CSIS

Center for Strategic and International Studies
1800 K Street N.W.
Washington, DC 20006
(202) 775-3270
Fax: (202) 466-4750
Web: CSIS.ORG

DEFENDING AMERICA

REDEFINING THE CONCEPTUAL BORDERS OF HOMELAND DEFENSE

DEFINING HOMELAND DEFENSE

ROUGH WORKING DRAFT

Anthony H. Cordesman
Senior Fellow for Strategic Assessment

APRIL 3, 2000

Copyright CSIS, all rights reserved.

Introduction

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

Copyright CSIS, all rights reserved.

I. Introduction

Defending the American Homeland has come into sharp focus in the public policy world, and for good reason. Events such as the World Trade Center and Oklahoma City bombings, the Sarin gas attack in the Tokyo subway, and the launch of a North Korean missile over Japan have focused the media and public alike on new and unwelcome vulnerabilities within the United States. Even NATO's recent bombing campaign against Yugoslavia featured a new element of warfare that points to the vulnerability of critical infrastructure within the American Homeland itself--the Serbian information attack on NATO's web-site. These threats are compounded by the rise of domestic extremism and terrorism, and risk that domestic threats with use biological and chemical weapons or attack critical domestic vulnerabilities.

The emerging threats to the US homeland have a highly diverse character, and can take many different forms. In many cases, even the best defense against one threat will do nothing to reduce the threat from another. In fact, improving defense against one threat may simply lead hostile powers and movements to shift to the area where the US is still vulnerable. Effective missile defenses may, for example, lead to a concentration on covert attacks. Furthermore, threats can be domestic as well as foreign, and some threats – like information warfare – do not provide any of the tangible warning signals of past threats.

In other cases, a hostile state, terrorist group, or extremist activists may use a range of different threats at the same time to threaten or attack the American Homeland. There are no rules that bind future attackers, and hostile states may even threaten to use one form of attack while actually executing others. For example, a power may threaten to launch missiles but actually execute the covert delivery of biological weapons. A hostile power may negotiate on the one hand and use a proxy to attack, just as Syria has negotiated with Israel over the Golan while using the Hizbollah in Lebanon to force Israel into a low-level border war in an effort to halt covert infiltration and terrorism. There is also a linkage between Homeland defense and the defense of our forces overseas and our allies. Attackers may choose the most vulnerable link in our position and defensive capabilities, whether it is domestic or foreign. Alternatively they may combine attacks on the homeland with attacks on US forces overseas or on our allies.

This makes it extraordinarily difficult to assign both a probability and a priority to any given threat. It also illustrates the dangers of adopting any strategy for Homeland Defense that focuses on one or more threats but leaves the US vulnerable to others. Missile defenses alone, for example, may end in doing little more than pushing attackers into trying to deliver weapons of mass destruction by covert means. Defenses against physical terrorism may drive attackers to emphasize information warfare. The US cannot choose the form of attack that will be launched against it, and it must assume that its opponents are intelligence and will make use of the fully range of possible forms of asymmetric warfare.

In some key cases like missile defense, the deployment of a Homeland defense system risks solving one set of problems only at the cost of creating new and potentially more serious ones. The deployment of a National Missile Defense system, for example, could well force the US to either renegotiate or withdraw from the ABM Treaty. The end result might be to block the US and Russian implementation of START II and III, leaving far more nuclear weapons on line and targeted against the US while providing only limited defense capability against limited potential

Copyright CSIS, all rights reserved.

threats like Iran and North Korea. Similarly, a National Missile Defense system might provoke China into developing a larger nuclear threat against the US than would otherwise be the case, again offsetting increased protection against limited threats with a great threat from other nations.

It is far easier to postulate threats than it is to deploy effective solutions. There are serious uncertainties regarding what kind of Homeland defense is cost-effective. In a number of cases, the technology is not yet available in deployable form to provide suitable defenses, and it is not clear when it will be. Many current research and development programs are virtually open-ended, and are managed as technology programs with little effort to examine potential deployment and operating. Virtually every aspect of Homeland Defense raises major issues regarding the cost-effectiveness of any given solution, some of which cannot be resolved without years of further research.

One thing *is* clear. It is far easier to call for new Homeland Defense efforts than it is to pay for them. The US has already taken a peace dividend that has left is military forces with severe modernization and readiness problems, and involved it in a wide range contingencies that strains its power projection and deployment capabilities. In spite of a boom economy, the US also faces serious long-term strains on the federal budget and on state and local budgets as well. There is no slack in the defense budget that can be used for Homeland Defense. The burden of a steadily growing mix of entitlement expenditures and the search to reduce civil expenditures and taxes means there is little political readiness to increase spending of any kind. New programs will either require a major increase in real defense spending over a period or decades, or force painful trade-offs that reduce other US defense capabilities. It is easy to cry wolf, it is extremely difficult to find anyone willing to pay for the shepherd.

This presents serious additional problems in making the right trade-offs. US power projection and nuclear offensive capabilities are a power deterrent to attacks on the American Homeland and often offer the ability to directly threaten potential foreign attackers. This makes both US conventional and nuclear forces an important element of Homeland defense, as well as tools that serve a wide variety of other American strategic interests. Alliances offer the US additional protection against foreign threats, terrorists, and extremists. They are as a means of containing such threats and often provide forward bases for attacking them. It is true that the best defense is both a strong offense and a strong defense, but if trade-offs have to be made, they do not always favor Homeland defense on American soil. This is often ignored by the advocates of specific forms of Homeland defense. For example, there is little analysis of the potential cost trade-offs between National Missile Defense and US power projection and nuclear offensive capabilities, or between efforts to contain rogue states with theater missile defenses and to contain them with National Missile Defenses.

Potential risk is often confused with both probable risk and avoidable risk. Many threat analyses are long on worst-case possibilities and short on actuarial probabilities. The grim fact remains, however, that all risks must eventually be dealt with in terms of probability as well as potential lethality. It is not enough to cry wolf, even if wolves are real and potentially hostile. It is not enough to postulate major threats to the US Homeland even if such threats are both

Copyright CSIS, all rights reserved.

credible and possible. The US must take a coherent approach to the emerging threats to its territory, not defend in one area and leave gaps in others. It must not adopt strategies and doctrines it cannot implement or fund, and it must take a realistic approach to either seeking increases in federal, state, and local budgets or making painful trade-offs by reducing expenditures in other areas.

Furthermore, the United States can only hope to afford and implement a coherent Homeland Defense program if it makes wise choices and purses them with some consistency. The US must continue to react to changes in the threat, but it cannot afford to lurch from one approach to another, making false starts and expending resources without buying real defensive capabilities.

This report examines the current state of progress in each of the areas that threatens US territory. It examines the current state of organizational and research efforts and makes recommendations as to the integration and prioritization of the threats, the proper organization required to develop an integrated approach, and the required programs and budget. It makes recommendations that cut across well-established analytic and bureaucratic lines, and suggests cost-benefit decisions and trade-offs that many will find difficult to accept. It also outlines areas where there are serious uncertainties that must be resolved over time. Homeland defense is a an evolving problem, and one which can change suddenly and virtually without warning from a wide range of potential threats to one or more very real threats or actual attacks.

A. The Changing Post War Threat

The world has not grown more violent since the end of the Cold War, nor is it clear that the US faces any near to mid-term prospect of a threat equal to the nuclear threat posed by the former Soviet Union. If one examines a recent analysis of the conflicts that occurred in the world after World War II and before 1994, one finds the results summarized in Table One:[1]

Copyright CSIS, all rights reserved.

Table One

Patterns in World Conflict: 1945-1994

	Number of Wars	Number of Wars Involving Over 10, 000 Dead	Number of Wars Involving US Military Action*	Total Dead
Caribbean and Latin America	19	6	8	477,000
Middle East and North Africa	19	11	9	993,000
Sub-Saharan Africa	26	15	5	4,177,000
Europe	6	0	0	186,000
Central and South Asia	10	6	1	2,857,000
East Asia	34	17	6	10,396,000
Total	114	55	29	19,086,000

* Includes significant US military assistance, covert action, demonstrative action, occupation, humanitarian efforts, combat, and emergency evacuations.

