

Chapter Eight described a number of illustrative planning vignettes that illuminated the sorts of capabilities that the Army might need to provide under different circumstances. This chapter analyzes Army DOTLMS and addresses the Army’s preparedness to undertake the missions identified in the vignettes. The chapter also addresses the question of adequacy of forces—whether the Army has enough of the right types of units for the likely homeland security contingencies.

The analysis began with an assessment of the DOTLMS in each of the four homeland security task areas that are the focus of this report:

- Domestic preparedness for WMD terrorism.
- COG.
- Continuity of operations, including force protection, critical asset assurance, critical infrastructure protection, and the continuity of headquarters operations.
- Border and coastal defense.

This analysis suggested that the Army’s DOTLMS have not been fully optimized for the challenges of homeland security, although areas of high capability exist. Figure 9.1 depicts our assessment of the current state of Army DOTLMS, with dark gray indicating a “high” level of capability, light gray a “medium” level, and black a “low” level.

The figure suggests that the greatest shortfalls are found in the continuity of operations areas of critical asset assurance and critical infra-

RANDMR1251-9.1

Task Area	D	O	T	L	M	S
Domestic preparedness	Dark Gray	Light Gray	Light Gray	Dark Gray	Light Gray	Light Gray
COO	White	White	White	White	White	White
Force protection	Light Gray	Dark Gray	Light Gray	Light Gray	Dark Gray	Dark Gray
CAA	Light Gray	Light Gray	Black	Light Gray	Light Gray	Dark Gray
CIP	Light Gray	Light Gray	Black	Light Gray	Light Gray	Dark Gray
HQDA CO	Dark Gray	Dark Gray	Dark Gray	Dark Gray	Dark Gray	Dark Gray
COG	Dark Gray	Dark Gray	Dark Gray	Light Gray	Dark Gray	Dark Gray
Border and coastal defense	Light Gray	Dark Gray	Light Gray	Dark Gray	Dark Gray	Light Gray

Figure 9.1—Summary of Homeland Security DOTLMS Status

structure protection and, for these two areas, in the realm of training. Where DOTLMS were assessed as less than high we then performed a screening analysis to try to identify cost-effective (i.e., high-payoff, low-cost) options for improving the relevant DOTLMS.

Next is the detailed evaluation of the DOTLMS for each homeland security task area. Where the assessment leads to a grading that is less than high, we describe the sorts of actions that would be necessary to bring them up to a high level, and their cost-effectiveness.

DOCTRINE

Domestic Preparedness

Overall, doctrine for domestic preparedness is rated high because, although the entire body of doctrine necessary for this task area has yet been developed, TRADOC is well on the way. Task lists are under

study and other progress is evident. Of particular importance will be the work already underway to develop the doctrinal underpinnings for the Response Task Forces (RTFs) and, if it is actually fielded, doctrine for Joint Task Force–Civil Support (JTF-CS).

The Army conception of WMD CSTs is in part based on the premise that the service must have a reconnaissance element establish requirements before attempting to dispatch substantial response elements to the scene of an incident. This notion, while sound in many circumstances, may be unfounded, given the need for prompt response to chemical events, the fact that other authorities—local and state—with appropriate training will most likely already be on-scene and able to provide credible assessments of initial requirements, and that biological events are most likely to be initially detected by health care providers.

COG

Army doctrine for federal COG activities is rated high. This doctrine should be reviewed periodically to ensure that it is relevant to emergent threats, however. Doctrine also should be reviewed to ensure the adequacy of local and state COG operations, at the very least, doctrine to ensure the speedy reestablishment of civilian governmental functions.

Continuity of Operations

Evaluation. *Force protection.* Doctrine for force protection is rated medium because additional doctrinal development is necessary to treat the critical issues of self-defense practices and cooperation with civilian security forces during movement to ports of embarkation.

Critical Asset Assurance/Critical Infrastructure Protection (CAAP/CIP). Critical asset assurance and critical infrastructure protection doctrine are assessed as medium because, although progress has been made in this area (e.g., creation of the ACERT), much remains to be done. Although the DoD instructions make clear the areas included in CAAP and CIP, funding has been tight, and the Army has not evolved doctrine for either of them.

