
**ENSURING MILITARY CAPABILITY:
CONTINUITY OF OPERATIONS**

This chapter addresses the third homeland security task area—the continuity of military operations in the United States, its territories, and its possessions.

As distinct from the COG operations, discussed in Chapter Five, this task area of homeland security consists of the continuity of *military* operations, including

- force protection, primarily for deploying units;
- critical infrastructure protection, i.e., the protection of mission-critical facilities and systems, i.e., the infrastructure necessary for the Army to carry out its missions; and
- protection of higher headquarters operations, which will help to ensure the integrity of the military chain of command.

The importance of this task lies in the following simple truth: Unless the Army and other military organizations can ensure the continuity of their own operations, they will be incapable of defending the United States and its vital interests at home and abroad and providing military capabilities for other purposes.

THREAT AND RISK ANALYSES

Threats

Conventional and WMD Attacks. Many of the threats requiring domestic preparedness described in Chapter Four probably apply

here as well, although in this task area one would anticipate a higher probability of involvement by state actors attempting to wage asymmetric war on the United States by attempting to hobble its ability to deploy military forces, rather than by nonstate or domestic actors.¹

Our analysis suggests that we would expect such threats to attack in breadth rather than depth. What this means is that attacking multiple targets separated in time and space could psychologically create the appearance of a far more formidable adversary than is actually the case. To be more explicit, a single 12-man team of terrorists inserted into the United States with four Stinger missiles would appear to be less formidable and have a lower shock value than if the team divided into four groups, each of which simultaneously attacked civilian or military aircraft in four different locations.²

Cyber Attacks. One also should add to the list of threats state and nonstate actors inimical to the United States who possess no known WMD programs or aspirations but appear to have active programs to develop offensive information capabilities that might be used against the U.S. military.³ This is a very dynamic and complex area, and our analysis accordingly only can skim the surface. Accordingly, the analysis that follows will address the issue in relatively broad strokes, supplying data where they are available.

The unclassified literature is somewhat contradictory on the degree of threat of cyber attack. Our reading is that catastrophic cyber

¹One can construct scenarios, however, in which right-wing groups attack U.S. military capabilities in the belief that they are in fact attacking efforts to impose a “new world order” by UN forces about to impose martial law on the United States.

²The potential for this type of asymmetric attack against deploying forces has been demonstrated in numerous war games conducted over the past decade. In fact, in every Army After Next war game conducted that “played” homeland security, adversaries consistently attempted to deter, degrade, and disrupt the flow of deploying forces to prevent the U.S. military from arriving in time to accomplish its mission. For a more detailed review of how potential adversaries might asymmetrically attack U.S. forces during deployment, in transit, and in theater, see the Joint Strategic Review for 1999. We are grateful to Rick Brennan for suggesting these points.

³Former Director of Central Intelligence John Deutch warned in 1996 that “[w]e have evidence that a number of countries around the world are developing the doctrine, strategies and tools to conduct information attacks,” and the *London Sunday Times* reported in July 1999 that Russian hackers were stealing U.S. weapon secrets (Deutch, 1996; Campbell, 1999).

attacks are not an imminent threat, but over time—and if actions are not taken to protect against them—the threat could grow.

Consider the transmittal letter of the President's Commission on Critical Infrastructure Protection, which noted that:

We found no evidence of an impending cyber attack which would have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm—particularly through information networks—is real; it is growing at an alarming rate; and we have little defense against it. (President's Commission, 1997a.)

And more recently, Willis Ware of RAND noted:

There is no evidence that the "sky is falling in"; the country is not in imminent danger of massive disruption through infrastructure cyber-attacks. In part, this stems from the natural resilience the country has evolved from having to deal with natural disasters and man-caused events of various kinds and magnitudes; in part, from the natural responses of organizations to protect themselves against anything that causes operational intrusions or upsets. (Ware, 1998, p. vii.)

According to the commander of DoD's Joint Task Force-Computer Network Defense:

The odds of the U.S. being attacked on line by a foreign nation state in some kind of cyber war in the near future are probably pretty low. But the odds of foreign nation states wanting to develop capabilities to help them if and when we are adversaries are probably pretty high. We need to have the same capability or better. (Wolfe, 1999, p. 1.)

Nevertheless, according to a 1996 study by GAO, the computer systems of the Department of Defense have come under increasing attack over the last several years:

The Department of Defense's computer systems are being attacked every day. Although Defense does not know exactly how often hackers try to break into its computers, the Defense Information

Systems Agency (DISA) estimates that as many as 250,000 attacks may have occurred last year [i.e., in 1995]. According to DISA, the number of attacks has been increasing each year for the past few years, and that trend is expected to continue. Equally worrisome are DISA's internal test results; in assessing vulnerabilities, DISA attacks and successfully penetrates Defense systems 65 percent of the time. Not all hacker attacks result in actual intrusions into computer systems; some are attempts to obtain information on systems in preparation for future attacks, while others are made by the curious or those who wish to challenge the Department's computer defenses. For example, Air Force officials at Wright-Patterson Air Force Base told us that, on average, they receive 3,000 to 4,000 attempts to access information each month from countries all around the world.

Many attacks, however, have been very serious. Hackers have stolen and destroyed sensitive data and software. They have installed "backdoors" into computer systems which allow them to surreptitiously regain entry into sensitive Defense systems. They have "crashed" entire systems and networks, denying computer service to authorized users and preventing Defense personnel from performing their duties. These are the attacks that warrant the most concern and highlight the need for greater information systems security at Defense. (GAO, 1996a, p. 2-3.)⁴

FBI Director Louis Freeh has indicated that cases of commercial, military, and infrastructure-related computer systems hacking incidents have doubled every year (Freeh, 1998). On July 25, 1999, Deputy Secretary of Defense John J. Hamre was quoted by the *London Sunday Times* as saying: "We're in the middle of a cyber war."

Anecdotally, in the spring of 1998, during the deployment of forces to the Persian Gulf in response to Iraqi provocations, Department of Defense networks reportedly experienced their most widespread and systematic attacks to date, with 20 major installations' networks compromised.⁵ Teenage hackers were behind attacks on Air Force

⁴See also Campbell (1999).