It is important to note that well over 75% of these conflicts and deaths occurred before the end of the Cold War. It is equally important to note, however, that the number and intensity of third world, ethnic, racial, and religious conflicts has not decreased since the end of the Cold War.[2] The patterns of global conflict are scarcely constant, but the levels since 1990 in no way depart from the levels between 1946-1989.

A Unsafe and Unfriendly World

At the same time, the world is neither safe nor friendly. The US continues to face the threat of major regional conflicts with powers like Iran, Iraq, and North Korea. These nations are proliferators that are developing weapons of mass destruction and which may acquire long-range missiles that can reach the United States. While these regional threats may end or be reduced with time, there is no guarantee that new regional threats will not emerge. China is a case in point, but history is warning that the emergence of new threats is (a) unpredictable and (b) inevitable.

Some of these powers are acquiring significant numbers of weapons of mass destruction, and may acquire long-range ballistic and cruise missiles that can be fired at targets in the United States. Russia remains a major nuclear power and presents the risk of accidental missile launches against the US; China is modernizing its missile force, including ICBMs and SLBMs that could hit American targets. Iraq has shown that a nation can suddenly launch missiles at a nation supposedly outside the focus of a conflict, such as Israel, and other new regional threats to the

Copyright CSIS, all rights reserved.

US have demonstrated that they are willing to take more risks than the FSU. One of ironies of the end of the Cold War is that deterrence may be far less stable than it was at the height of the East-West arms race, even though the scale of potential attacks on the American homeland has diminished.

There are many nations that have developed extensive capabilities for covert warfare, and are sponsors of both state terrorism and supporters of terrorist and extremist movements. The US engagement in peacemaking, ending humanitarian crises, and preserving regional stability means that the US is also engaged in nearly constant confrontations with hostile foreign governments and movements that are capable of covert or terrorist attacks.

This is not a new development. The US has had to use force over 240 times since the end of World War II, often in unpredictable and low-level actions against nations and movements capable of covert or terrorist attacks in the US. The end of the Cold War has inevitably freed the US to engage in more peacemaking activities. The US Army, for example, has deployed ground troops 36 times since 1989 – largely in peacekeeping missions. This compares with 10 times during the previous 40 years of the Cold War, including deployments for Korea and Vietnam. Table Two illustrates the patterns in recent peacekeeping activity, and it is a warning that the US is likely to remain engaged in such operations for decades to come.

Engagement does, however, open up the prospect hostile states and extremist movements may react by attacks on the American Homeland. The incentive to launch such attacks on the US is reinforced by two factors. First, the collapse of the Former Soviet Union has left regional powers, smaller hostile states, and many extremist movements without a superpower sponsor. They cannot turn to any direct rival of the US for protection, arms or military assistance. Second, US success in creating the most effective conventional forces in the world, in exploiting the revolution in military affairs, and in creating a near-monopoly on global power projection capabilities means that few powers can challenge the US in conventional combat on even a regional basis. The choices are asymmetric warfare or defeat.

Copyright CSIS, all rights reserved.

Table Two

Frequency, Duration, and Intensity of Recent Peacekeeping Operations

Peacekeeping Activity	Number of Activities	Duration in Years		More than 10,000 Peacekeepers Involved	Some Combat Activity*	US Involvement
		Over Two	Over Five			
Current UN Operations	17	14	11	0	3	5
Past UN Operations	27	23	6	5	7	7
Current Non-UN Operations	6	5	1	1	3	2
Past Non-UN Operations	5	2	1	1	4	1
Total	55	44	19	7	17	15

* Generally very low-level or indirect involvement during fighting between principals.

Allies, Neutrals, and Foreign Defense

The developments also create important linkages between Homeland and foreign defense. Few foreign threats will affect the US alone. Most will also affect the allies of the US in a given action region, confrontation, or coalition. The lines between foreign and Homeland defense will often be blurred, and the US may often find that the best form of Homeland defense is to work with allied powers to contain or end such threats while they are still overseas. At the same time, the US cannot expect its allies to accept major threats or attacks on their homelands while the US protects itself or limits its vulnerability in ways they cannot match. Homeland Defense probably does not require parity to allow the US to maintain its security structure overseas or ensure the availability of allies in coalition warfare, but allied nations are not likely to tolerate massive disparities. In fact, the failure to provide allied states with appropriate capabilities may lead them to either be intimidated by hostile regional powers or to take action like acquiring their own missiles and weapons of mass destruction.

Every step forward in Homeland defense will have an impact on the global arms race and the attitudes neutral powers and nations that are potential, but not current threats. A strong defense will often be a useful deterrent, but it may also provoke. Powers like Russia and China may see defenses like strategic missile defense as a reason to maintain or increase their capabilities to launch missile forces and other strikes that can overwhelm US defenses – not because they are necessarily hostile, but because they will not accept unilateral vulnerability and further reinforcement of America's status as the only global superpower. Homeland defense is already having a major impact on Russian and Chinese nuclear programs, the START II and III Treaties, and the future of the ABM Treaty.

These points are crucial because they again affect any trade-offs the US must make between improving its Homeland defense capabilities and foreign defense. Homeland defense

Copyright CSIS, all rights reserved.

does not simply mean action on US territory. It means a mix of capabilities that combine activity in the US with activity overseas. Furthermore, the US cannot afford an imbalance in these capabilities. Strong US and allied capabilities overseas, and weak US defenses, create a major incentive to strike at US territory. Strong defenses on US territory, and weak defenses overseas, confront our allies and partners with the fact that the US is asking them to take risks that it will not assume for itself. Given the fact that some of these risks will be existential, many nations will not accept such a partnership.

Domestic Threats

Not all threats, however, come from abroad. The US has tensions and problems of its own, and domestic extremists and terrorists. The Oklahoma City bombing is a very real example of the fact that violent individuals or groups lash out at American society or at the American process of government. Such attacks can use conventional weapons and high explosives to strike at the most vulnerable points in the US, including utilities, courts, government offices, stock markets, political centers, the media, and symbols of American history and culture. It is also all too clear that domestic terrorists and extremists can manufacture biological and chemical weapons, and potentially launch vastly more lethal attacks in the future.

Uncertain Threats for Homeland Defense: Narcotics and Organized Crime

Changes in technology are also creating new forms of threats. The US is becoming increasingly dependent on computers and complex information systems at virtually every level of its government, economy, and society. The result can be direct physical attacks on such systems, but it can also be a new form of electronic warfare that uses other computers to launch attacks directly within an information system. This kind of “information warfare” can be used by states, foreign extremists and terrorists, domestic extremists and terrorists, foreign and domestic criminals, and casually by hobbyists and hackers. It is perhaps the only emerging threat to the American Homeland where an attack can be the result of moral indifference rather than deliberate hostility.

Two other threats are also sometimes included in Homeland defense. One is the threat posed by international crime. Another is narcotics. Both present very real and ongoing threats to the US that already have force federal, state, and local agencies to respond. Narcotics, in particular, involves massive government activity. The total street value of imports is estimated to be $*** billion a year. The cost of federal, state, and local efforts to halt the traffic in narcotics is estimated at $*** billion a year, and the social cost of dealing with the medical and treatment cost of narcotics at $*** billion a year.

This study does not examine these two threats in detail, not because they are not important, but because including them in “Homeland Defense” risks making international law enforcement part of a set of threats that are different in character and which involve deliberate acts or war or violence against the territory of the US. The dividing line, however, is a thin one.

Copyright CSIS, all rights reserved.

Many terrorist movements already have some link to the traffic in narcotics. Drug smugglers and international criminals can be used as proxies or mercenaries by foreign states or terrorist movements. Designer drugs could conceivably be a form of biological weapon, and the practical difference between extremist and criminal use of information warfare is non-existent.

B. The Problem of Assigning Priorities for Action

These risks confront the US with the following major types of threats to its Homeland or territory:

- Direct military attacks on the US using long-range delivery systems and weapons of mass destruction,
- Foreign terrorist or covert attacks using weapons of mass destruction,
- Foreign terrorist or covert attacks using more conventional means.
- Domestic terrorist or extremist attacks using weapons of mass destruction,
- Domestic terrorist or extremist attacks using conventional means.
- Domestic or foreign use of information warfare.
- The use of international crime and/or narcotics trafficking to attack the US.