For example, no clear doctrinal basis exists for identifying which facilities and systems are mission-critical, for performing the necessary threat and risk assessments that would help in targeting mitigation efforts, or cost-effectiveness or tradeoff analyses to determine the most attractive of the available options. Neither is there clear guidance on how best to hedge against the possibility of interruptions that might arise from the failure of supporting civilian infrastructures (e.g., through the establishment of stockpiles or inventories of needed materiel) or how best to speed the post-incident reconstitution of supporting civilian services. Finally, it is unclear what if any role the Army should have in protecting civilian information infrastructure. Our view is that such a role will be the exception rather than the rule.

Continuity of Headquarters Operations. Army Headquarters continuity of operations doctrine is evaluated as high because doctrine and decades of Army field practices have established the basis for reconstituting the functions of any key headquarters. Nevertheless, the unique functions of Army Headquarters (e.g., its Title 10 functions raising, training, and equipping forces) and the size and scope of any reconstitution effort place a premium on exercising plans for continuity of operations. Furthermore, because most of the doctrine and planning for this area were aimed at addressing continuity of operations in the context of a nuclear exchange, doctrine and planning should be reviewed to ensure that they remain salient with regard to emerging threats.

Cost-Effectiveness Considerations. *Force protection.* Force protection doctrine currently emphasizes those actions necessary to protect U.S. forces overseas while very little attention is paid to force protection requirements for the fort-to-port deployment sequence.

To overcome this shortfall, doctrine should generate more guidance on self-defense appropriate for CONUS. The practices outlined in the guidance must be both legal (not overstepping the bounds between self-defense and police activities) and useful. Doctrine should adapt those tactical practices that could improve force protection at home station when confronting an enemy campaign plan.

In some instances, a need will arise for additional guidance. For example, normal tactical convoy security practices—rules of deadly

force—would have to be modified to fit behind the primary security offered by civilian law enforcement. In other instances, local commanders must be made more aware of their options. For example, doctrine might stress the potential desirability of taking precautionary measures when alerted to the possibility of attack. Units in their predeployment load-out areas might deploy their NBC detection equipment or increase their overall protective posture in accordance with the best current information. Or, if the concern runs toward food tampering, unit veterinarians might be detailed to inspect food service at the deployment airfield or port. Alternatively, packaged rations might be issued. Finally, there is almost sure to be a need to jointly develop procedures and doctrine with the Air Force and Navy regarding CONUS-based force protection roles and missions, particularly at points of embarkation.

Fundamentally, doctrine must provide a basis for prudent military actions for safeguarding Army forces in the United States, in conformity with peacetime law, while confronting a concerted enemy campaign aimed at attacking those forces.

The principal costs in upgrading doctrine fall in three areas: arriving at agreement with civil and police authorities on an appropriate role for deploying units; developing new doctrine, as required, to fulfill that role; and screening and selecting current tactical practices and modifying them to make them suitable for the new force protection tasks.

Any agreement with civil authorities must address the difference between today's understanding of the use of deadly force in direct self-defense and the potential requirements that arise from facing down an enemy campaign carried out in the United States. For example, will units awaiting deployment be allowed to conduct patrols to increase their own security? If so, must they wait until they are fired on before they can use deadly force? New doctrine and rules of engagement may need to contemplate other means of providing force protection—use of less-than-lethal-force weapons, for example. The principal task confronting the adaptation of common tactical practices for CONUS must deal with the reasonable public expectation that recourse to the use of force will be reserved for civilian law enforcement organizations. That is, the public is completely unaccustomed to war on its doorstep. Doctrine should there-

fore consider what steps make sense for coordinating with law enforcement officials and informing the public under circumstances where the Army must combat enemy special operations forces and similar hostile military elements on U.S. soil.

CAAP/CIP. The whole approach to critical infrastructure protection makes crafting appropriate doctrine very difficult. At its heart, the problem is a lack of DOD-wide consensus on what constitutes critical infrastructure, no standardized procedures for threat and risk assessments or cost-effectiveness and tradeoff analyses in the area, and decentralized interpretation and execution of guidance.

In fairness to the Army, the problems in this area arise at least in part because CAAP/CIP has been somewhat of an unfunded mandate. They also arise from a rather unrealistic perception that appears to be widely held in DoD, that commercial organizations will make investments to improve the security of critical infrastructure on some basis other than the business case that arises from risk assessments. Although the Army (or DoD) may have influence in cases where it is a large customer, in other—perhaps most—cases, neither mandates nor sufficiently compelling incentives may be possible.

