In a way, homeland security looks like defense analysis probably did before it became analytic, i.e., before the advent of gaming, simulation, cost-effectiveness, and trade-off analyses and the application of other techniques that are, by now, standard tools for assessing options in defense.\(^1\) Most of the work done in the area of homeland security seems to be focused on essentially organizational solutions whose premise seems to be that if only more centralized control of policy were in evidence, the problem would be far more tractable.\(^2\) While more centralized control and policy direction almost certainly would help, we take a somewhat different view of the problem.

To be sure, it is a hard problem to analyze. The data in this area are difficult to obtain and uneven in quality, and no computer or other models can be used to evaluate cost-effectiveness, trade-offs, or robustness. With this in mind, we begin by proposing an analytic framework for assessing homeland security that focuses on four key policy questions that, once answered, provide the necessary information for designing homeland security programs. The questions are:

---

\(^1\)We have not, for example, seen a thorough analysis of the question of the optimal locations for response units for consequence management, what sorts of mobility assets will be necessary to assure their responsiveness, and what sorts of capabilities they should have. In a way, this is not unlike strategic analysis before Albert Wohlstetter’s seminal assessment of the optimal basing for strategic aircraft. See Wohlstetter’s (1958) classic piece, posted at http://www.rand.org/publications/classics/wohlstetter/P1472/P1472.html.

\(^2\)In this vein, see Carter et al. (1998a, 1998b), and Iklé (1999).
Preparing the U.S. Army for Homeland Security

- What types and magnitudes of threat are we planning against, and what risks do we face?
- What level of performance will we demand from our homeland security capabilities?
- What are the most cost-effective program options for providing capabilities with the needed performance levels in incidents of specified planning magnitude?
- What resources will be available for homeland security programs?

Each will be discussed at greater length.

**THREAT AND RISK ANALYSES**

The first question that needs to be addressed: What types and magnitudes of threats are we planning against, and what risks do we face?

The first element of the analytic framework for analyzing homeland security is thus an assessment of threats and risks. The General Accounting Office (GAO) has strongly and consistently recommended the use of threat and risk assessments in designing programs to combat terrorism. As described by the GAO:

> Threat and risk assessments are widely recognized as valid decision support tools to establish and prioritize security program requirements. A threat analysis, the first step in determining risk, identifies and evaluates each threat on the basis of various factors, such as its capability and intent to attack an asset, the likelihood of a successful attack, and its lethality. Risk management is the deliberate process of understanding “risk”—the likelihood that a threat will harm an asset with some severity of consequences—and deciding on and implementing actions to reduce it. (GAO, 1998b, p. 3.)

Risk management principles acknowledge that (1) while risk generally cannot be eliminated, it can be reduced by enhancing protection from validated and credible threats; (2) although many threats are possible, some are more likely to occur than others; and (3) assets are not equally critical. (GAO, 1998b, p. 3.)
Threat and risk assessments enable organizations to determine how to prioritize scarce resources across various threats and risks, largely in terms of the conditions—in terms of probability and consequence—under which specific actions are and are not warranted (see Figure 3.1).\(^3\)

The darkest regions in the figure include those cases where the probability/magnitude combination is unacceptable and efforts need to be made to reduce risk through countermeasures. The next two cases are “indeterminate” and require management decision or review. The regions that contain narrow stripes consist of cases that are undesirable but where a management decision is required to determine what if any actions should be taken. The white regions include cases where the combination of probability and magnitude are probably acceptable, although management review is required. Finally, the areas with wider stripes include cases that are acceptable without any management review.

---

\(^3\)The figure is adapted from GAO, 1998b, p. 8.
The foregoing suggests that threats and risks can be considered in a systematic framework that uses both probability and severity of consequence as criteria for decisionmaking about whether to take action.\(^4\) The question remains, however, what planning magnitude should we use to size our capabilities?

Not unlike the “spectrum of threat” charts that often accompany defense analyses—where the probability and lethality or consequence of different types of military operations are inversely related—a similar approach can be used for establishing the desirable planning magnitude for a specific type of threat (see Figure 3.2).