⁵During the attacks, dubbed "Solar Sunrise":

[T]he defense community and law enforcement agencies struggled to understand the nature of the attacks and identify the threat. The attacks were launched from computers within the United States and overseas. As it turned out, this incident involved a couple of Califor-

systems in February 1998 (Graham, 1998; CNN, 1998). The 1999 “Solar Sunrise” exercise also showed the potential consequences of cyber attacks, although these were “attacks” carried out by DoD players in a larger war game (CNN, 1999b). The trashing of web sites apparently has become a part of the larger battle for public opinion, although its consequence for military operations seems dubious.⁶ Nevertheless, attacks in March 1999 were traced to computers in Russia (CNN, 1999a), and attacks that resulted in stolen military secrets also have been reported (Agence France-Presse, 1999).

Thus there seems little doubt that defense computers are under *increasing* risk of attack, although the evidence on the frequency and severity of past and current attacks is generally anecdotal rather than statistical and therefore difficult to assess.⁷ Put another way, the unclassified public statements, anecdotal evidence, and empirical data in this area are somewhat contradictory.⁸ One suspects the existence of a gap between rhetoric and actual experience, in part stemming from the tension, described in Chapter Four, between the need to prudently alert the public so that they are not complacent about the threat and the desire to avoid frightening the public.⁹

An analysis of open-source data on computer incidents revealed that the distribution of frequency versus magnitude for cyber attacks taken as a whole follows the by-now familiar pattern of an inverse relationship (See Figure 6.1), with incidents of small or modest con-

nia teenagers. But “Solar Sunrise” demonstrated an enormous vulnerability in our unclassified computer systems which nevertheless play a critical role in management and moving U.S. armed forces all over the globe. (U.S. Senate, 1998.)

⁶Attacks on web sites presenting the public case in crises and conflicts have been observed in India and Pakistan and during the war in Kosovo, which included denial-of-service attacks against the White House website. See Varma (1999) and Messmer (1999).

⁷Or, in the case of the widely cited figure of 250,000 attacks in 1995, the result of somewhat liberal interpretations of what constitutes an attack, and a potentially questionable extrapolation on the basis of the experience of a rather small number of defense systems

⁸We believe that the Army could make quite good use of classified data, however, if used as we describe in our methodology.

⁹In any case, we detect more than a little hyperbole in many of these statements.

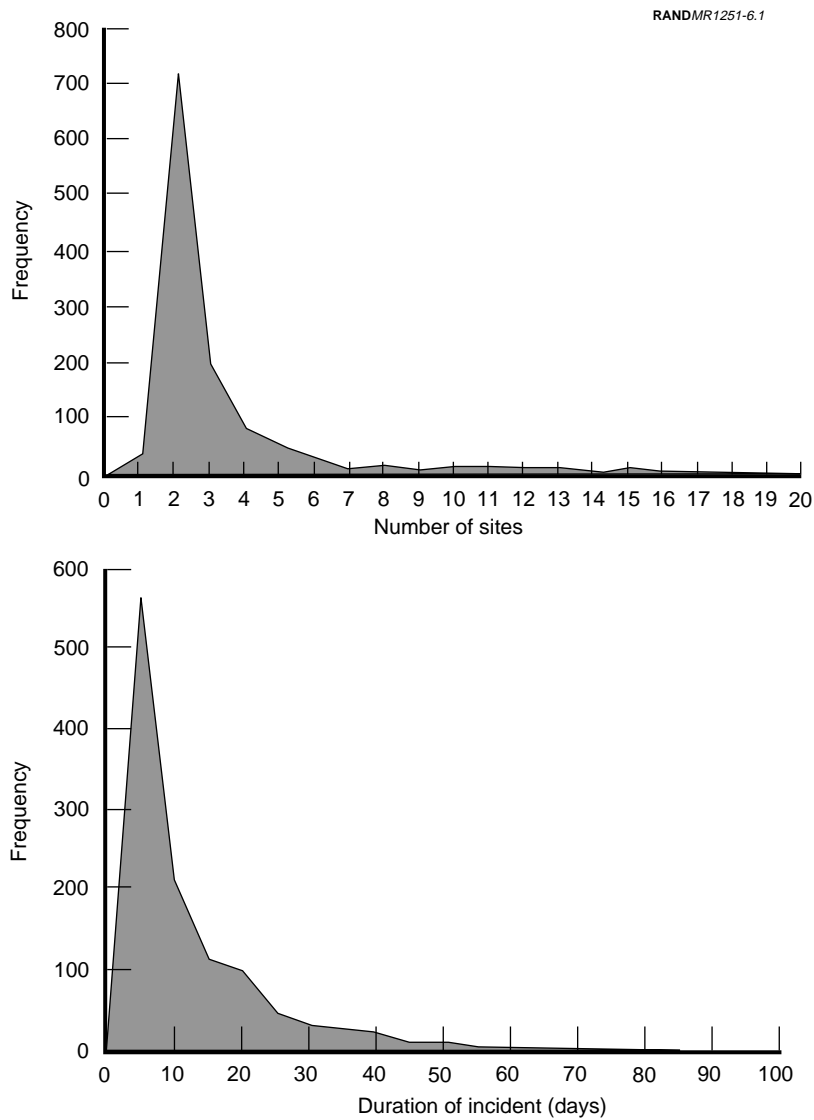


Figure 6.1—Two Measures of Consequence for Cyber Attacks (CERT/CC)

sequence predominating but with long tails containing occasional incidents of much greater consequence.

The two panels of the figure are built from data from the Computer Emergency Response Team Coordination Center (CERT/CC) for 1995 and convey two different measures of consequence.¹⁰

The top panel uses the number of sites involved in an incident to connote the magnitude of consequence, while the bottom panel uses the duration in days of incidents.¹¹

The trend data suggest a growing threat. Figure 6.2 presents CERT/CC trend data on computer incidents, showing the number of incidents handled, the number of hot line calls received, and the number of mail messages handled.

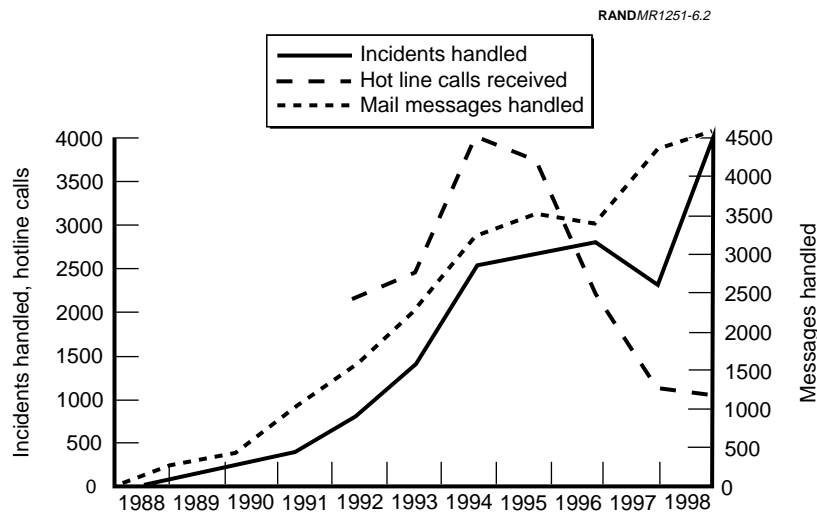


Figure 6.2

SOURCE: CERT/CC, 1999.