Because OSD is currently reevaluating CAAP/CIP and Executive Branch responsibilities in this area, however, and because it appears that funding may be forthcoming for protecting mission-critical systems, the Army needs to address these issues to ensure that continuity activities are analytically justified and well-coordinated, so that available resources are well spent

Army doctrine should, to a greater extent than the CAAP program did, emphasize centralized direction, coordination, and monitoring to ensure that vulnerabilities to Army-wide mission-critical facilities and systems are treated consistently across the Department of the Army and that a realistic appraisal of the options available to enhance the security of supporting civilian infrastructures is made.

Discussions with DOMS officials indicate that installation commanders tend to be fairly parochial and short-sighted in their appreciation of what is critical. Within DoD, the process of nominating various assets as “critical” has produced an uneven collection of assets that the executive agency is responsible for surveying and, potentially, safeguarding.

To be assessed as high, doctrine for CAAP/CIP must somehow describe an Army role appropriate to safeguarding all the various types of infrastructure that potentially could be identified as “critical,” as well as the nature of any supporting infrastructure (e.g., civilian public utilities). The appropriate doctrine would have to address both the Army’s peacetime role, in which it is more or less a consultant to the infrastructure owners, and the wartime role, in which the Army is expected to take active measures to safeguard critical infrastructure in the face of an enemy campaign intended to attack, disrupt, and destroy it.

Sound doctrine also must establish the practices Army units follow. Some types of infrastructure will prove more straightforward to deal with than others. For example, it is not at all clear that the Army has leading-edge expertise in safeguarding computer and communications systems. Its ACERT notwithstanding, given the rapid changes in software and processing systems—and the constant evolution and adaptation of computer threats—the Army should not view itself as a consultant or protector for commercial systems. Therefore, doctrine must establish for the Army a reasonable role, consistent with DoD directives and mindful of its ability to influence civilian actors. That is, the Army’s doctrine should play to the service’s strengths and steer clear of those areas in which its expertise may be highly circumscribed (e.g., in caring for its own computer and communications systems).

The principal costs associated with appropriate improvements in doctrine will arise from two areas.

First, the governmental and civil sectors must reach a consensus about what constitutes critical infrastructure. Although the Army can embark on some missions without a clear consensus, without one in this case, the danger is that some asset that ought to be included might be omitted. Despite the current emphasis in the critical infrastructure debate on computers and networked electronic systems, other infrastructure may also be critical. Doctrine must anticipate the need to provide a wide variety of safeguards, perhaps including guarding physical facilities but also extending to providing other sorts of security—perhaps encryption, for example. The Army will probably face a major educational challenge in the effort necessary to acquaint the rest of the governmental and civil sectors with its

capabilities and limitations for critical infrastructure protection. The danger of unwanted outcomes also exists. For example, in the early days of World War II, many industrial officials argued for Army units to secure their plants. The point is, in undertaking the educational mission necessary to build a consensus for the Army role, the Army must be prepared to deal with bad ideas that might impinge on its primary warfighting role.

Second, as just noted, critical infrastructure responsibilities must somehow be reconciled with deployment and other warfighting tasks. Doctrine should address the critical infrastructure protection responsibilities of the table of organization and equipment (TO&E) and the table of distribution and allowances parts of the Army in such a way that the TO&E forces are not distracted by infrastructure protection tasks when they should be preparing to fight.

The use of reserve component forces may be particularly appropriate in protecting such mission-critical facilities as power projection platforms, and options to involve the Guard and Reserve should be actively explored.

Border and Coastal Defense

Evaluation. Border and coastal defense doctrine is rated medium. Although doctrine already establishes a basis for cooperation and joint operations with other services, doctrine should also specifically treat the Army role in support of the U.S. Customs Service, ATF, Coast Guard, and other agencies involved in border and coastal defense. For example, doctrine should indicate the level of involvement appropriate for troops from the general-purpose force (e.g., directly confronting intruders or merely supporting law enforcement officers) and procedures for resolving any friction that might arise.