The figure is a modified “spectrum of threat” plot, with the consequence or magnitude of events on the x-axis and the probability of

\[\text{Figure 3.2—Threats in Terms of Probability and Consequence}\]

\(^4\)For a particularly good discussion of the importance of considering both probability and magnitude of consequence, see Falkenrath (1998).
the events on the y-axis. The figure portrays two curves. If we focus on the threat of terrorism, the bottom curve would describe the frequency (or probability, if we assume that the distribution of historical incidents also is representative of what we will see in the future) of terrorist incidents of various magnitudes. The upper curve represents the cumulative frequency or probability of incidents that are of equal or smaller consequence. In other words, if $p^*$ in the figure is assumed to be 90 percent, then programs considered adequate to deal with cases at the ninetieth percentile also would be adequate for all of the smaller terrorist attacks as well. They would, however, only represent partial solutions to the larger 10 percent of cases.5

Figure 3.3 plots data on American casualties in terrorist incidents. The number of casualties in each incident (the consequences of these events) is on the x-axis, and the frequency of events is on the y-axis. The figure demonstrates that such curves easily can be constructed from empirical historical data on the past incidence of terrorist or other attacks or on the basis of integrated threat and risks assessments that aim to project the future threat and risk environment.

As shown, the frequency (probability) and consequence of terrorist incidents are inversely related, i.e., injuries are more likely than deaths, small numbers of casualties are more likely than large numbers, and the probability quickly declines as the consequence of the incidents increases.

Two basic methods for establishing the appropriate planning magnitude are suggested. First, based on data from the intelligence and law enforcement community or other sources, we can specify a cumulative probability ($p^*$ in the figure) that is sufficiently high that (a) results in a consequence level that is larger than state and local

---

5We note that one could also establish planning magnitudes by selecting cases whose consequences are larger than any that have been seen in the past. For example, one might use for a planning magnitude an incident 25 percent, 50 percent, or 100 percent larger than the largest incident that has to date been seen. Indeed, in Chapter Four, we suggest a planning magnitude for chemical incidents (2,500) that is 200 times larger than the number of deaths that occurred in the Aum Shinrikyo sarin attack in Tokyo.
The foregoing has demonstrated that empirical data can be used to construct cumulative frequency (or probability) distributions. It will later be shown that, whether one is looking at terrorist incidents or the consequences of cyber attacks, these distributions follow the same pattern: The most likely incidents are the ones that are the
smallest in magnitude or consequence, and the largest events are exceedingly rare.

**ESTABLISHING DESIRED PERFORMANCE LEVELS**

The second question that needs to be addressed: What level of performance will we demand from our homeland security capabilities?

The Government Performance and Results Act (GPRA) of 1993 aims to improve governmental effectiveness by setting program goals, and measuring program performance against those goals. In the National Defense Authorization Act for Fiscal Year 2000, the Senate Armed Services Committee has furthermore directed the Secretary of the Army to review existing modernization programs and provide an assessment not later than February 1, 2000, on how these plans will meet the future challenges associated with, among other mission areas, homeland security (U.S. Senate, 1999, pp. 132–133). Although certain aspects of the Army’s homeland security activities have been identified as being in compliance with the Act, each homeland security task area requires different measures of performance.

We now address the issue of measures of performance for homeland security and the establishment of performance levels to guide the development of operational concepts, programs, plans, and budgets.

The previous section suggested that the first step in defining homeland security programs is to undertake threat and risk analyses that specify the types and magnitudes of events against which we will plan. The output of this process was a planning magnitude—designated as m*—that established the first parameter for sizing homeland security capabilities. The next step in the process is defining the performance levels for responses to homeland security attacks (see Figure 3.4).

As in the previous figures, Figure 3.4 portrays the consequence of an event on the x-axis. The y-axis represents needed capabilities, and

---

6The GAO found that Soldier Biological Chemical Command’s (SBCCOM’s) chemical and biological defense research, development, test, and evaluation (RDT&E) program is quite admirable in this respect.
the contour lines represent different performance levels (low, medium, and high). Low performance might mean, for example, a capability to save the life of one in 10 who were injured, while a high performance level might mean the capability to save seven out of 10 of the injured.

The figure suggests that needed capabilities to respond to a homeland security attack (on the y-axis) are highly sensitive both to the planning magnitude ($m^*$) established earlier and normative beliefs about desired performance levels (i.e., whether one chooses to be on the low, medium, or high line).

