitute for real time intelligence in a crisis.* The intelligence community has been tasked with improving strategic warning for nearly 40 years, and virtually every time a new strategic problem arises or the nation has not prepared for a new crisis or event. In case after case,

however, the problem remains that decisive and unambiguous warning is impossible and that decision-makers tend to ignore any warning with honest caveats and uncertainties. The reality that intelligence may also not have better access to indicators and decision-makers is ignored, sometimes in ways which try to shift the blame for failing to foresee a given crisis or event to the intelligence community. In the real world, strategic warning is a net assessment activity, the added data available to the intelligence community does not give it the gift of prophecy or a crystal ball, and no amount of warning can compensate for the policymakers refusal or inability to act.

- *Humint or human intelligence can help, but it is not the answer to warning or uncertainty.* Intelligence resource managers have every reason to cringe when outsiders call for added resources for human intelligence. Such recommendations have been made for decades and the result is almost invariably to increase intelligence tasking without providing the resources. Far too often, such recommendations are also made without an adequate understanding of just how difficult it is to improve human intelligence and make it reliable, of the level of effort and resources required, and of the need to become deeply involved with terrorists and officials in some of the world's most repressive governments.

- *Major challenges will also exist in improving National Technical Means (NTM), and the work of the National Security Agency (NSA) and National Reconnaissance Office (NRO).* The idea that resources can be freed to improve Humint by taking them from NTM requires far more validation that simple policy-level assertions. The US faces massive technical and resource challenges in maintaining the current level of NSA and NRO activity in the face of changes in technology, and they will be compounded by shifts towards asymmetric warfare, improvements in terrorist operations, and changes in CBRN technology and means of delivery. The Cold War is over, but the fact remains that there is still the same ongoing average of 25-30 conflicts in the world that has existed during every day since the end of World War II. Unless far better analysis and programming becomes available, there is no reason to assume that NTM can preserve even it current coverage with its current resources.

- *Technology is unlikely to be a magic bullet for improving intelligence, law enforcement, or operations.* Technology can greatly improve US detection, characterization, attribution, and targeting capabilities. However, far more promises are being made than can possibly be kept, and many are repetitions of promises about the same use of new sensors, detection, and characterization equipment during the height of efforts to improve technology for the war on drugs, or even in Vietnam. Far too often, promises are made about devices and new analytic techniques like data mining that bear little relation to their real world capability, availability, and cost. In some cases, the technology is being developed as a device or technique without any practical plan to deploy a system to use it or examination of such an effort's cost effectiveness. This is as true of technology for defense, response, and military operations as for intelligence. However, the compartmentation of intelligence, and the need to protect sources and means, often exacerbates these problems.

Once again, it must be stressed that improving intelligence is a vital aspect of effective Homeland defense. However, pre-delegating the blame for the failure to create effective defense is not. Neither is making promises that cannot be kept.

The Challenge of Operations

As yet, there are no clear plans to provide effective command, control, communications,

computer support, intelligence, and "battle management" (C^4I/BM) capability to defend and respond to asymmetric state and large-scale CBRN terrorist attacks of the kind that would saturate and/or destroy local capabilities to use law enforcement and emergency response techniques. There is also a tendency within the federal government to assume that agency-level coordination in Washington could substitute for the deployment of a C^4I/BM capability to the area or areas of attack, and for the fusion of all capabilities into a single operations and crisis management center.

This approach tacitly relies on pre-crisis exercises and coordination methods within the federal government -- between federal, state, and local governments – to create an effective operational capability to deal with events that require on-the-scene expertise in the field, the fusion of information and operations, and decision-making and response in real time. It may well be adequate in dealing with low to medium level threats and attacks, but it goes against all of the painful lessons the US military have learned about jointness, fusion, and the need to put operations firmly on the scene. It relies heavily on the assumption that FEMA can be restructured to improvise the needed crisis management authority in Washington and the field, and often on the assumption that the reaction times and focus of Washington-based federal coordination, coupled to federal activities elsewhere in the country are adequate to meet regional, state, and local needs in a true mass emergency.

These are exceedingly dangerous assumptions, and state and local responders have already raised challenging questions about how well federal programs can be managed that are remote from the scene and the reactions times for federal decision-making and response in a wide range of fields. There is no way to provide firm recommendations without a great deal more planning and exercise data, however, some things are clear:

- *An operations center may be needed at the federal level with an integrated command and the one the scene fusion of all the necessary expertise and decision-making authority*. Serious study is needed of exactly what kind of operations center, authority, expertise, and facilities will be needed and how to immediately tailor this federal effort to specific contingency conditions.

- *Similar examination is needed of what kind of operations center will be needed in the field, what role the federal government should play, and how to allocate federal, state, and local levels of authority and*

jurisdiction at different levels of attack. Today, there is far too great a gap between planning to use state and local authority and vague discussions of what would happen if the President should declare a state of national emergency. There is far too little study of real-world timeline and reaction requirements. Coordination is generally used as a substitute for fusion, and too many assumptions are made about what can be improvised in Washington and what needs to be immediately deployable in the field.

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.

As has been touched upon earlier, however, 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 of the Federal Effort

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 that 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. are vital parts of an effective Homeland defense effort.

They all have limits, and these limits generally are far more serious in detecting and preventing the development of small asymmetric threats and terrorism than the deployment of large war fighting capabilities. Existing arms control inspection and verification regimes can also act to license the transfer of key nuclear and chemical technologies to suspect countries or countries where terrorists and extremists operate, while they have little impact on the threat of internal terrorism and extremism in a sophisticated industrial power like the US. Nevertheless, they can be useful tools in creating a more effective approach to Homeland defense.

- The problem of controlling biological threats in the form of asymmetric warfare and terrorist attacks requires a zero-based reexamination of efforts to create an inspection regime for the Biological Warfare Convention, develop effective export and supply control regimes, and improve the detection and characterization capability of world medical facilities and the WHO. Far more open debate and net technical assessment is needed of what can and cannot be done to control the spread of biotechnology, convertible pharmaceutical and food processing equipment, and access to them. The ongoing debate between those who say control regimes are feasible and those who deny this needs to be resolved with far more objective analysis and explicit attention to the new threats that may emerge to the US Homeland.

As has been stressed at the beginning of this chapter, and throughout this analysis, the US must both take an all-inclusive approach to Homeland defense and rethink what is sometimes a near isolationist approach to Homeland defense. Much of the literature assumes that the US will be the primary target of attacks and the only scene of attacks. One classic argument is that the generic nature of the US role as the "world's only super power" makes it the primary target of foreign action. Similarly, there is a tendency to assume that US deterrence, defense, response, and political, economic, and political action can occur as part of a two person, zero sum game.

In actual practice, the US is a target of foreign movements largely as an extension of theater-driven conflicts and tensions where it is often a secondary target for state and terrorist attacks. This is certainly true today in Northeast Asia, the Gulf, and the Middle East. In many, if not most, cases involving state, proxy, and large-scale terrorist attacks, attacks on the US Homeland will be an extension of theater conflicts by other means. The US will be linked to its allies, to coalitions, to regional peace making efforts, or other critical foreign involvements. Even where this is not the case, the US will often badly need the support of its allies and international law enforcement agencies. Homeland defense is not an exercise in isolationism, and if the US does try to play a two person, zero sum game it will probably lose or pay an extraordinarily high price for its conceptual and practical failure to deal with the world it lives in.

[1] 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.
[2] FBI, Uniform Crime Reports, January-June 1999, November 21, 1999. Table 4.