Cost-Effectiveness Considerations. The doctrinal shortcoming attending border and coastal defense reflects the policy-level ambiguities surrounding the question. Doctrine can only mature when the Army receives appropriate policy guidance to indicate what specific role the service will have, its level of interaction with the civilian populace, and the specific types of support it will provide to other federal and local agencies. Put another way, the Army could play any number of roles in border and coastal defense, depending on the

charter worked out with the FBI, the Customs Service, and others. The Army might support at arms-length, by providing surveillance and communications, or play a more direct role, depending on the latitude available in the law and the preference of other agencies, such as the Department of Justice. The doctrinal challenge is to develop appropriate practices, tactics, techniques, and procedures for whatever role emerges.

ORGANIZATIONS

Organizations deserve careful scrutiny for several of the task areas.

Domestic Preparedness

Evaluation. Domestic preparedness organizations currently rated medium in part because of the ambiguity surrounding the utility of the WMD CSTs. A broader problem arises because the actual capacity of civilian organizations to deliver services is unmeasured, so the need for Army organizations is difficult to ascertain. The question of “missioned” forces for domestic preparedness can only be answered when the size of specific gaps in civilian capabilities is understood. Continued reliance on RTFs and JTFs—organizational approaches that have proven their worth responding to individual events—should be reviewed to determine whether these organizational forms are optimal for combating a protracted enemy campaign.

There also are some reasons for concern about the WMD CST. Although the WMD CST can perhaps be justified on the basis of providing force protection to the follow-on incident response capabilities of the RTFs, it appears to be of questionable value to localities and states. In large part, this is because it effectively lacks the key sort of capacity (i.e., decontamination) that would make the greatest contribution. It is also because it is unclear that the WMD CST can be on-scene in the four hours claimed. We have seen little evidence that the WMD CSTs can provide the claimed 24-hour-a-day, seven-days-a-week quick response capability; that sufficient Air National Guard or other mobility assets will be maintained at the necessary state of readiness and alert to move the WMD CST to the incident site in the four-hour window; or that the WMD CST will be maintained at a sufficiently high state of readiness to be on-scene in four hours.

Accordingly, the Army should examine closely the WMD CST concept; its personnel, readiness, and mobility requirements; and the full costs associated with a responsive WMD CST. The Army also should explore the possibility of a different sort of WMD CST, providing a rapid assessment and initial *decontamination* element that would exercise with state and local first responders for incidents ranging from standard hazmat incidents to WMD incidents. The Army also should examine more closely how the integration of the Pennsylvania WMD CST into “all hazards” responses, ranging from hazmat to WMD, may offer a good model for integrating WMD CSTs into state and local response systems, which might serve as a better model in terms of ensuring the WMD CST’s involvement in incident responses.

Cost-Effectiveness Considerations. The trouble with the organizations for domestic preparedness results from uncertainties about the type, frequency, and magnitude of events; shortfalls in civilian capacity to respond to them; and the resulting net requirement for support to domestic preparedness that devolves to the Army and other military forces. For the Army, the problem extends to options for providing supporting capabilities.

To achieve a high assessment, the Army must be able to base its decisions about further organizational requirements on sound threat and risk assessments and cost-effectiveness and trade-off analyses. These must be calculated at a level of detail that will allow the Army to understand whether it, among all possible providers, is capable of providing the most cost-effective capabilities in an area and, ultimately, “how much is enough.” For example, the Army needs to understand better whether WMD CSTs or some other organization (perhaps chemical companies optimized for civilian support requirements) are better situated to enhance first providers’ capabilities.

The second issue the Army must deal with to achieve a high assessment is maintaining the RTF/JTF framework as the primary basis for facing an enemy campaign plan. Although the approach makes sense as a means for dealing with individual consequence management missions, these organizations appear inadequate for confronting an enemy campaign in the United States. To garner a high assessment in organizing for domestic preparedness, the Army must

consider a total organization, complete with planning and budgeting arms as well as action arms so that, collectively, the various functions of a U.S. countercampaign can be planned, resourced, executed, and controlled. These organizations must also be adequate in number and capability to handle a threat campaign of multiple incidents, spread over time and space.

The price of attaining a high rating for organizations is fairly steep because it involves a level of problem-solving and local-federal, civil-military cooperation rarely encountered. To ascertain which organizations are necessary for domestic preparedness, the Army and its interlocutors must come to a common understanding of the total requirement to respond to an enemy domestic campaign. That task in hand, the next requirement is to establish how much response capacity exists in the civilian sector and the requirement for military capacity to round it out. Finally, it requires the Army to develop simple, industrial measures of capacity for decontamination, patient treatment, victim housing, and similar services so that civilian communities that consume Army domestic preparedness support have a common basis for ordering help.