This sensitivity of needed capabilities to planning magnitude for a fixed performance level can be seen by following any one of the three illustrative performance levels (low, medium, or high) from the origin to the bottom right part of the figure: the greater the planning magnitude, the greater the capabilities needed to provide a fixed level performance level.
Sensitivity to performance level can be seen by fixing the planning magnitude at $m^*$, and observing the capability level implied by the three levels of performance (low, medium, and high). For any planning magnitude, the greater the desired performance level, the greater the capabilities implied. As we will see in the next section, with the planning magnitude and desired performance level established, we have sufficient information to begin designing cost-effective programs that provide the needed capabilities.

It also is the case that performance improvements can either be realized by simply increasing the amount of resources allocated to the response or by improving (through improvements in equipment, mobility, or training) the effectiveness of the response capability.

Figure 3.5 illustrates these points by comparing the number of systems of various types needed to yield specific performance levels, here defined in terms of the total number of victims that can be evacuated by litter.

In the figure, the x-axis is the magnitude of the consequence of a disaster or WMD event, in terms of the total number of victims that
need evacuation on litters (this would be the \( m^* \) selected earlier). The y-axis is the number of sorties (or trips) by various systems. The lines represent various combinations of performance level (whether we desire a capability for evacuating 50, 75, or 90 percent of the victims) and systems (e.g., CH-47D and UH-1 helicopters and quarter-ton and three-quarter-ton trucks used as ambulances) that can provide the desired capabilities. Thus, each point on a line represents the number of sorties for a specific system that would be required to evacuate a specified percentage of victims for an incident of a given magnitude.7

To illustrate, if one wanted the highest level of performance (a capacity to evacuate 90 percent of the victims in a WMD incident), the CH-47Ds can be seen to provide the greatest capacity of the options presented: If our planning magnitude were 1,500, it would take fewer than 60 CH-47D sorties to evacuate the 1,500 victims; if the planning magnitude were 2,500 victims, fewer than 100 sorties would be needed.8 By comparison, it would take 675 trips by a quarter-ton truck serving as an ambulance to evacuate 1,500 victims, or 1,145 trips to evacuate 2,500 victims.

The main point of the figure is the obvious one that smaller incidents generally require smaller amounts of capability, but also the less obvious points that the needed capabilities are highly sensitive both to the capacity of the units or systems being considered (in this case, UH-1s, CH-47Ds, and quarter-ton and three-quarter-ton trucks), and to the demanded performance levels (a capacity to evacuate 50, 75, or 90 percent of the victims).

These calculations can provide insights into the volumetrics of the capabilities needed, given specified planning magnitudes and desired performance levels. Nevertheless, one needs to impose additional parameters on performance levels (e.g., the ability to evacuate a specified percentage of victims in three hours) or constraints (e.g., no helicopters larger than UH-1s, no more than 120

7We assumed simply that a quarter-ton truck could carry two litters and a three-quarter-ton truck could carry five litters, a UH-1 could carry six litters, and a CH-47D could carry 24 litters. These numbers are illustrative only.

8We assumed that a CH-47D could carry no more than 24 patients on litters.
trucks) to identify the actual numbers of systems (or units) that would need to be deployed to respond adequately to an incident.

Figure 3.6 suggests why this should be the case. In the figure, as we apply additional manpower (labor) and equipment (capital) in balanced combinations, our isoperformance curves shift up and to the right. Additional resources increase the number of victims that can be quickly and effectively located, triaged, evacuated, and medically treated.9

---

9The reason the isoperformance curves have the shape they do is that they are subject to strong assumptions about diminishing returns. For example, if we have only one truck to perform evacuations but keep increasing the manpower associated with that single truck, beyond a certain number of troops, no additional benefits accrue in terms of performance. In fact, at some point, so-called “shoulder space” considerations may begin to apply, where the situation becomes so crowded with personnel that the use of the truck is in fact prevented.
IDENTIFYING COST-EFFECTIVE PROGRAM MIXES

The third homeland security question that needs to be answered: What are the most cost-effective programmatic alternatives for providing capabilities with the needed performance levels for incidents of the type and planning magnitude we specified?