Figure 6.2—Various CERT/CC Measures of Cyber Attacks, 1988–1998

¹⁰The authors wish to thank RAND colleague John Pinder for providing these data, which were used in Howard (1997).

¹¹Of course, we would want to monitor a number of other, more-specific measures of consequence, such as the number of incidents involving the destruction or theft of critical files.

Two of the measures (incidents handled and mail messages received) show fairly consistent annual growth, while the third (hot line calls) shows a decline. How much of the growth results from increases in the number of attacks and how much it reflects an increasing ability to detect or willingness to report such attacks is unclear.

Data from the Federal Computer Incident Response Capability (FedCIRC, see Figure 6.3) suggest the number of federal computer security incidents has generally been below 100 per month, but these incidents vary greatly in the number of affected sites, apparently stemming, in the main, from such computer viruses as Melissa and ExploreZip.¹²

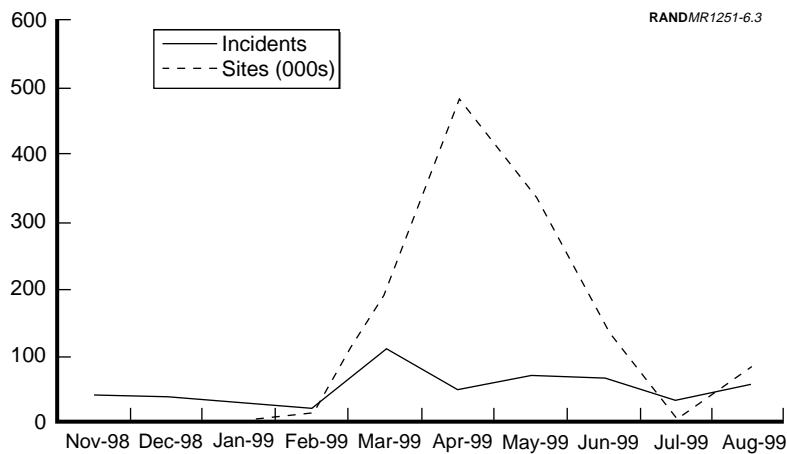


Figure 6.3—Federal Computer Security Incidents and Sites¹³

¹²We suspect that the increase over March–April 1999 is attributable to the Melissa virus. According to *U.S. News and World Report*, hundreds of thousands of computers were infected by Melissa. To aid in interpretation, CERT/CC's advisory on Melissa is dated March 27, 1999, while its advisory for the ExploreZip virus is dated June 10, 1999. Of the 59 incidents reported in August 1999, 23 were attributed to reconnaissance efforts, 10 were of unknown type, nine were information requests, six were root compromises, five were viruses, four were denials of service, two were user compromises. See Mitchell (1999).

¹³Monthly data are available from <http://www.fedcirc.gov>.

Data from the Army’s Land Information Warfare Activity’s (LIWA’s) Army Computer Emergency Response Team (ACERT, see Figure 6.4) show an increasing frequency of attacks, although again, it is impossible to separate actual increases from improved detection and reporting capabilities.

Taken together, while the open-source data are somewhat incomplete, relatively compelling evidence suggests increasing incidents and numbers of affected sites.

Weapons

Conventional Weapons and WMD. It is entirely possible that WMD could be used, but significant impact could be felt even in uses of small arms or other portable weapons. In particular, because of their portability and lethality, three types of threats would seem particularly attractive to enemy special operations forces or saboteurs bent on disrupting U.S. military operations, facilities, or systems:¹⁴

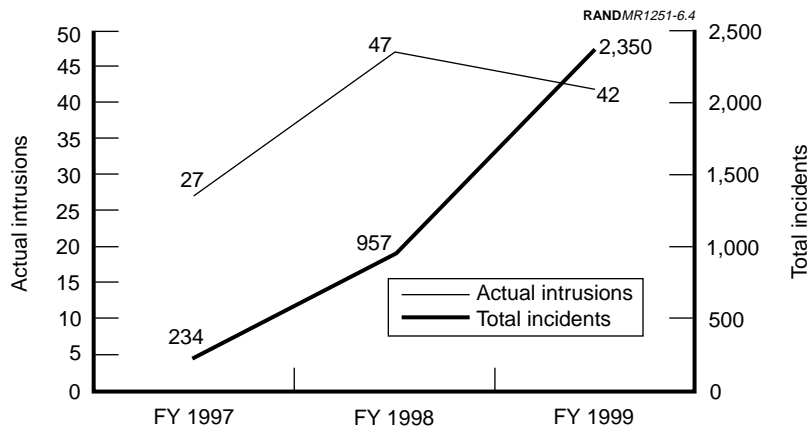


Figure 6.4—Incidents and Actual Intrusions of Army Systems¹⁵

¹⁴Some attacks on the United States may not be terrorism but rather acts of war brought to the U.S. homeland.

¹⁵Year-to-date data for 1999 are as of June 1999.

- Man-portable air defense missiles, such as Stingers, are of significant concern, since they could be used either against deploying airlifters or commercial carriers, and in either case result in hundreds of victims.¹⁶
- Rocket-propelled grenades (RPGs), which also could be used against low-flying aircraft as well as against troop convoys.
- Mortars, which were used effectively in an attack on a Sarajevo marketplace and could easily be used against a fort or Air Force base or against a port facility.

Cyber Attacks. While mission-critical systems could be attacked by conventional means, it seems more likely to us that, with the proper training, planning, and preparation, a committed adversary could launch computer attacks on mission-critical computer systems and networks.¹⁷

Potential Targets

Potential targets are divided into four general classes: deploying forces, mission-critical facilities, mission-critical systems, and higher headquarters.