COG

Organization for COG rates a high assessment because the program is long-standing and sized to the perceived threat. The program has undergone a number of adjustments since 1989 and could expand if future threats warranted doing so. Army COG organizations should be reviewed to ensure that they are relevant to emerging threats.

Continuity of Operations

Evaluation. *Force protection.* Organizations for force protection currently are rated high, but, if the immediacy of the threat grows, installations should consider the value of installation reaction forces to protect the fort-to-port sequence and potential for reserve component forces to enhance security at mission-critical facilities, such as power-projection platforms.

Critical Asset Assurance. Critical asset assurance organizations are judged medium because of the high degree of uncertainty surround-

ing what is critical. Until the Army garners further intelligence that enables it to discern the priorities enemy campaign plans place on attacking various assets and relies on threat and risk assessments to assist in prioritizing mitigation efforts, the service will be unprepared to create organizations to protect its own critical assets and to exercise its responsibilities as the executive agent for the CAA program in DoD.

Critical Infrastructure Protection. Organizations for critical infrastructure protection are assessed as medium for basically the same reasons. Consideration of likely enemy campaign plans is essential to understanding the value of additional specialized organizations for critical infrastructure protection (e.g., CERTs).

Continuity of Headquarters Operations. Organization for Department of the Army Headquarters continuity of operations earns a high rating because an abundance of four-star headquarters could assume Department of the Army Headquarters functions on an interim basis. Both TRADOC and FORSCOM are reasonably available. Officer assignment practices make it highly likely that a significant percentage of officers at these headquarters would have Army Headquarters experience, making them suitable temporary substitutes or staff augmentees.

Cost-Effectiveness Considerations. *CAAP/CIP.* CAAP and CIP, although distinct from each other, share common problems insofar as organizations go. In order to be rated high, they both need a clear definition of what “critical” means. Until a common picture of critical infrastructure and assets emerges, both task areas will find it difficult to determine how many and what types of organizations are necessary to fulfill the Army’s responsibilities. Both programs will remain medium until a better idea of vulnerabilities and enemy interest in various facilities emerges. Only when the dimensions of the threat are better understood will it be possible to ascertain whether the current organizations (e.g., JTF-CND) are sufficient or not.

The costs of addressing the current uncertainties about critical assets and infrastructure are considerable. In the military sector, for example, it will be necessary to assess power projection installations and facilities to determine which are mission-critical and what addi-

tional force protection capabilities are necessary. Doing so means understanding the role of civilian utilities and infrastructure as well as on-post assets. Understanding must also be comprehensive. It cannot be overly focused on computer resources to the exclusion of potentially important hardware and facilities. In the civilian sector, a similar survey is essential to understanding those resources central to the functioning of society.

Intelligence must evolve to provide a clearer sense of the threat and potential enemy capabilities for attack. This task could be especially demanding for computer and network security because the attackers themselves could be insular and difficult to identify, much less collect against.

Finally, the Army may have to build a consensus with the civilian sector about what the service can and cannot help to protect. By understanding with greater specificity what the civilian sector will demand of it, the Army will then be in a position to determine the size, type, characteristics, and number of organizations it will need to fulfill its responsibilities for CAAP and CIP.

Border and Coastal Defense

Organization for border and coastal defense is assessed as high because the tasks involved suit mainstream Army tactical units. Most maneuver units are designed to occupy or control terrain and so are well designed for this task area.

TRAINING

Training contains the most shortcomings across the homeland security task areas.

Domestic Preparedness

Evaluation. In domestic preparedness training, the Army is rated medium. Civilian authorities expect Army units to be prepared to handle tasks that local emergency workers are not: large numbers of contaminated corpses, for example. No evidence exists that mainstream Army units are trained for this task. Neither is it clear that

civilian authorities and the Army are generally in agreement on the conditions and standards for accomplishing the job. Put another way, civil authorities and the Army might have different notions about how some tasks would be carried out. Civilians may expect individual treatment for the dead, while the Army may expect to treat them en masse.