The previous section suggested a number of measures of performance that could be used to establish performance levels for meeting various types of threat. This section addresses programmatic considerations (i.e., the effectiveness and cost of homeland security programs) by describing the Army role in homeland security in the larger federal setting.

The national capabilities for preventing and responding to WMD terrorism—and the capabilities for the other homeland security threats—provide a “layered defense in depth” that cuts across federal departments and agencies and the military services. Throughout this section to simplify the exposition we describe this layered defense in terms of three layers: one focused on preventing attacks, one engaged in preincident activities to prepare for and defend against possible attacks, and one used to respond to attacks and manage their consequences. There are two principal aims in building such a layered defense.

First, the aim of a layered defense in depth is to achieve a robust defense that does not create the possibility of single-point failures by relying solely on the success of any one specific program or solely on the expected effectiveness of prevention or consequence mitigation. Such a robust layered defense can only be achieved by understanding the trade-offs inherent in striking a balance between policies and programs that can provide a high probability of preventing acts of WMD terrorism and policies and programs that can substantially mitigate the consequences of an act of WMD terrorism.

Figure 3.7 describes notional constant-cost combinations of prevention and consequence reduction capabilities that result in different probabilities of prevention and consequence reduction.\textsuperscript{10}

\textsuperscript{10}As will be described later, for example, federal spending on countering terrorism and WMD is weighted toward prevention.
In the figure, the x-axis is the degree of consequence reduction (e.g., the percentage reduction in victims, deaths, or dollar damage) that results from a specific policy. The y-axis is the effectiveness of the prevention efforts in terms of the probability that the policy will prevent the undesired events. The three isocontour curves represent the possible policies, i.e., combinations of prevention and consequence reduction activities, for three fixed budgets (low, medium, and high). Finally, the lines stemming from the origin connote distinct policies: Policy 1 emphasizes prevention at the expense of consequence reduction, and Policy 2 emphasizes consequence reduction.

The second principal aim in building a layered defense is that it should be cost-effective, representing an efficient use of scarce resources to obtain a specified level of performance or effective-
ness—i.e., the preferred mix of prevention and consequence reduction—at least-cost. Figure 3.8 presents a curve that traces the most cost-effective programmatic-providing capabilities that yield various performance levels.

The reader will recall that in the previous section, we chose a high performance level that provided a good balance between high assurance capabilities.

Figure 3.8—Cost-Effective Options at Various Performance Levels

---

11See Appendix B for an illustration of the sort of notional tradeoff analysis that could help reveal the most cost-effective solution for providing consequence mitigation capabilities.

12The figure makes the simplifying assumption that investments exhibit diminishing marginal returns. It also is possible that such a curve would not be a continuous function but would be made up of stair-steps, as the next most expensive cost-effective program options could come at considerable additional cost.
ance of preventing terrorist incidents and high assurance of mitigating the consequences of an event, should prevention efforts fail. This performance mix was shown to lead to a needed capability level of \( c^* \), i.e., a fairly high performance level.

The figure suggests that the higher the performance and capability level established (described in the third panel of the nomogram), the higher the cost. The rationale is that each marginal increase in performance level typically requires an increase in resources, whether in terms of additional labor (personnel), capital (materiel), or other inputs (e.g., enhanced training), and these come at some cost.\(^{13}\)

To summarize, the national programs that address the homeland security threats—including local, state, and federal actors and a range of activities both at home and abroad—should provide the sort of robust and cost-effective layered defense just described, irrespective of the nature of the threat (e.g., WMD versus “cyber”).

**BUDGETING AND RESOURCING**

The final question to be answered: What resources will be available for homeland security programs?

Once we have identified the most cost-effective mix of programs that meet the needed performance levels for preventing and mitigating the consequences of incidents of specified magnitude, we can examine the budgetary implications of these programs.

As described in Figure 3.9, this exercise essentially involves determining whether the total cost of the program specified in the preceding step is less than or equal to the maximum amount of resources we are willing to allocate to homeland security, in light of warfighting and other obligations.