This is an extraordinarily wide spectrum of threats, and most are emerging threats whose future character, probability, and impact is difficult to estimate. It is easy to create a wide range of possible worst case contingencies under each threat, as well as interactive mixes of such threats. In practice, however, the US cannot possible response with a form of Homeland defense that can deal effectively with all of these threats and every worst case. Homeland defense is quite literally a problem where in the worst case, we are all already dead.

Even a focus on more probable cases, however, presents serious problems. The threats interact and the US may face more than one threat simultaneously. One hostile power may exploit a crisis generated by another. Distinctions between kinds of terrorists and extremist threats are always uncertain since the leap from limited attacks to large-scale conventional attacks or the use of weapons of mass destruction is not predictable.

Each threat is evolving rapidly and the future form threats take is likely to respond to US efforts to improve its Homeland Defense capability. Improved ballistic missile defenses, for example, may push hostile states toward covert attacks or the use of cruise missiles. Terrorists and extremists will look for the points of greatest vulnerability, and any gaps and imbalances in Homeland defense will become the natural targets of threat seeking to create countervailing power and exploit asymmetric warfare.

Copyright CSIS, all rights reserved.

Each threat also involves major technological uncertainties. There is a race between the offensive and defense in most of the related technologies whose outcome is unclear and unstable, and the threat is certain to evolve to respond to any improvement in US Homeland capabilities and focus on the areas where the US remains vulnerable. The mix of threats in each category is likely to change sharply over the next 5-15 years. For example, low cost cruise missiles, advanced genetic warfare, new information systems, and steady changes in the volume and nature of global trade are all almost certain to alter the kinds of threat the US faces. This means that any defensive response must change as well, and programs must be flexible. They must be designed to deal with changes that are inherently unpredictable, which can occur without warning, and whose course is then event-driven rather than follows some logical course.

The problem of shaping a coherent response is further complicated by the fact that the casualty and damage effect of many threats is also unknown. It is possible to speculate with considerable expertise on the possible impact of nuclear-armed missile attacks in terms of prompt casualties, but little is known about the long-term impact of fall-out or the real-world impact of biological weapons and much depends on the specific form of weaponization. These same uncertainties affect terrorists attack using weapons of mass destruction, or which use more conventional means to attack critical targets in the US economy, strike at the security of our population and our ability to maintain civil freedoms and human rights, or strike at symbolic targets like historical centers. It is easy to postulate the impact of such strikes, but there is little empirical evidence. Information warfare creates whole new areas of uncertainty. Crying wolf is easy, but there is no reliable way to determine the severity of the wolf's bite.

C. Finding the Right Trade-offs in Terms of Budgets and Programs

The one thing that is certain about Homeland Defense is that the US is going to have to make hard choices as to the level of Homeland Defense capability it can afford, and explicit choices between improvements in direct Homeland Defense capabilities and other security considerations. In many cases, it is also going to have to make hard choices between civil liberties and defense, and between improvements in Homeland defense and cuts in other defense and civil programs. These problems will be compounded by the fact that choices will have to be made between improving defenses and alliances overseas to provide a barrier to attacks on the US, creating deterrents that do not provide defense per se but limit the probability of an attack, and providing direct defense. These are not public policy choices the US is familiar with, or has previously made, and they will at best involve a considerable degree of uncertainty.

In an ideal world, the US could approach Homeland Defense from the viewpoint of some master architecture that would assign a stable set of priorities and goals, design a program to implement them, and fund them according. In practice, the US can develop a Homeland Defense program based on the best estimates it can make today, but it will then be confronted with having to perform an evolutionary process of triage. It is also virtually certain that any program it can afford will have important gaps and weaknesses until it becomes much clearer as to what threat threats will actually materialize and in what form. Today, there are multiple threats with

Copyright CSIS, all rights reserved.

uncertain probabilities. Everyone's favorite threat cannot be critical or have the highest priority. Furthermore, it now seems certain that that the US cannot afford or implement a seamless, leak-proof, or highly effective defense against all of the major threats to the Homeland at any point in the foreseeable future, and that it cannot approach high levels of security in any one category of threat at any point in the next 10 years.

Continued near to mid-term risk is unavoidable and inevitable. The US cannot afford to over-react to threats which may be repellant or horrific in character, but which are of low probability or which have no more actuarial consequences than the kind of natural disasters that are a constant occurrence. It cannot give Homeland defense a higher public policy priority than other risks with equivalent impact.

This means that the US response must consider actuarial and not absolute risk, the cost-effectiveness of given Homeland defense measures in a wide range of applicable scenarios, and whether investment in direct Homeland defense really offers more benefits than the same investment in strengthening counterproliferation and counterterrorism activities overseas, improving foreign intelligence collection and warning, and reinforcing nuclear and conventional deterrence against a spectrum of foreign threats.

At the same time, the US cannot afford to under-react. There are many areas like public health and reactions to natural disasters where limited expenditures on new programs may create a natural synergy between Homeland defense and other public policy goals. The US must also prepare now for sudden catalytic changes in the threat. For example, it is one thing to consider a threat like biological terrorism as one of many potential events; it is quite another to confront a sudden series of actual attacks that make that threat real and a new paradigm for US security planning. The same is true of new missile threats to the US, or a sudden series of major information warfare attack on the US or its allies.

In practice, this means that the US needs programs that deal with the most urgent threats as quickly as possible, but must often accept limited levels of initial or pre-crisis capability and must rely more on deterrence than effective defense. It means steadily building on existing capabilities and strengths, and in means developing programs that have a well-tailored research and development component to determine the cost-effectiveness of more effective solutions. Britain has called the search for such trade-offs "suboptimization theory." In essence, its means breaking the analytic effort to determine the proper program into manageable efforts that can support a budget and program that is flexible and adaptive, rather than committed to a given series of efforts.

This emphasis on clearly defined programs with estimated deployment times, effectiveness levels, and costs is not one of the strengths of most of today's nascent Homeland defense programs. Many are highly politicized, threat-oriented programs that have not be subject to normal planning and programming constraints. In many cases, "research" has been used as an excuse for not carrying out more than vague conceptual deployment planning.

In other cases, program managers have been allowed to develop proprietary or program-

Copyright CSIS, all rights reserved.

specific cost models that almost invariably minimize costs and the probable impact of the real-world problems in deploying, refining, and supporting real-world programs. A great deal of the test and evaluation procedures being used or proposed raise extraordinarily serious questions about their validity and the level of independent review involved.

In some cases, minimal and self-serving test and evaluation procedures are being used to evaluate extremely complex and innovative programs; historically, such efforts have almost inevitably proved to be analytic, planning, and program disasters. There is a lack of explicit and independent risk analysis at both the technical and strategic level, and many programs are briefed without an explicit analysis of how they fit in with other or competing programs, and of the countermeasures and costs to defeat the Homeland Defense capabilities they provide.

Correcting this situation is one of the highest priorities for effective Homeland Defense, but it is totally unrealistic to assume that this can be accomplished in less than half a decade, or that all Homeland Defense efforts can somehow wait until they can be effectively managed. Any such effort would ensure that Homeland Defense would lag behind the threat, and a major cap between the quality of the technology being developed for defense and the quality available for the offense.

"Evolutionary triage" is not likely to be popular with either those who decry the existence of new threats and any added spending on defense. Any one who takes the ideological position that the US does not need Homeland defense will find good and valid reasons to challenge the probability of a given threat and the cost-effectiveness of any response. At the same time, such an approach to allocating resources is likely to be equally unpopular with those that focus on a given threat and/or a given solution. Advocates who only consider the worst case impact of proliferation or terrorism will not be satisfied with any strategy that does not poor resources into dealing with their particular threat. Ironically, neither Dr. Pangloss nor Chicken Little are likely to accept the need for a program filled with half-measures and uncertainties and driven by change.

However, such a program is the only program that is organizationally, financially, and technically feasible. It is also a program that may be easier to implement than many think. The US has already made a powerful start towards implementing various elements of such a program in many diverse areas. These efforts may lack coordination, but they often represent the state of the art in individual areas, particularly if real-world resource constraints are taken into account.