Deploying Forces. In the context of a larger military action, early deploying forces will be among the most attractive targets for asymmetric attacks. The reasoning is that such forces can halt invasions and stabilize the situation on the ground in anticipation of counter-offensive operations. By this reasoning, a campaign against deploying Army units would probably preferentially target such early deploying forces as the Ready Brigade of the 82d Airborne Division

¹⁶According to press reporting, in 1989 DoD estimated that between 200 and 500 Stinger missiles were in the hands of the Afghan mujahedin (Weiner, 1994a).

¹⁷The reason we judge cyber attacks on critical computer systems and networks as more likely than conventional attacks is that the difficulties and costs of mounting computer attacks appear lower than conventional attacks on critical nodes and communications systems, and the opportunities for deception and deniability appear higher. Indeed, recent experience suggests that cyber attacks are far more prevalent than conventional attacks on mission-critical systems and networks. In the event that an adversary were willing to use special operations forces or terrorist capabilities for conventional attacks on military targets in the United States, however, mission-critical computer systems and networks could prove to be attractive targets.

and advance echelons of mechanized and armored forces.¹⁸ These attacks probably would be directed at such power projection platforms as airfields where U.S. forces are deploying and probably would aim to kill large numbers of troops through such actions as downing one or more airlifters.

Mission-Critical Facilities. For the Army's purposes, continuity of operations in the sense of force protection and the continuous operation of mission-critical facilities and systems seems most likely to be placed at risk by attacks on the forts that maintain deployable forces, the air and sea ports of embarkation (APOEs/SPOEs), and key depots and ammunition facilities.¹⁹

Mission-Critical Systems. Continuity of operations, in the sense of Critical Infrastructure Protection of mission-critical systems (computers, networks, and communications systems), could be jeopardized either by attacks using small arms and other light weapons, those using mortars or RPGs, or through the use of so-called "cyber attacks."²⁰

The Year 2000 remediation problem provides insight into the nature of the potential target set of mission-critical systems. According to Secretary of Defense William S. Cohen, the DoD has

10,000 separate computer systems involving 1.5 million individual computers which are spread at hundreds of locations across the globe. Of these, over 2,000 systems are so-called mission-critical—communication, navigational, targeting systems—that absolutely must work for the military to meet its missions on January 1, the year 2000. In fact, over one-third of the government's critical systems are in the Department of Defense.²¹

¹⁸By the same logic, Air Force and other early deploying airpower will be preferred targets, since they will be essential to the halt phase of a major theater war. Marine Air Ground Task Forces (MAGTFs) also could be attractive targets for asymmetric attacks.

¹⁹See Appendix I for a listing of illustrative mission-critical facilities. The Army should evaluate the list to determine priorities, e.g., on the basis of whether units or facilities are critical to early deployments.

²⁰See Appendix I for a listing of illustrative Army mission-critical systems that could come under attack. The list might be too inclusive. The Army should constantly evaluate which systems are mission-critical ones.

²¹Of these, 198 are mission-critical, nuclear-related systems (DoD, 1999d).

According to the GAO, as of February 1998, the Army had 376 mission-critical systems and nearly 20,000 nonmission-critical ones;²² DoD mission-critical systems totaled 2,915, and DoD non-mission-critical systems totaled 25,671, and total networks were estimated at 10,000 (GAO, 1998a, pp. 1 and 10).

Higher Headquarters. To be sure, the continuity of higher headquarters operations ensures the integrity of command and control, but it also provides the connecting link between the continuity of military operations and the continuity of government.²³ For both reasons, threat and risk assessments should be used to establish what actions should be taken to assure the continuity of headquarters operations.

Net Assessment

With the possible exception of cyber threats—where attacks appear already to be under way but where data on the frequency and magnitude of consequence of these attacks are notably lacking—we believe that most threats to continuity of operations are at best future, not imminent ones.

As described in Chapter Four, the bars to WMD appear to be rather higher than often is acknowledged, but it seems probable that U.S. adversaries at some point will acquire these weapons. Although such weapons could be used to disrupt U.S. future military operations, other weapons, ranging from small arms to man-portable missiles, rocket-propelled grenades, and mortars appear more likely.

Thus, as with the domestic preparedness task area and as will be discussed in the remainder of this chapter, our recommendation is that efforts should begin to, at a minimum, assess more carefully and plan against these threats, while making selected investments to mitigate the threats to key warfighting and supporting units,

²²The GAO reported that the Army had a total of 18,731 nonmission-critical systems. See GAO (1998c, p. 8).

²³We consider higher headquarters to include OSD and OJCS; Headquarters, Department of the Army; the headquarters of the various CONUS armies; the headquarters of CONUS-based CINCs; and other, comparable high-level commands.

mission-critical facilities and systems, and higher headquarters. Larger investments should await more complete analysis.

Threat Campaigns

If one takes seriously the possibility of asymmetric attacks against the homeland in response to the deployment of U.S. conventional military capabilities or in an act of regime preservation to coerce the United States to cease military operations before the total defeat of the adversary, then it is relatively easy to envision a determined adversary undertaking an extended campaign against the United States.

In such a situation, it is possible to envision simultaneous attacks on multiple military targets, a sequence of attacks against such high-payoff targets as deploying airlifters, or a differentiated strategy in which attacks on military targets are interspersed with attacks on civilian targets. Such a campaign could easily tax civilian and military capacity. It might do this, for example, by requiring extended alerts or by exhausting one-of-a-kind capabilities.²⁴

Put another way, although the threats and risks now seem relatively remote and with the capacity for the use of WMD yet to be proved, a future, sustained conventional campaign against U.S. military forces could prove quite stressing.

PERFORMANCE MEASURES

Performance measures for continuity of operations and COG activities appear to be somewhat similar, although the specific activities depend on which aspect of this problem set is considered.

Prevention Activities

Because the threats are assumed to overlap with those in the domestic preparedness task area—state and nonstate sponsors of terrorism and disaffected domestic groups—the same sorts of prevention-

²⁴For example, there is only one USMC Chemical Biological Incident Response Force (CBIRF).

based performance measures apply, e.g., the number of actual attacks, the number of known, credible attack plans discovered, and the number of preventions.

Preparedness Activities

Threat and risk analyses would lead to a prioritization of potential mission-critical targets, whether focused on the continuity of headquarters operations, critical facilities, or critical systems and networks. A wide range of preparedness activities could then be undertaken, including improving defenses (e.g., hardened facilities, improved network security for systems) and contingency planning for relocation.