Our concerns about the WMD CST suggest that it will be quite important for the WMD CSTs to exercise with local and state first responders to establish whether they are as responsive and capable as they need to be. This training and exercising should be an “all hazards” curriculum and include training across the full spectrum of potential operations, from standard hazmat incidents to chemical and biological WMD incidents.

Also of concern in the domestic preparedness area is the possibility of confusion regarding the scope and applicability of the Posse Comitatus Act and the exceptions that have been specified in congressional or executive action. There were indications of confusion regarding the applicability and constraints imposed by the Posse Comitatus Act in Joint Task Force–Los Angeles (JTF-LA) in 1992 that suggest to us that additional attention should be given to curriculum development, education, and training regarding the circumstances under which specific restrictions apply when National Guard forces are acting in their state and federal capacity and when other Army forces are acting in a federal capacity. See Appendix D, “Overview of the Posse Comitatus Act,” for a more detailed discussion.

Cost-Effectiveness Considerations. The concern leading to a medium assessment of domestic preparedness arises from some of the scenarios about WMD. There appears to be a gap between civilian expectations and Army capabilities for dealing with WMD contingencies. For example, in questioning participants in local exercises, a commonly held expectation is that the Army will be able to handle large numbers of contaminated human remains. Few units train for this task. Moreover, in mass casualty conditions, disposition may involve earth-moving equipment and mass burial rather than individual recovery, preparation, and burial. The concern is that communities expect a different standard of treatment and a certain level of specialized capability that does not exist in large amounts. Earning a high rating involves training together and discussing the spe-

cific requirements of various scenarios in enough detail to square civilian expectations with Army capabilities. Earning a high assessment also requires that psychological aid and bereavement programs become part of the training so the Army can assist survivors in accepting the kind of treatment their deceased relatives receive.

The costs of addressing the issue could be moderate. The Army could produce training support packages that deal with mass casualty events and its doctrine for handling them. These packages could be a resource issued independently to localities to support their training, whether or not a military unit is participating in the training event. Nevertheless, if an agreed-on set of practices is to be developed, the Army must send participants to more local training events. Through such interaction, the tasks, conditions, and standards can be discussed and if necessary, modified.

COG

Training for COG rates high. The program has operated for years at different levels of intensity, and its current posture seems appropriate for today's environment, where the threat is probably small but may be growing. If the threat becomes more immediate, it would be relatively simple to increase the training and exercises involved in this task area.

Training programs for federal COG nevertheless should be reviewed to ensure that they are relevant to the emerging threats. Training for local and state continuity of government activities also should be reviewed.

Continuity of Operations

Evaluation. *Force protection.* Training for force protection is evaluated as medium because it still emphasizes protection in the theater of operations to the exclusion of defensive measures during deployment. The Army should emphasize potential force protection tasks for units during crisis deployment, including NBC preparedness during movement and security (e.g., in the load area control center, the passenger terminal, and similar places where troops may be highly concentrated and vulnerable).

Critical Asset Assurance. Critical asset assurance is rated low because so little has been done to prepare for the relatively large number of training tasks associated with this area. Despite the existence of detailed plans at highly classified levels, critical asset dependencies are not completely understood at the installation (or Army) level and are not reflected in unit mission-essential task lists. Most installations have very limited conceptions of critical assets: the ammunition storage area, load-out rail head, and similar facilities.

Critical Infrastructure Protection. Critical infrastructure protection also rates low. This task area potentially includes many training challenges for the Army, because the service could find itself responsible for securing transportation nodes and networks off post as well as on. The Army should create a specific set of JMETLs/UJTLs as a basis for understanding all of the tasks they may have to be trained for.

Continuity of Headquarters Operations. Army Headquarters continuity of operations is rated high for the present. However, if threats become more immediate, the headquarters would benefit from a more deliberate training program that exercises the transfer of functions to another major headquarters. At present, however, the experiential base in officers who have served in the headquarters and who are also experienced in transferring control between tactical headquarters (e.g., division main and forward command posts) seems adequate.

Cost-Effectiveness Considerations. *Force protection.* Force protection training rates medium because it overemphasizes the overseas theater and pays insufficient attention to the potential requirements for force protection in the United States. To achieve a high assessment, a set of force protection practices suitable for CONUS should be developed and units indoctrinated in them.