Furthermore, the fact that the US will remain vulnerable even if it does implement a Homeland defense program is neither new nor a reason not to act. The US faced a massive threat to its Homeland from Russia throughout the Cold War. If the US has many vulnerabilities, it also has many strengths. The US has near monopoly on power projection. It is the only nation in the world now capable of implementing much of the "revolution in military affairs," It leads in terms of global alliances and the capability for coalition warfare, still has strong nuclear forces, and is the world's preeminent technological power. The US can build its approach to Homeland defense on both the world's strongest deterrent and the world's greatest capability to use technology to counter threats to its territory. In short, the perfect is the enemy of the good, the

Copyright CSIS, all rights reserved.

search for stable integrated approach is the enemy of the possible, and ideology is the enemy of the art of the practical.

The Starting Point

It is difficult to provide any precise estimate of what the US is already doing to develop and improve its homeland defense capabilities and is spending on programs that can contribute to Homeland The United States federal budget is not organized or structured to support functional program analysis even within a single branch of government. It uses an input-oriented budget whose roots date back to the 20th century, and where departments and agencies normally only report their planned expenditures for one year in the future – the coming fiscal year. Program descriptions are often limited or inaccurate. Program and budget analysis is even more difficult when programs become fashionable, which is the case with Homeland defense. Departments and agencies often tailor existing programs or functions to seek resources under new names. This is so much an art form with the research and development community that recycling technology programs under new names has become a "science."

There is no requirement that agencies examine the efforts of other agencies in detail, particularly when there involve new or developmental programs. OMB provides a limited review of such activity, but more to prevent direct duplication than develop coordinated programs. The few Departments that do have detailed program budgets classify them largely to avoid outside challenges and criticism. There is, for example, no valid reason that the Department of Defense classifies more than a small portion of its Future Year Defense Program. This is done solely for bureaucratic self-defense and convenience.

Even if such data were available, they would not include the deployment costs of many new options for Homeland defense. Such deployment is not yet programmed and the cost estimates of the federal government tend to be a self-serving travesty. Worse, massive cost escalation is virtually the rule for innovative programs, usually compounded by long delays in delivery and deployment and major cuts in effectiveness. The B-1B is a classic case in point where a project touted as meeting all its performance goals on time and at cost, has still not fully met its original performance goals 15 years after deployment and where past and currently programmed "fixes" have raised its real cost by well over 50%. The debate over the F-22 is another case in point: The cost per aircraft has risen from around $60 million to around $200 million. No public policy analysis can ignore the fact that the US government can neither estimate nor manage the costs of new programs with anything approaching meaningful accuracy.

Many aspects of Homeland defense also involve state, local, private sector, and NGO activity. In most cases, such programs must have other functions. This is particularly true of counter-terrorism and virtually every program that involves a reaction to an attack on the American Homeland. Law enforcement, emergency services, disaster relief, and reaction to catastrophic accidents and natural catastrophes all contribute to Homeland defense. Few such expenditures can be ascribed to Homeland defense. The most that analysis can hope to do is to make rough estimates of the incremental cost of new programs that are dedicated to providing

Copyright CSIS, all rights reserved.

added Homeland defense capabilities to existing state, local, private sector, and NGO activities.

Fortunately, a high degree of accuracy is unnecessary and pointless. It is unnecessary because a Homeland defense effort must be managed largely in terms of new and incremental programs. It is pointless because programs are constantly evolving and changing, and today's costs – even if they could be known precisely – will not be tomorrow's – much less the costs and cost estimates of 2010. At this point in time, it is also almost axiomatic that if there is no effective federal effort to create a program, no effective state, local, private sector, and NGO program exists. The level of federal effort is in no way a measure of the ultimate cost of effective action, but it is a valid way of determining the broad trends in current overall activity.

Table Three provides a rough estimate of the level of current federal activity, based on reporting in the federal budget, and reporting by federal departments and agencies. It also provides rough estimates of the cost of effective programs where these have been estimated, plus a "factor of three" figure which simply trebles the government estimate to provide a rough illustration of the true cost to the federal government might ultimately be. There is no way to provide an analytic defense of such a guesstimate, or to support it with detailed regression analysis. On the other hand, there is no way to provide an historical defense of past federal program cost estimates.

Table Three

Federal Homeland Defense Programs: A Guesstimate
(in FY2000 $US Billions)

Threat	Agency	FY	Spending	Source
Counter-terrorism	**DOD**	1995		
		1996	$3244.2 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1997	$3671.1 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1998		
		1999	$3900 m	US Budget FY 1999 Pg 136
		2000		
		2001		
	DOE	1995		
		1996	$1324.7 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6

Copyright CSIS, all rights reserved.

		1997	$1420 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1998		
		1999		
		2000		
		2001		
	DOJ	1995	$171 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1996	$332 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
Counter-terrorism		1997	$451 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1998		
		1999		
		2000	$838 m	
		2001		
	FBI	1995	$256 m	
		1996		
		1997		
		1998	$581 m	
		1999	$609 m	
		2000	$498 m	
		2001		
	DOS	1995	$169.4 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1996	$161.5 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1997	$162.5 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1998		

Copyright CSIS, all rights reserved.

		1999		
		2000		
		2001		
Counter-terrorism	**DOT**	1995	$95.9 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1996	$115.6 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1997	$296.8 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1998		
		1999		
		2000		
		2001		
	DOH	1995		
		1996	$7 m	GAO Report December, 1997, Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination, Pg 6
		1997	$13.8 m	www.hhs.gov/proorg/asmb/budget/fy99budget/pdffiles/1999pr.pdf
		1998	$10 m	www.hhs.gov/proorg/asmb/budget/fy99budget/pdffiles/1999pr.pdf
		1999	$160 m	GAO Report March, 1999, Combating Terrorism: Observations on Federal Spending to Combat Terrorism, Pg 5
		2000	$230 m	GAO Report March, 1999, Combating Terrorism: Observations on Federal Spending to Combat Terrorism, Pg 5
		2001		
Narcotics	**DOD**	1995		
		1996		
		1997	$940 m	
		1998	$831.6 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html
		1999	$937.1 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html amount enacted

Copyright CSIS, all rights reserved.

		2000	$954.6 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html amount requested
		2001		
	DOJ	1995		
		1996		
		1997	$6703.7 m	http://www.whitehousedrugpolicy.gov/pdf/sum_pt1.pdf Pg 17
		1998	$7340 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html
		1999	$7708 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html amount enacted
		2000	$7895.8 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html amount requested
		2001		
Narcotics	**DOT**	1995		
		1996		
		1997	$526.7 m	http://www.whitehousedrugpolicy.gov/pdf/sum_pt1.pdf Pg 17
		1998	$538.8 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html
		1999	$821.4 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html amount enacted
		2000	$624.6 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html amount requested
		2001		
	Treas	1995		
		1996		
		1997	$1175.9 m	http://www.whitehousedrugpolicy.gov/pdf/sum_pt1.pdf Pg 17
		1998	$1346.5 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html
		1999	$1659.4 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html amount enacted
		2000	$1454.4 m	www.whitehousedrugpolicy.gov/policy/99ndcsbudget/table4.html amount requested
		2001		
Information Warfare	**DOD**	1995		

Copyright CSIS, all rights reserved.

		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
	DOE	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
	DOJ	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
	FBI	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
Information Warfare	**DOS**	1995		
		1996		
		1997		
		1998		
		1999		

Copyright CSIS, all rights reserved.

		2000		
		2001		
	DOT	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
	Treas	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
International Crime	**DOD**	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
	DOE	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
	DOJ	1995		
		1996		
		1997		
		1998		

Copyright CSIS, all rights reserved.

		1999		
		2000		
		2001		
	FBI	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
International Crime	**DOS**	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
	DOT	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		
	Treas	1995		
		1996		
		1997		
		1998		
		1999		
		2000		
		2001		

Copyright CSIS, all rights reserved.

Near-Term, Mid-Term, and Long-Term Options.