Measures for preparedness activities would aim to reduce the level of damage and the time that any set of mission-critical assets was unavailable. These measures could include

- percentage of mission-critical facilities that have a high capability to withstand attack (e.g., blast effects or introduction chemical or biological attack);
- expected maximum time that normal operations of mission-critical organizations or facilities are likely to be disrupted;
- expected maximum time mission-critical facilities are unavailable; and
- expected maximum time until mitigation or reconstitution capabilities are deployed.

Response and Reconstitution Activities

Some of the operational measures associated with responses in the domestic preparedness area also would apply to response activities. Added to these, however, would be the speed at which headquarters could be relocated to areas of lower risk.

In addition to response performance, planners also need to consider performance in terms of the speed with which basic functions and services can be restored. Perhaps the best measure would be time, i.e., the time until operations can resume at their normal tempo.

Threat Campaigns

An additional measure of performance would be the ability to sustain the full range of continuity operations over a sustained threat campaign that involved multiple attacks in dispersed locations.

NOTIONAL PERFORMANCE LEVELS

We believe technical analyses and policy deliberations could lead to lower or higher levels than those suggested below but offer the following notional performance levels for the continuity of operations task area to provide a flavor of the levels we have in mind:

- For Force Protection of deploying forces, the capability of deploying forces to suffer no more than one half-day delay in mobilization and deployment as a result of attacks on fort-to-port movements or mission-critical facilities and systems. We believe that limiting delays to a half day would minimize the flow of forces to a military contingency.
- For mission-critical facilities, the ability to reconstitute and restore operations within one day.
- For mission-critical systems, networks, and communications systems, an ability to detect and isolate or terminate all external intrusions within minutes of penetration and an ability to reconstitute mission-critical systems, networks, and databases within three hours of penetration.
- For Continuity of Headquarters Operations, an ability to recover and reconstitute headquarters and mission-critical functions within 12 hours of an attack.
- For threat campaigns, an ability to sustain continuity operations activities over at least 60–90 days in the face of enemy attacks.

PROGRAM DESIGN ISSUES

Force Protection

In most cases, force protection is organic to units and their bases, i.e., the commander for each unit and base is responsible for meeting

force protection needs.²⁵ Table 6.1 describes the sorts of capabilities available to support enhanced force protection activities.

The DoD, furthermore, has embarked on a DoD Force Protection Initiative:

The Secretary of Defense has tasked the [Chairman of the Joint Chiefs of Staff] to review the force protection capabilities of U.S. forces worldwide. Several DoD Agencies and OSD organizations are actively involved in this initiative. Currently, each Service is responsible for protecting its own personnel and facilities. Near-term force protection enhancements are being fielded through the Physical Security Equipment Action Group under the guidance of the Physical Security Equipment Steering Group (chaired by the Director of Strategic and Tactical Systems, PDUSD (A&T) (S&TS)) and funded under the OSD Physical Security Equipment Program.

Table 6.1
Force Protection Capabilities

	Type of Event					
	HE	CHEM	BIO	RAD	NUC	CYBER
Operational Capabilities						
Installation alert system and physical security measures	X	X	X	X	X	
Installation military police	X	X	X	X	X	
Tenant units and their security SOP	X	X	X	X	X	
Local police, fire, and rescue services	X	X	X	X	X	
Local FBI	X	X	X	X	X	X
ATF	X	X		X	X	
Civilian port and airport police	X			X	X	
Reachback Capabilities						
USACOM J-2						
Installation G-2	X	X	X	X	X	X
DIA	X	X	X	X	X	X
FBI intelligence	X	X	X	X	X	X
State and local police	X	X	X	X	X	

²⁵The dictum of “mission first, people always” applies.

These efforts are being coordinated with the technology development activities of the [Technical Support Working Group Counterterrorism Technical Support] TSWG/CTTS. DSWA is supporting the initiative by conducting force protection assessments of facilities worldwide, fielding assessment teams to identify and evaluate force protection shortfalls, and assisting commanders in rectifying the identified shortfalls. The CBD Program is also assisting in this effort. The CJCS has approved DSWA's proposed methodology and concept of operations for conducting the assessments. Using ideas and inputs to fulfill CINC and Service requirements to address force protection shortfalls. Key milestones are to i) complete 50 assessments by the end of calendar year 1997 and complete 100 assessments by the end of 1998; ii) continue to apply the latest technology to achieve enhanced force protection; and iii) define a prioritized technology R&D plan to address key force protection shortfalls. (CPRC, 1997, Section Eight, "DoD, DOE, and U.S. Intelligence Programs for Countering Paramilitary and NBC Threats.")

Although the threat of such an eventuality is currently judged to be low, in an asymmetric enemy campaign against deploying forces and their power project platforms, the organic assets that provide force protection could easily prove inadequate. As described above, particular concern is warranted about the vulnerabilities and force protection of early deploying forces, particularly when they are massed at air bases or seaports, or on board airlifters.

The Army should work with the other services, predominantly the Air Force and Navy, to establish what sorts of enhanced force protection might be possible to reduce the vulnerability of deploying forces and to clarify the respective roles of the services for providing this protection. Particular attention should be given to the vulnerability of APOEs and SPOEs and to the vulnerability of airlifters as they egress fly-out zones adjacent to air bases. The Army and Air Force should jointly explore the trade space associated with alternative concepts for enhancement of force protection (e.g., additional security forces versus equipping airlifters with decoys, chaff, or other countermeasures).

Continuity of Operations

Table 6.2 describes what appear to us to be the key continuity of operations capabilities in the National Capital area.²⁶ These capabilities include a host of DoD, joint, and service activities that could play important roles in the continuity of operations task area.²⁷

Although these capabilities are judged to be adequate under normal circumstances, it seems likely that they would be greatly stressed by a prolonged enemy asymmetric campaign against deploying forces and mission-critical facilities.

Mission-Critical Facilities

In 1997, DoD-wide efforts to improve the security of mission-critical facilities included an OSD Joint Physical Security Equipment Program that aimed to undertake RDT&E that would enhance the security of forces and mission-critical facilities:

This program consolidates related DoD Joint Service and Agency RDT&E programs developing advanced technologies for protecting critical, high-value military assets from paramilitary, terrorist, intelligence, and other hostile threats. Efforts focus on protecting personnel, facilities, and high-value weapon systems, including nuclear and chemical weapon systems and storage facilities. This program is serving as the focal point for near-term upgrades to U.S. facilities under the Force Protection initiative discussed above.