The figure puts funding for homeland security activities on the x-axis and funding for other activities—generally, in the case of the Army and DoD, warfighting activities—on the y-axis. The straight line rep-

\(^{13}\)Performance increases also could come with the same level of resources, but where processes have been reengineered to be more effective and efficient.
Figure 3.9—Budgeting for Homeland Security

represents the total budget that can be allocated among homeland security and other activities. The indifference curve represents combinations of homeland security and other activities where a policy-maker has constant utility, i.e., the various combinations along the curve are equally attractive. Finally, the point where the indifference curve touches the budget curve is the optimum or preferred policy, where marginal cost and marginal utility are equal.

**PROCESS AND STRATEGY**

Each element of the foregoing four-step process has a great deal of activity associated with it—both in terms of analytic work and in terms of decisions that need to be taken—but its proper application also is quite critical, both in the short term and the long term.
Iterative in the Short Term

In the short term, we envision that the Army and DoD would need to iterate a number of times through the entire four-step process described above.

One reason is that empirical data are not routinely collected or reported, and it may take some effort to define the data requirements. In a similar vein, few off-the-shelf tools (e.g., simulation models) are available for doing the underlying analyses, and some effort will necessarily be involved in building and refining these tools to support the larger analytic effort.

Another reason is that the trade-offs between performance and cost—and which planning magnitudes and performance objectives are even deemed feasible from a cost perspective—can only be established by determining the minimum needed response capabilities that meet these objectives and costing them out. Put another way, we believe that attempts to establish exceedingly high planning magnitudes and performance criteria will in fact result in comparably high costs, that these will be seen as prohibitively expensive, and that they will necessitate downward revision to less ambitious short-term objectives, which can then be costed out. Since none of the steps of the process is independent of the others, a substantial number of iterations may be required to build consensus around the planning magnitudes and performance levels that establish needed capabilities and their associated costs. This will not be a strictly analytic enterprise, but will engage value trade-offs made by decision-makers from different disciplines and parts of the defense community, and it may simply take multiple iterations of the process to identify feasible solutions.

Part of an Adaptive Long-Term Strategy

In the longer term, we see the process as embedded in a larger long-term policy development strategy inherently adaptive in nature. Planning magnitudes, for example, would need to be established in large part on the basis of threat and risk analyses that include intelligence, law enforcement, and military personnel, and on the basis of policymakers’ desire to hedge against the unexpected. But because the threats and risks may increase or recede over time, these threat
and risk analyses would need to be updated periodically, and the suggested planning magnitude revised in light of the increasing (or decreasing) threat. Put another way, any initial numbers selected as planning magnitudes would be “marks on the wall,” subject to further refinement or to wholesale change as the threat environment changed or, as described above, if they proved too costly.

This adaptive, long-term strategy would dictate that, for the short term (e.g., one to five years), preparations be made to deal successfully with modest—yet still stressing—threats, rather than less probable, “worst case” scenarios. This will provide a bar high enough to be challenging, without making it impossible to surmount, and will give incentives for the development of the necessary prototype doctrine, organizations, training, and equipment, providing for mobility needs and creating a set of capabilities that can exercise with local, state, and federal civilian responders. If the threat environment has changed enough in three to five years to warrant increased planning magnitudes, then existing organizations can be expanded or new, more capable organizations can be fielded, with a higher degree of confidence that they will be able to address the situations they might encounter. If new capabilities are available at that time that permit much higher performance levels, those can be introduced into the force and tested in the crucible of training and exercises.

In short, the proposed framework is meant to be embedded in a process that involves threat and risk assessments and policy-level decisions regarding what is desirable, what is cost-effective, and, ultimately, what is affordable.

CONCLUSIONS

This chapter has provided a simple analytic framework and methodology that addresses the four key questions that need to be answered in homeland security. The four questions are:

- What magnitudes of events should the United States plan against for high-explosive, chemical, biological, radiological, nuclear, and cyber threats?
- What levels of performance will the nation demand in the national (local, state, and federal) responses to these events?
• What are the most cost-effective options for providing the capabilities that will address these events at the desired performance levels?

• What resources will be made available, and will they be sufficient to provide the necessary capabilities?

Chapters Four through Seven apply the framework to the four homeland security task areas that are the focus of this study and, where possible, populate some of the notional figures presented in this chapter with empirical data.