There is no way to draw a similar chart based on the currently projected program budgets of the US government in these areas. First, the US government does not publish such data in unclassified form. Second, there is no evidence that any effort has been made to make detailed inter-departmental comparisons of existing spending in most areas or to identify both dedicated and related programs. As a result, there is nothing like a Future Year Defense Program (FYDP) for Homeland defense.

Even if there were, such a FYDP would only identify existing programs, which generally have a high research and development content. The cost of actually deploying given solutions and defenses is often unknown or a subject of intense debate. For example, estimates of the cost of the current strategic defense program range from $*** billion to $*** for a one complex defense and from $*** billion to $*** for a two complex defense. There are no detail cost estimates for the deployment of an effective program to deal with terrorism, either conventional terrorism or terrorism using weapons of mass destruction. This is equally true of both defenses and response costs. Similar uncertainties affect the cost of any program to defend against information warfare.

One of the potential lessons of this situation is that the Federal government needs to look beyond its individual program efforts, develop an overview of its current and planned spending, and then begin to insist that its Departments and program managers provide a regularly updated estimate of the cost and effectiveness of actually deploying the programs they are working on. There is little evidence that Homeland Defense needs more rhetoric. It is clear that it needs more planning and management.

A survey of current estimates of program costs does, however, provide some insights into the range of possible costs:

Copyright CSIS, all rights reserved.

Table Four

Range of Current Estimates of the Cost of Federal Homeland Defense Programs:
(in FY2000 $US Billions)

Threat	Range of Costs	Program Summary	Source
Direct military attacks on the US using long-range delivery systems and WMD			
Foreign terrorist or covert attacks using WMD			
Foreign terrorist or covert attacks using more conventional means.			
Domestic terrorist or extremist attacks using WMD,			
Domestic terrorist or extremist attacks using conventional means.			
Domestic or foreign use of information warfare.			
International crime			
Narcotics trafficking.			

D. Determining the Relative Role of the Federal Government, State and Local Agencies, the Private Sector, and Private Citizens.

Virtually all of the previous cost estimates focus on the federal role in Homeland Defense. Federal action, however, is only part of the response the US must make to the new threats to its Homeland. State and local law enforcement officials and National Guard units must deal with many aspects of terrorist and extremist threats, regardless of whether these are foreign or domestic. Much of the emergency response capabilities of the United States consists of state

Copyright CSIS, all rights reserved.

and local capabilities, plus a substantial capability in the private sector, charitable organizations, and NGOs. The operators of key infrastructure functions, like utilities, must create both much of their own defense capability and much of any response. The same is true of the operators of virtually all information systems.

Effective Homeland Defense requires that state and local authorities be organized and trained to work with the federal government. It also requires the funding of the proper capabilities, and that these capabilities exist throughout the US in ways that are interoperable and that support effective joint action by the federal, state, and local governments. This latter point is critical. No amount of task forces, coordinating bodies, and reorganization can substitute for a lack of investment in the proper training, facilities, and equipment. Rhetoric and committees are never a substitute for real-world capabilities, and they will be tragically ineffective against the more serious threats to the American Homeland.

At present, far more has been done to deal with rhetoric and organization than to create real-world capabilities. Moreover, it is extremely difficult to measure both what level of activity state and local authorities have underway, and what kinds of capabilities they have that might be adaptable to Homeland defense. Enough preliminary training and organization has taken place to show that law enforcement officials can play a major role in tracking down terrorists and defending against them. It is clear that properly trained state and local health and emergency response teams can play a major role in reducing casualties and repairing damage. At the same time, it is clear that capabilities different sharply by state and locality, that state and local authorities are only beginning to address the issues involved, and that major new investments may be needed in training and equipment.

These issues can only be addressed by a comprehensive survey and examination of state and local capabilities. Such a survey, however, requires a clear picture of what capabilities are required, and what overall strategy the US should pursue. At some point, hard choices must also be made as to what programs and capabilities must be mandated by law and regulation, and of how to verify compliance and proficiency. This raises questions about who should fund such efforts, and questions about the proper balance between federal authority, state and local independence, and legal and human rights. It is easy to call for dramatic and decisive action. The problem lies in finding out what action is really needed, making the best use of existing capabilities, funding new activities, and ensuring that Homeland defense does not become the problem, rather than the solution.

E. Determining the Role of the Private Sector

It is equally important that clear guidelines be established for the private sector and to ensure the rights of American citizens. In the case of the private sector, hard choices have to be made regarding the responsibility of the private sector for the defense of its operations and for any emergency response.

For example, utilities are already responsible for designing their facilities, equipment, and systems to withstand substantial physical damage from weather and acts of God. They are

Copyright CSIS, all rights reserved.

equally responsible for response to most damage and emergencies. It is doubtful that federal, state, and local authorities can provide either the equipment or skills to replace or supplement many of these functions in any emergency other than a catastrophic attack on the US, and even then the core skills and equipment might have to come from other utilities. This raises further questions about the role of federal, state, and local laws and regulation to mandate improvements in Homeland defense capabilities, the use of voluntary recommendations and standards, and how the costs of such programs should be paid for. It also raises questions about the legal liability of utilities and other companies performing critical functions, and the penalties for failing to take effective action.

Information systems are emerging as a new form of national infrastructure, as well as part of virtually every significant private sector operation. They have steadily greater importance and cost, and they create steadily rising risks. They also tend to be highly specialized and require great expertise. Once again, it is doubtful that federal, state, and local authorities can provide the equipment or skills to replace or supplement such systems. In many cases, outside defense or repair would be impossible even in the case of a catastrophic attack unless expertise and dedicated equipment could be brought in from other parts of the private sector that were not subject to attack.

As a result, both the physical and cyber defense of information systems requires the private sector – as well as state and local authorities and NGOs – to assume a new level of responsibility for their own defense. At the same time, it raises questions about the role of federal, state, and local laws and regulation in a new area, the use of voluntary recommendations and standards, and how the costs of such programs should be paid for. It also raises major questions about the legal liability for the defense of information systems, and the penalties for failing to take effective action.

Medical services and other emergency response capabilities present are equally complex problem. There are acute pressures to reduce the cost of virtually all medical services, reduce redundancy, improve efficiency, and limit investment in catastrophic care. These pressures apply equally at the federal, state, local, and private sector levels. There are equal budgetary pressures on emergency response capabilities, although FEMA, the National Guard, and state and local emergency services face fewer cost-driven constraints than most health professionals. Homeland defense requires major catastrophic response capabilities, some of which duplicate existing capabilities and other of which may require totally new capabilities and facilities. A nuclear attack and the use of biological weapons are clear cases in point.

The practical problem in all of these cases is that there are no national standards. Every state, locality, company, and NGO has different capabilities. It is often possible to identify key facilities in some areas, but once again no survey exists of national capabilities and programs. The trade-offs involved in improving Homeland Defense capabilities also go far beyond the kind of trade-offs involved in dealing with national defense issues. They involve costs and legal and regulatory national basis that affect the entire private sector, all states and localities, and virtually every individual.

Copyright CSIS, all rights reserved.

F. The Rights of Private Citizens.

Finally, Homeland Defense presents new problems in terms of the rights of private citizens, although it may be equally vital in protecting them in every other way. This is not true of missile defense, but questions immediately arise over the impact of federal, state, and local actions in a catastrophic emergency involving the use of weapons of mass destruction. What level of martial law is justified? What can private citizens be compelled to do in a case like the use of biological weapons? What changes occur to property rights in case of contaminated facilities? Do the precedents set in dealing with natural disasters apply? Are they adequate?

Virtually all efforts to check terrorism and extremist violence present some human rights issues. There have also been many past abuses of such rights in the name of anti-communism and other perceived threats that did not prove to be justified by the actual threat to the American homeland. At the same time, the threat posed by the terrorist use of weapons of mass destruction involves a new kind of threats, and threats like biological weapons are extremely difficult to detect and may require a massive human intelligence effort.

The issue of victims rights can also take on a whole new meaning when the victims are the subject of attack using weapons of mass destruction. It is one thing to debate the rights of private citizens – and terrorists – in the context of a government effort to deal with a threat that has not yet materialized or which is confined to isolated incidents with limited casualties. It is quite another thing to consider a world in which terrorists and extremists have access to much more lethal weapons, organize to use them, and actually do use them.