Key accomplishments since last year's report include: i) completion of numerous qualification tests and evaluations of integrating video motion detection capabilities into the Tactical Automated Security System; ii) installation of an interior Mobile Detection Assessment Response System in a Naval facility for operational evaluation; iii) installation of a Waterside Security System at Submarine Base Kings Bay, Georgia; iv) testing of promising commercial off-the-shelf technologies for the Portable Explosive Detection project; and v)

²⁶Many of these are deployable to locations outside of the District of Columbia.

²⁷Service headquarters also should be included.

Table 6.2
Continuity of Operations Capabilities in the National Capital Area

	Type of Event					
	HE	CHEM	BIO	RAD	NUC	CYBER
Operational Capabilities: DoD						
Defense Protective Service	X	X	X	X	X	
Defense Information Systems Agency					X	X
Defense Communications Agency	X	X	X	X	X	X
Criminal Investigation Command	X	X	X	X	X	X
Military District of Washington MPs	X	X	X	X	X	
Army Computer Emergency Response Team (ACERT)						X
USMC/Navy security detachments	X	X	X	X	X	
Other Operational Capabilities						
National Capitol Region hospitals and clinics	X	X	X	X	X	
Reachback: DoD						
INSCOM	X	X	X	X	X	X
DIA	X	X	X	X	X	X
JTF-CND	X	X	X	X	X	X
Walter Reed AMC	X	X	X	X	X	
Criminal Investigation Command	X	X	X	X	X	X
Defense Information Systems Agency					X	X
Defense Communications Agency	X	X	X	X	X	X

NOTE: This chart treats only those Military District of Washington assets and National Capitol Region assets that might be involved. From the perspective of an outsider, any of the physical attacks and the responses to them would involve the agencies that normally respond to a domestic preparedness event.

demonstration of prototype sensor hardware for various detection systems. (CPRC, 1997, Section Eight, “DoD, DOE, and U.S. Intelligence Programs for Countering Paramilitary and NBC Threats.”)

The Army should perform the necessary threat and risk assessments to assist in developing formal risk management programs that can be

used as a basis for prioritizing and allocating resources, and these assessments probably should focus on mission-critical facilities at home, such as power projection platforms.

Mission-Critical Systems

Although the threat data basically conform to the sort of distribution described in Chapter Three, the threat of cyber attack requires a slightly different interpretation: Rather than seeking to prepare for events of a given magnitude, the aim instead is to keep the consequences below a specific threshold.

Preferential attention and resources should be given to mission-critical systems that support power projection and the employment of military forces to conduct assigned missions.²⁸ As in other areas of emerging threat, the GAO has advocated the use of threat and risk assessment and risk management and cost-effectiveness to guide DoD responses to the cyber threat.

In addition, since absolute protection is not feasible, developing effective information systems security involves an often-complicated set of trade-offs. Organizations have to consider the (1) type and sensitivity of the information to be protected, (2) vulnerabilities of the computers and networks, (3) various threats, including hackers, thieves, disgruntled employees, competitors, and in Defense's case, foreign adversaries and spies, (4) countermeasures available to combat the problem, and (5) costs.

In managing security risks, organizations must decide how great the risk is to their systems and information, what they are going to do to defend themselves, and what risks they are willing to accept. In most cases, a prudent approach involves selecting an appropriate level of protection and then ensuring that any security breaches that do occur can be effectively detected and countered. (GAO, 1996a, pp. 1-2.)

²⁸The GAO indicated that, DoD-wide, resources for Y2K remediation efforts were being spent on nonmission-critical systems even though most mission-critical systems had not been corrected (GAO, 1998a, p. 2). An illustrative list of potential mission-critical systems can be found in Appendix I of this report.

The GAO further recommends a range of actions that can be taken to reduce threats and risks, with decisions ultimately to be based on the analytic or business case that results from risk assessments.

This generally means that controls be established in a number of areas, including, but not limited to: a comprehensive security program with top management commitment, sufficient resources, and clearly assigned roles and responsibilities for those responsible for the program's implementation; clear, consistent, and up-to-date information on security policies and procedures; vulnerability assessments to identify security weaknesses; awareness training to ensure that computer users understand the security risks associated with networked computers; assurance that systems administrators and information security officials have sufficient time and training to do their jobs properly; cost-effective use of technical and automated security solutions; and a robust incident response capability to detect and react to attacks and to aggressively track and prosecute attackers. (GAO, 1996a, pp. 1-2.)

In the area of cyber threats, prevention, preparedness, and response activities should focus on mission-critical systems, i.e., those systems essential to undertaking or supporting military operations and other key missions.

Unfortunately, the absence of reliable data makes it impossible to establish where the greatest payoffs might be. Consider the following instructive example: Most of the discussion in the broader policy environment is focused on "cyber attack" by state and nonstate actors, and great interest lies in developing advanced technologies to detect and mitigate these threats. However, it generally has been established in the private sector that insider misuse is a more frequent problem than "cyber attacks" from outside organizations.²⁹ If

²⁹In the 1999 Computer Security Institute/FBI survey of computer crime, 24 percent of the organizations reported system penetration by an outsider, while 76 percent reported insider abuse of net access and 43 percent reported unauthorized insider access to information. Seventy-nine percent of these organizations judged as unlikely the possibility of foreign government involvement, and 70 percent judged as unlikely the possibility of foreign corporation involvement. Nevertheless, the number of reports of system penetration by outsiders, unauthorized access by insiders, and theft of proprietary information rose from 1998 to 1999. See CSI/FBI (1999) and Department of Defense (1999c).

A study of the threat of insider misuse in the DoD has recently been published.

DoD experience is at all comparable, it would suggest that, rather than emphasizing external attacks, the greatest emphasis should be placed on ensuring that routine administrative and security controls are being effectively implemented to guard against this sort of misuse.³⁰

The Department of Defense has taken some actions already on the threat of computer attack, including removing potentially sensitive information from web-accessible locations (Hamre, 1998b), reducing to six the number of “portals” through which Internet users can access DoD computers (Bender, 1999), and standing up a computer network defense center, a Joint Task Force-Computer Network Defense (JTF-CND), and a DoD Computer Emergency Response Team (DoD CERT) (Keeter, 1999, p. 7; Wolfe, 1999, p. 1).³¹

Within the Army, in addition to the consolidation of Information Assurance activities in LIWA and the Army Computer Emergency Response Team (ACERT), an active-duty/reserve component initiative to strengthen the Total Army’s information operations posture is under way. The plan is to expand LIWA’s ability to respond to emergencies using reserve component CERT/Vulnerability Teams as well as providing tactical commanders with trained reserve component information operations (IO) sections to plan, coordinate, and execute “full spectrum information operations” (DAMO-SSW, 1999).