Moreover, the use of weapons of mass destruction can involve major new human rights problems in terms of response activity. Limited medical resources may require drastic forms of triage that themselves mean taking a deliberate decision to allow large numbers of Americans to die. Containment of the effect of attacks using active biological and persistent chemical weapons may force the use of Draconian forms of martial law and detention or execution of those who try to leave a containment area.

Information warfare presents a host of new problems. It offers a new way to attack the rights of private citizens, and at the same time, requires new forms of law enforcement and surveillance. What kinds of defense are justified? How intrusive can they be? What level of activity is really merited? Can the equivalent of firewalls be created that allow enhanced protection against foreign attacks while limiting surveillance or interference in the activities of private American citizens?

There is also the problem of liability. If defense must often begin at the level of private corporations, then what level of government intervention should be tolerated to insure that such defense is provided? If many of the attackers are private citizens or criminals capable of causing immense harm to a wide range of people, what level of government action is justified to protect the victims.

These are questions that really cannot be answered at this point in time. It is easy to

Copyright CSIS, all rights reserved.

address such issues on a case by case basis in discussing Homeland defense measure. It is not possible to develop an overall strategy for dealing with human rights issues until both the nature of some threats becomes clearer, and the US has developed a broad program for Homeland Defense. What is clear, however, is that there is an inherent dilemma in Homeland Defense. Any overreaction that affects human rights is not justified, and any under-reaction could cost thousands of Americans their lives or do massive economic damage.

Copyright CSIS, all rights reserved.

II. Establishing a Practical Definition of Homeland Defense

A practical strategy for allocating resources to Homeland defense must determine the most useful way to define precisely what " Homeland Defense" means in policy terms. At present, there is no clear agreement as to what issues and policies are most usefully included in Homeland Defense. Some experts include organized crime and narcotics. Others see organized crime and narcotics as peripheral threats that the US has long had to live with and which existing law enforcement systems can deal with. There is an argument over whether information warfare is part of Homeland Defense, or an emerging risk that is part of the normal cost of doing business and one which both industry and the US government must learn to defend themselves against as a matter of course.

Some experts argue that Homeland Defense should focus only on defending within the territory of the US and at the border. Others argue that measures to strengthen defense within US territory must be integrated with measures to improve foreign intelligence, deterrence, and defense capabilities using US and allied capabilities abroad. Deciding on the right definition and focus will be a key aspect of shaping the proper public policy response.

A great many advocates of given threats and solutions attempt to tailor Homeland defense in ways that support their beliefs or causes. The is particularly true of the advocates of ballistic missile defense, who have gone through more than a decade of bitter partisan wrangling and who increasingly tailor both their threat analysis and definition of Homeland defense to support the current concept of a limited National Missile Defense system. It is equally true, however, of those who have made a cause out of publicizing superterrorism and more orthodox forms of terrorism, information warfare, narcotics, and organized crime.

It must be said in defense of such approaches that advocacy is virtually the only way in which to develop public consciousness, create suitable defense programs, and force decision-makers to act. At the same time, a sharply resource-constrained US defense structure cannot afford to use a definition of Homeland defense that simply piles on threat upon another, and which does not explicitly consider the priorities for action in the broadest possible sense.

A. Establishing a Practical Core Definition of Homeland Defense

There is no "right" way to resolve the debate over how to define Homeland defense. There are too many uncertainties and intangibles. In practical terms, however, a definition of Homeland Defense must includes and major threat to US territory, and US citizens, economy, infrastructure, and government. The previous analysis has already suggested that such core threats include:

Copyright CSIS, all rights reserved.

- Direct military attacks on the US using long-range delivery systems and weapons of mass destruction,
- Foreign terrorist or covert attacks using weapons of mass destruction,
- Foreign terrorist or covert attacks using more conventional means.
- Domestic terrorist or extremist attacks using weapons of mass destruction,
- Domestic terrorist or extremist attacks using conventional means.

These threats all have certain things in common. They involve threats where the US government must normally play a dominant role. They involve threats to which state and local authorities and the private sector cannot respond adequately without federal aid, and they involve what potentially are serious nation-wide risks to American citizens.

1. Information Warfare

The threat of information warfare presents more serious definitional problems. It is clear that providers and users must assume a far larger role in their own defense, and that they are likely to be under repeated attacks from hackers and criminals in the US and abroad. Users of complex information systems must routinely defend their systems as a cost of doing business, and must be on the cutting edge of technology. Reliance on the federal government as a primary defense is almost certain to fail and to virtually invite attack, and there is a good case to be made that information defense is not only a requirement for the use of information systems, but that the failure to create and update effective defenses should be subject to civil and criminal penalties.

At the same time, foreign governments and major terrorist and extremist groups can pose an extraordinary threat to information systems that may require federal intervention. As a result, the most practical way to resolve the issue is to define Homeland Defense so that it includes large-scale uses of information warfare in attacks directed at the US as a government or a nation, but does not include defense against criminal and random attacks on given elements of the US government, the private sector, or private individuals.

2. Narcotics and Organized Crime

Narcotics and organized crime collectively pose a threat to American society. In virtually all cases to date, however, they are diverse criminal activities that are properly deal with by ordinary law enforcement activities, regardless of their source of origin and whether the net effect of criminal behavior has a serious impact on the US economy and society. The traditional distinction between defense and law enforcement is a wise one, and US efforts to use the military in the “war on drugs” have been sufficiently ineffective so that there is little historical reason to assume that reinforcing such a mission would accomplish any more to raise the street price of drugs or limit their availability than in the past.

Copyright CSIS, all rights reserved.

There is the possibility that a foreign power or terrorist organization could use international crime and/or narcotics trafficking to attack the US as part of a deliberate attack directed at the US as a government or a nation. This is equally true, however, of a wide range of other legal trade and financial activities, and there is only limited historical precedent for such activity.

The most practical way to resolve the issue seems to be to define Homeland Defense so that it only the use of narcotics and organized crime in attacks which are directed at the US as a government or a nation. There does not seem to be any valid reason to include defense against ordinary criminal activity.

B. Homeland Defense Foreign Defense, and Deterrence

The definitional problem becomes more serious in dealing with the distinctions between Homeland defense, foreign defense, and deterrence. The first line of Homeland Defense still begins overseas in every case but attacks by domestic extremists. US power projection capabilities and the threat of American retaliation provide a major deterrent to any attack on the American Homeland, and an effective Homeland Defense strategy must pay close attention to both how to strengthen deterrence and how to defeat or destroy an enemy's capability to conduct further attacks on the US.

Strategic defense is a good case in point. It may be more than a decade before the US can develop effective strategic missile defenses. In the interim, the best defense is the threat of offensive retaliatory strikes. Even if strategic missile defenses are deployed, serious questions are likely to remain about the threshold of attack they can deal with and whether they are leak proof. At the same time, strategic missile defenses also make the threat of US retaliation and power projection more credible in those cases where a foreign threat could launch missiles against the US in retaliation to US action in defense of a regional interest or ally. This interaction between offensive and defense is a critical one, as is the interaction between deterrence and defense.

Foreign covert, terrorist, and proxy threats are best deal with before they enter the United States. A strong US presence in unstable regions, and close ties to regional allies, may often help the US locate and defeat such threats before they can approach the borders of the US. The tangible presence of US conventional forces in a region and American strike assets may again act as a deterrent threat as well as allow the US to strike in ways that limit or prevent follow-on attacks.

As a result, US foreign defense and deterrent capabilities must be considered as an important aspect of Homeland Defense, particularly in a financial environment where any improvement in Homeland Defense capabilities may involve trade-offs that reduce these aspects of US military capabilities.

Undersecretary of Defense for Policy, Walter Slocombe, made similar points in his address to the CSIS on National Missile Defenses,[3]

Copyright CSIS, all rights reserved.