³⁰As reported by the National Research Council: “Troops in the field did not appear to take the protection of their C4I systems nearly as seriously as they do other aspects of defense.” See National Research Council, *Realizing the Potential of C4I: Fundamental Challenges*, reported in Saldarini, undated. Saldarini reported the following:

[r]eviewers observed instances of insufficient security such as sticky notes with important systems data attached to computers. In other instances, computers holding sensitive information were found to be vulnerable to hostile applets from the World Wide Web. The report attributed slack computer security to a DoD organizational culture accustomed to mounting offensive attacks. Cyber-terrorist threats instead must be countered with defensive action.

For example, it may well be that 95 percent of the attacks can be prevented by simply making sure that system administrators disable accounts when users leave an organization, that system-level passwords are changed routinely, and that other, similar low-tech measures are taken.

³¹The DoD CERT reportedly consolidated the functions of two earlier teams: ASSIST, which monitored intrusions and provided responses to the attacks, and DIAMOND, a group that surveyed past attack data to enhance future network security.

The ARNG has launched a 15-state Information Operations pilot program that includes nine CERTs with six at the state level, two in direct support of LIWA, and one CERT located at the National Guard Bureau (NGB). Additionally, nine Tactical IO Sections (four division level and five for enhanced brigades); four Vulnerability Assessment Teams (VATs), two of which will be in direct support of LIWA and two supporting National Guard networks and tactical units; and five Field Support Teams have been established. The ARNG's goal in FY 2000 was to establish ARNG CERTs at the NGB and in each state; create five field support teams and four VATs in support of the JTF/theater commanders and warfighting exercises; and establish IO sections in all eight combat divisions and in all 15 enhanced brigades by December 2000 (DAMO-SSW, 1999). The USAR's aim for FY 2000 was to establish three fully mission-capable IO Centers and a LIWA Enhancement Center (DAMO-SSW, 1999).

A number of serious efforts have gone into providing detailed recommendations on reducing the exposure of systems and networks to threats.³² Although choices should be guided by formal threat and risk assessments, and cost-effectiveness and tradeoff analyses, the following examples will provide a sense of the range of possible actions:

- Improving data on incidents of cyber attack, including capabilities to log suspect activity and analyze these data to discern emerging patterns of activity that need to be addressed.³³ In such a case, there might be tradeoffs between monitoring capabilities and computer performance for legitimate users.
- Prioritizing information assurance efforts to invest preferentially in efforts to protect mission-critical systems at highest risk.

³²For example, the Defense Science Board (1996) provided 13 overarching categories of recommended actions and 50 specific actions to improve the defensive information warfare capabilities of the DoD. See Appendix J of this report. The President's Commission on Critical Infrastructure Protection (1997a, pp. 60–62) provided the outlines of a strategy that included activities in policy formulation; prevention and mitigation; information sharing and operational warning; counteraction (incident management); and response, restoration, and reconstitution (consequence management). See Appendix K for a listing of these activities. Also see Ware's (1998) recommendations and the recommendations in Department of Defense (1999c).

³³According to press reporting, this is one of the functions being performed by the DoD CERT and possibly Army CERT.

- Performing risk assessments and developing realistic contingency plans for critical systems and activities in the event that service is disrupted.
- Removing mission-critical systems from Internet-accessible servers or placing them on less vulnerable platforms.³⁴ In this case, the tradeoff would include the costs of having to create or have users rely on secure systems for unclassified computing on mission-critical systems.
- Routine efforts by system administrators to remove old accounts, to change all system-level passwords, and other administrator functions that can reduce vulnerabilities.
- R&D in furtherance of better capabilities to detect and track intrusions and insider misuse, to locate the intruders, and to terminate these sessions. Cyber-counterattacks and FBI action are also being used.³⁵

In particular, the Army should continue to develop a more comprehensive and reliable incident data collection effort to assist in understanding the nature of the threats and risks it faces.³⁶ Such an effort would seek to develop taxonomies to facilitate threat and risk assessments and make possible a “divide-and-conquer” approach to target the highest-priority threats and risks with cost-effective solutions. We believe the best strategy would be the one that

- defines Army-wide, given the potential for inconsistent execution in information assurance activities, which systems are mission-critical and which are to have some sort of centralized execution of information assurance activities;³⁷

³⁴The Army reportedly has switched from Windows NT to Mac OS-based servers for its home page (“Tired of Hacks,” 1999).

³⁵Pentagon computers reportedly responded to an attack in the form of a flood of requests by “flooding the browsers used to launch the attack with graphics and messages, causing them to crash” (Schwartau, 1999). The FBI also has begun raiding hackers’ homes (CNN, 1999c).

³⁶ACERT and LIWA have the beginnings of such an effort.

³⁷Efforts to ensure system security could be centrally executed, for example, by a security manager associated with each mission-critical system, who would assure its security by validating the dispersed base of user sites.

- establishes the necessary training and procedures to ensure that routine administrative actions (e.g., disabling of old accounts, changing system passwords, installing patches for newly discovered vulnerabilities, installing upgraded security software) are taken;
- on the basis of cost-effectiveness and tradeoff analyses, enables decisions on which systems also should benefit from other actions, e.g., moving the system from an unsecured network (telephone or web-accessible) to a more secure (e.g., NIPRNET or SIPRNET) network, installing additional detection and monitoring software; and
- continues to invest in long-term software RDT&E efforts to develop code that can substantially reduce the risk to mission-critical systems.

Threat Campaigns

As described above, an extended threat campaign that attacked dispersed targets could exhaust capabilities and erode readiness to prevent or respond to still other attacks. Accordingly, an important capacity issue is the rotation base that might be required. In fact, the possible future need for a rotation base might be one of the most important arguments in favor of conversion of the Guard to homeland security functions.

BUDGETING ISSUES

Federal Spending

Because federal funding is reported in governmentwide aggregates, it is exceedingly difficult to establish the funding levels associated with DoD and Army continuity of operations programs.