> "…a national missile defense is only a part of the effort to protect ourselves from these and other ballistic missile threats. The United States seeks to prevent and reduce the threat through a whole range of means: export control measures, such as the missile technology control regime; arms reduction agreements such as START I and II; international non-proliferation arrangements such as a the nonproliferation treaty; and cooperative nonproliferation efforts such as the Cooperative Threat Reduction Program. We also maintain an active program of bilateral and multilateral diplomacy to discourage the transfer and indeed the acquisition of missiles and capabilities that would threaten the United States or key allies.
>
> We also deter the threat by maintaining powerful nuclear and conventional forces. Those who would threaten America or its allies should have no doubt any attack on us would meet an overwhelming response. There is no contradiction between defenses and deterrence. At the core of deterrence is convincing an adversary that the assured negative consequences of an action greatly outweigh any potential positive results of that action.
>
> There are thus two sides to deterrence. The threat of retaliation drives home that the negative consequences would be huge. But it is also valuable for deterrence to reduce the chance that an attack would succeed in the first place -- that is, to reduce the prospect of positive results. And missile defenses can do that.
>
> Missile defenses further complement deterrence by enhancing the United States' ability to fulfill its global security commitments to allies and friends. This is because defenses render less credible any possible attempts by a rogue state adversary to use ballistic missiles armed with weapons of mass destruction to coerce the United States into holding back from supporting a friend or ally that the rogue state threatens with attack. Defenses from such attacks can therefore reinforce the commitment of the United States to support our allies and friends from NATO to Israel, to the Persian Gulf, to Northeast Asia in the event they face a direct military threat from a rogue state.

Similarly, Secretary Cohen's FY1999 Annual Report stresses the need for a broad counterproliferation program, of which direct Homeland defense is only part:

> DoD's extensive <counterproliferation> and export control efforts are designed to slow the spread of technologies that can threaten the security of U.S. forces and infrastructure and undermine regional stability. The Department has progressed substantially toward fully integrating considerations of NBC weapons use against U.S. forces into its military planning, acquisition, intelligence, and international cooperation activities. These include efforts to embed <counterproliferation> in all aspects of the planning and programming process adapt military doctrine and operational plans to deal with NBC weapons in regional contingencies; mature acquisition programs to ensure that U.S. forces will be adequately trained and equipped to operate effectively in contingencies involving NBC threats; reallocate intelligence resources to provide better information about adversary NBC capabilities and how they are likely to be used; and undertake multilateral and bilateral cooperative efforts with U.S. allies and friends to develop a common defense response to the military risks posed by NBC proliferation. The Quadrennial Defense Review underscored the need for these efforts; accordingly, the Secretary of Defense increased planned spending on <counterproliferation> by $1 billion over the Future Years Defense Program.
>
> DoD must meet two key challenges as part of its strategy to ensure future <counterproliferation> preparedness. It must institutionalize <counterproliferation> as an organizing principle in every facet of military activity, from logistics to maneuver and strike warfare, and it must internationalize those same efforts to ensure U.S. allies and potential coalition partners train, equip, and prepare their forces to operate with U.S. forces under NBC conditions.
>
> To advance the institutionalization of <counterproliferation>, the Joint Staff and CINCs are developing a joint counter-NBC weapons operational concept that integrates both offensive and defensive measures. This strategy will serve as the basis for refining existing doctrine so that it more fully integrates all aspects

Copyright CSIS, all rights reserved.

of counter-NBC operations. In addition, the Services and CINCs are placing greater emphasis on regular individual, unit, joint, and combined training and exercises that incorporate realistic NBC threats. The Services are working to develop new training standards for specialized units, such as logistics and medical units, and larger formations to improve their ability to perform complex tasks under prolonged NBC conditions. Finally, many <counterproliferation>-related capabilities must be available prior to or very early in a conflict. The Services are developing capability packages that provide for early deployment or prepositioning of NBC defense and theater missile defense capabilities and personnel into theaters of operations. The timing necessary for the arrival of such capabilities should in part determine whether or not those capabilities reside in active or reserve components.

Unless properly prepared to deal with NBC threats or attacks, allies and friends may present vulnerabilities for a U.S.-led coalition. In particular, potential coalition partners cannot depend on U.S. forces to provide passive and active defense capabilities to counter NBC threats. U.S. <counterproliferation> cooperation with its NATO allies through the Senior Defense Group on Proliferation provides a template for improving the preparedness of long-standing allies and other countries that may choose to act in concert with the United States in future military coalitions. Similar efforts with allies in Southwest Asia and Asia-Pacific will continue to ensure that potential coalition partners for major theater wars have effective plans for CBW defense of populations and forces.

… As part of broader efforts to enhance the security of U.S., allied, and coalition forces against ballistic missile strikes and to complement U.S. <counterproliferation> strategy, the United States is exploring opportunities for theater ballistic missile defense cooperation with its allies and friends. The objectives of U.S. cooperative efforts are:

- To provide effective missile defense for U.S., allied, and friendly troops, and for allied and friendly civilian populations.

- To strengthen U.S. security relationships.

- To enhance collective deterrence of missile attacks.

- To share the burden of developing and fielding theater missile defenses.

- To enhance interoperability between U.S. forces and those of allies and friends.

The United States is taking an evolutionary and tailored approach to allied cooperation that accommodates varying national programs and plans, as well as special national capabilities. This approach includes bilateral and multilateral research and development, off-the-shelf purchases, and coproduction of TMD components or entire systems. Furthermore, as part of an ongoing initiative aimed at countering the TBM threat, the United States is sharing early warning data on launches of theater-range ballistic missiles with allies and friends as a means of engendering greater cooperation on theater missile defense.

In its 1991 New Strategic Concept, NATO recognized the risk posed by proliferation of WMD and ballistic missiles. Since then, the Alliance has reached general agreement on the framework for addressing this threat. The consensus is that layered theater ballistic missile defense is necessary for NATO's deployed forces. For the past several years, DoD has also held discussions with Japan regarding cooperative research in support of developing a TMD capability, and Japan recently decided to participate in and provide funding for such cooperative research.

U.S. TMD cooperation with Russia is an excellent example of how cooperative approaches to dealing with new regional security challenges of mutual interest, such as the proliferation of ballistic missiles, can advance U.S. security objectives. The United States and Russia have conducted two TMD exercises and

Copyright CSIS, all rights reserved.

> have agreed to a third, multiple-phase effort in 1999 and 2000. These exercises have provided a practical basis for U.S. and Russian forces to develop agreed procedures to conduct theater missile defense operations during regional contingencies where they could be deployed together, facing a common adversary that resorts to employment of theater ballistic missiles.
>
> Additionally, at the September 1998 Summit, President Clinton and President Yeltsin announced a new U.S.-Russian initiative. The two countries have agreed to establish a jointly-manned center in Russia for the timely sharing of information on the launches of ballistic missiles and space launch vehicles detected by each sides' early warning systems. The United States and Russia will also establish a voluntary multinational system for prelaunch notification of planned missile launches. The initiatives are designed to minimize the risks associated with dangerous reactions to false warning of a missile attack.
>
> U.S.-Israeli cooperative programs, including shared early warning on theater missile launches and the development of the Arrow TMD system, assist Tel Aviv in developing a ballistic missile defense capability to deter and, if necessary, defend against current and emerging ballistic missile threats in the region. Planned interoperability with U.S. theater missile defense systems could afford Israel a more robust defense. Moreover, the program provides technical benefits for both sides by expanding the theater missile defense technology base and providing risk mitigation for U.S. weapon systems.

He makes similar points about the linkage between domestic and foreign counterterrorist activity:

> The terrorist threat has changed markedly in recent years, due primarily to five factors: changing terrorist motivations; the proliferation of technologies of mass destruction; increased access to information, information technologies, and mass media; a perception that the United States is unwilling to accept casualties; and the accelerated centralization of vital components of the national infrastructure.
>
> DoD divides its response to terrorism into two categories. Antiterrorism refers to defensive measures used to reduce the vulnerability of individuals and property to terrorist acts. Counterterrorism refers to offensive measures taken to prevent, deter, and respond to terrorism. Both fall under the rubric of combating terrorism. Force protection is the umbrella security program involving the coordinated efforts of key U.S. departments and agencies designed to protect military and civilian personnel, their family members, and U.S. property.
>
> DoD has initiated a wide range of actions designed to enhance antiterrorism, requiring threat and force protection to be constantly evaluated and giving commanders increased resources and flexibility to be fully responsive to changes in the threat. The Department has established programs to expand protection measures worldwide where appropriate. At all levels, the Department has developed and carried out policies, processes, and programs designed to integrate force protection into the culture and institutional fabric of the United States military.
>
> Because intelligence represents the first line of defense, DoD has implemented procedures to improve its collection and use of terrorism-related intelligence, getting the needed product into the hands of the local commander as rapidly as possible. The Defense Intelligence Agency (DIA) is engaged in an aggressive long-term collection and analytic effort designed to provide information that can help local commanders detect, deter, and prevent terrorist attack. Close working relationships between DIA and other members of the national intelligence community are being strengthened, and intelligence exchanges with U.S. friends and allies have been increased.
>
> DoD is also taking steps to improve force protection, including programs for U.S. military forces, family members, and DoD civilians. DoD has actively worked to enhance training and awareness of the terrorist threat facing U.S. forces. In 1998, the Department began to implement a set of worldwide, prescriptive

Copyright CSIS, all rights reserved.