It is known, for example, that the President's FY 2000 budget included \$206 million to protect federal government facilities (White House, 1999a); and \$1.464 billion to address critical federal infrastructure protection (White House, 1999a), including

- \$500 million for a Critical Infrastructure Applied Research Initiative;
- \$2 million for intrusion and detection systems;
- \$8 million for Information Sharing and Analysis Centers (ISACs); and
- funding for a “Cyber Corps” to respond to attacks on computer networks (White House, 1999a).

In the area of threats to computer systems and networks, the General Services Administration, the Critical Infrastructure Assurance Office, the National Security Agency, and the FBI’s National Infrastructure Protection Center are developing a Federal Intrusion Detection Network that will provide a common center for response to cyber attacks on federal departments and agencies. The system reportedly is based on the DoD’s incident-reporting network, which is said to be further along than civilian agencies’ efforts (Frank, 1999). More recently, the Clinton Administration offered a revised plan that, it was hoped, would raise fewer fears about on-line privacy (White House, 1999c; O’Harrow, 1999, p. A31).

The Senate Armed Services Committee has reported that DoD-wide information assurance activities are underfunded:

The committee notes the important steps taken by the administration and the Department to secure critical information infrastructures. In particular, DOD has established a Task Force for Computer Network Defense, a Defense-wide Information Assurance Program, and an integrated working relationship with the National Infrastructure Protection Center at the Federal Bureau of Investigation. Notwithstanding these positive steps, significant funding deficiencies remain in the Department’s fiscal year 2000 budget request and the FYDP for information assurance and related matters.

During a hearing on March 16, 1999, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I) stated that a \$420.0 million increase to the fiscal year 2000 budget request and a \$1.9 billion increase to the FYDP would be required for information assurance programs. These funding shortfalls are of great concern to the committee. Therefore, the committee recommends additional funding in this area and provision that

would strengthen the Department's information assurance program and provide for improved congressional oversight. (U.S. Senate, 1999, pp. 7-8.)

In large part, this funding shortfall appears to have been because the Critical Asset Assurance Program (CAAP), which was slated to address the security of facilities and systems, essentially was an unfunded mandate ("DoD: Infrastructure," 1999, p. 1).³⁸

As of late summer 1999, the DoD planned to create a new program to replace CAAP, and was weighing additional funding for infrastructure protection;³⁹ including increased funding for R&D aimed at improving detection and reducing the vulnerability of defense computer systems.⁴⁰ The Senate Armed Services Committee approvingly cited the ASD (C3I)'s claim that a \$420.0 million increase to the FY 2000 budget request and a \$1.9 billion increase to the FYDP were required to address information assurance problems (U.S. House of Representatives, 1999b, pp. 7-8).

This suggests to us that DoD (and the Army) may be faced not so much with the question of how it will pay for information assurance but rather what the priorities and allocation of resources should be to protect its computer systems and networks. As described earlier, it seems that justifications for programs to mitigate threats increasingly will need to rely on formal threat and risk assessments and cost-effectiveness analysis.

Army Spending

The Army also tends to deal in budgetary aggregates when spending on the security of systems and facilities is concerned. These data suggest that Army-wide spending on security programs will increase

³⁸The CAAP ultimately was canceled in August 1999.

³⁹The report suggested that one option under consideration was to put \$149 million in additional funding into the FYDP for information assurance activities.

⁴⁰This may include a spending increase for a DARPA demonstration project on a computer system concept that employs random network paths and computer redundancy techniques to reduce the vulnerability of military information technology systems (U.S. Senate, 1999, p. 227).

through FY 2001, while spending on information security is hovering around \$40 million annually.⁴¹

CONCLUSIONS

The analysis provided in this chapter has suggested that the continuity of operations task area consists of three principal activities: force protection for deploying forces, the protection of mission-critical facilities and systems, and the continuity of higher headquarters operations.

Our analyses suggest that, although the threats seem remote, it is prudent to begin planning now to ensure the continued security of Army forces, facilities, systems, and higher headquarters and, in the case of computer systems and networks, actually make investments. In other words, planning should begin for additional force protection capabilities, although acquisition of additional capability in other than cyber areas should be delayed until formal threat and risk assessments and cost-effectiveness and tradeoff analyses reveal where the greatest leverage is to be found. In the case of computer security, investments also should have an analytic basis.

In the area of force protection, it may be desirable to plan for more robust monitoring and surveillance capabilities near key forts, ports, and airfields, as well as capabilities for assuring the safety of fly-out zones and air corridors. It is easy for us to imagine hundreds of deaths resulting from a missile attack on a departing airlifter, as well as the cessation of deployments until security is established.

Multiple attacks within CONUS against civilian and military targets during a wartime mobilization also could stress low-density assets that have dual missions of warfighting and homeland security (e.g., the TEU, but also chemical units). In such a circumstance, military commanders could be confronted with the need to leave behind certain low-density units for homeland security activities that also

⁴¹Security Programs (BA 4) constituted \$372 million in 1998, \$402 million in 1999, \$427 million in FY 2000, and \$439 million in FY 2001, while spending on Information Security in the Other Procurement, Army, category, was \$26 million in FY 1998, \$44 million in FY 1999, \$40 million in FY 2000, and \$42 million in FY 2001 (Assistant Secretary of the Army, 1999a, pp. 40–41; 1999b, p. 19).

would be needed for force protection in theater (Joint Chiefs of Staff, 1999).

In the area of protecting mission-critical facilities and systems, it is necessary to begin with an end-to-end analysis of key missions and the facilities and systems essential to the accomplishment of these missions and those that are not. It also appears to be critical to have centralized coordination of risk mitigation efforts, to ensure that no “weak links” are in the chain that result from varying interpretations of guidance. As suggested by the FedCIRC data, a fairly large number of computer security incidents appear to have been reconnaissance efforts to identify and probe vulnerabilities. Such incidents can be used to target remediation efforts for mission-critical systems.

In the area of protecting higher headquarters operations, security, relocation, and reconstitution plans should be reviewed for their adequacy in light of the potentially emerging threats.

As was noted at the beginning of the chapter, the continuity of military operations remains one of the cornerstones of homeland security because, without it, the Army’s ability to accomplish its assigned missions could be compromised. Because resources are likely to be limited, however, the Army should make every effort to ensure that its security investments—whether directed at protecting forces, mission-critical facilities or systems, or higher headquarters—are prioritized based on formal threat and risk assessments and cost-effectiveness and tradeoff analyses that identify where the greatest leverage is to be found.

The next chapter considers the final homeland security task area covered in this study—border and coastal defense.