> standards for antiterrorism and force protection. Vulnerability assessments conducted by the Joint Staff, combatant commanders, and the Services provided an effective means to evaluate and improve installation commanders' antiterrorism readiness programs. Based on findings in these assessments, the Joint Staff developed a planning tool that provides installation commanders with mechanisms to develop comprehensive, tailored antiterrorism and force protection plans for their specific facilities. The Department also worked with the Department of State to ensure that rigorous force protection programs are provided for U.S. forces overseas.
>
> DoD's counterterrorism capabilities provide the offensive means to deter, defeat, and respond vigorously to all forms of terrorist attack against U.S. interests, wherever they may occur. The Department has significantly increased the resources allocated to these sensitive activities, and efforts are under way to maximize readiness so that U.S. counterterrorism forces are trained and equipped to meet any future forms of terrorism. U.S. counterterrorism forces receive the most advanced and diverse training available and continually exercise to maintain proficiency and to develop new skills. They regularly train with their foreign counterparts to maximize coordination and effectiveness. They also engage with counterpart organizations in a variety of exchange programs which not only hone their skills, but also contribute to the development of mutual confidence and trust.

These comments are more than strategic boilerplate and no realistic discussion of Homeland defense can ignore them. US cooperation with other states in limiting the flow of the technologies and weapons need to proliferate, tracking terrorist and extremist movements, and international law enforcement is equally important. US efforts to limit foreign arms sales and technology transfers have already had a major impact in slowing down proliferation in nations like Iran and North Korea. Even neutral or otherwise hostile governments will often take action against terrorists and extremists, particularly if they fear US retaliation for such attacks. Friendly governments have no reason to tolerate terrorist and extremist activities. It is also all too possible that any major terrorist success in an attack on US forces or an ally overseas will encourage such movements to attack the US.

No threat or program analysis that fails to include such considerations can be regarded as valid or as anything other than “rigged” advocacy analysis designed to support a given program or cause. Such efforts are intellectual dishonest by definition. As a result, this report not only includes foreign defense and deterrence in the broader definition of Homeland Defense, it examines the extent to which overseas US defense and law enforcement activities contribute to Homeland Defense and the possible trade-offs between such activities and direct defense within the American homeland.

C. Capabilities and Technology: The Race Between Offensive and Defensive Solutions

The difference between “defensive” and “offensive” capabilities and technology is almost always an artificial one. It the case of Homeland Defense, however, it is important to point out that any capability or technology that reduces the threat or its effectiveness must be included in the definition of Homeland defense, regardless of whether it is “offensive” or “defensive” in character. For example, new sensor and strike systems that allow the US to detect the manufacture of weapons of mass destruction and improve its ability to destroy them are

Copyright CSIS, all rights reserved.

important potential improvements in Homeland Defense. A system that can detect a nuclear device in a ship or aircraft entering US air space may be "defensive" in the sense it provides warning, but it is "offensive" in the sense that warning inevitably provides a targeting capability.

This would be a minor issue except that many analysts of Homeland Defense only analyze the defensive aspects of Homeland Defense options while an increasing number of the US military feel that the technology presently favors the offense and that too heavy an emphasis on defensive options weakens the US response. They point to the emphasis on missile defense versus US retaliation and deterrence.

More broadly, there is a tendency to define Homeland Defense largely in terms of current threats, rather than examine the value of defensive options against the range of offensive options that may be developed during their projected operational life time. This is not a definitional issue per se, but it is an important issue in terms of choosing between options. Homeland Defense must be based upon the assumption that enemies are intelligent and innovative. It cannot be frozen in time, and options must be explicitly analyzed in terms of the options available to defeat them, the probable evolution of offensive options in the future, and the cost to defeat a defense. While these points may seem obvious, far too much of the literature on defensive programs compares the merits of tomorrow's solutions against today's threat.

D. Dealing With Multiple Threats and the Linkage Between the Homeland, US Power Projection Forces, and Allied/Coalition Territory

A practical definition of Homeland Defense cannot be compartmentalized. As has been pointed out earlier, there are no rules saying that an attacker cannot use several different methods of attack, or even appear to emphasize one form of attack while actually launching another. Missile development programs are a current example. Nothing about the missile programs of Iran and North Korea precludes them from launching covert attacks on the US.

It is also possible that foreign nations may use domestic US proxies, supporting US extremist groups and terrorists, or may "piggyback" on a crisis to attack the US covertly while it is confronting a more over threat from another nation. Alternatively, an attacker may strike at both the Homeland and US forces overseas, or simultaneously at the US and an ally. Homeland Defense must be prepared to deal with complex multiple threats and a sudden shift or escalation to another threat that occurs with little or no warning.

Equally important, partial defenses are an invitation to a potential attacker to chose the line of least resistance and the areas where the US has no defenses. They are also an invitation to extremely expensive wastes of money which will force trade-offs that reduce some other aspect of US defenses. A valid definition of Homeland defense must recognize the need to explicitly analyze the cost to defeat any given defensive action, either by using other forces of attack or by exploiting asymmetric warfare to change the nature of a given threat so that it is more practical

Copyright CSIS, all rights reserved.

and cheaper for the attacker to increase a given type of threat than it is for the US to defend.

E. The Problem of Complexity

To sum up, a simple or narrow definition of Homeland may suit given program advocates but it cannot serve the US national interest. Programs have to be defined and structure in terms of some core definition of Homeland defense, but such a definition cannot credibly be used to justify any given program or form of defense. At some point, far more complex and comprehensive definitions of Homeland defense must be used and applied.

A core definition of Homeland Defense that focuses on direct military attacks using long-range delivery systems and weapons of mass destruction, foreign terrorist or covert attacks using weapons of mass destruction, foreign terrorist or covert attacks using more conventional means, domestic terrorist or extremist attacks using weapons of mass destruction, and domestic terrorist or extremist attacks using conventional means, and state-driven threats using information warfare begins to meet this test. It at least forces the analyst to consider all major direct threats and not simply selected threats in a form suitable to advocating given programs.

A full definition of Homeland defense must, however, consider the value of regional defenses, alliances and coalitions, power projection, nuclear deterrence, the other aspects of counterproliferation and counterterrorism programs, and arms control. It must analyze Homeland defense in a broad context and one suited to examining the full range of trade-offs that have to be made between different US programs. A core definition of Homeland defense cannot validly serve this purpose.

This will not be a popular definition of Homeland defense. The use of “chaos” or “complexity theory” goes against the American grain, and the same is true of complex definitions which require an explicit analysis of all the variables involved. Americans recognize that complexity is the enemy of action. The fact remains, however, that Homeland defense cannot usefully be defined in any other way. To paraphrase an old joke, there may be nothing uglier than watching a beautiful theory being raped to death by a gang of ugly facts, but any less ruthless approach to Homeland defense is pointless.

Copyright CSIS, all rights reserved.

[1] IISS, The 1998 Chart of Armed Conflict, London, IISS, 1998.

[2] The historical survey work of Herbert J. Tillema, International Conflict Since 1945, Boulder, Westview, 1991.

[3] Remarks of the Honorable Walter B. Slocombe, Under Secretary of Defense for Policy, to the Center for Strategic and International Studies Statesmen's Forum, November 5, 1999.

Copyright CSIS, all rights reserved.