Some force protection practices could be transplanted directly from current training. For example, training a unit to deploy its chemical agent alarms would be no different in the United States than overseas. That said, the unit commanders must be trained to think about CONUS as a part of the theater of war and to place their units in protective postures commensurate to the threat. Other costs would be slight and would involve recasting today's force protection prac-

tices for application in the United States, with special emphasis on protecting units during deployment. The training tasks would emphasize force protection at home station on alert, force protection in the railyard, force protection at the departure airfield, and force protection at the port of embarkation.

CAAP/CIP. The conceptual problems mentioned above (e.g., what is “critical”) manifest themselves in training, to earn low ratings. Although some basic training tasks will transfer to CAA and CIP (i.e., those that call for Army strong-suit skills in observing, occupying, guarding, controlling, denying access), others may not. The low assessment reflects the high levels of uncertainty about training requirements and the dangers associated with that lack of knowledge. To train effectively and earn a high assessment, the Army must know what assets and infrastructure it must protect and safeguard so it can develop the appropriate set of tasks, conditions, and standards. It can then get the asset and infrastructure protection missions on the mission-essential task lists of appropriate units.

The costs in correcting the CAAP/CIP training shortcomings are minimal. Once the difficult intellectual work of identifying critical resources is done, involved parties agree on what the critical resources are that must be assured, and the Army’s role is agreed on (e.g., will the Army really play a direct role in securing the money and banking system? If so, what role?), then the Army can develop the requisite tasks, conditions, and standards for accomplishing the mission.

Border and Coastal Defense

Evaluation. Training for border and coastal defense is rated medium because the ambiguities surrounding the policy issue of the specific role that military forces should have raise questions about the adequacy of the Army’s training. Although the tasks involved in border and coastal defense are mainstream Army business, it is difficult to imagine effective training to appropriate conditions and standards until the policy question surrounding the exact Army role is resolved.

Cost-Effectiveness Considerations. As noted in the earlier chapters treating border and coastal defense, the military could play any number of roles, from direct support to law enforcement to more

removed roles. These ambiguities must be resolved before training can be assessed as high.

Once the role of the Army and other military forces is agreed on, the costs of addressing the associated training issues should be modest. Most of the tasks involved in border and coastal defense fall in the mainstream of Army and other service skills. If a more direct form of involvement with security emerges, training might have to expand somewhat to include use of less-than-lethal weapons. Otherwise, much of the mission-essential task list for peace support, stability, and humanitarian assistance operations can be repackaged for border and coastal defense.

LEADERSHIP

As the threats to homeland security grow or become more imminent, leadership preparation must keep pace. The professional military education system for officers and NCOs should consider which homeland security task areas should be dealt with in leadership training and how they should be addressed—in institutional training, unit schools, distance learning, or some other mode of instruction.

Domestic Preparedness

Leadership for domestic preparedness is currently assessed as high because the basic leadership skills in the officer and NCO corps have served well in the domestic preparedness and disaster relief events that served as case studies.

COG

Evaluation. Leadership for COG is rated medium because, although the COG program has a record of sound training, few officers are exposed to the notion until they serve in the Pentagon. The subject might be treated at the War College and as part of the curriculum in the Army Management College. Curricula should be reviewed to ensure that leadership programs address the sorts of issues that could arise in the emerging threat environment, as well as issues related to local and state level continuity of government.

Cost-Effectiveness Considerations. Few officers are familiar with COG before assignment to the National Capital region. The overall program is not as robust as it was prior to 1991. To overcome this rating, COG requires a basic introduction among more senior field grade officers so that an adequate pool of leaders is available as a hedge against surprise.

The cost of hedging would seem to be slight. The War College might provide a special instructional module to familiarize those for whom the next assignment will be Washington. Civilian leaders could be likewise prepared at the Army Management Staff College.

Continuity of Operations

Evaluation. *Force protection.* Leadership in force protection is rated medium for an easily correctable reason. The current mind set of most leaders emphasizes the overseas, deployed nature of force protection. The Army could quickly correct this by teaching force protection at officer advanced courses and the basic NCO course, where the curriculum could treat explicitly the homeland security and overseas dimensions of the question.

Critical Asset Assurance. Leadership in critical asset assurance is medium because midlevel Army leaders receive so little preparation for understanding these issues. Most conceive of critical assets as their motor pools and the major items of equipment in them or the post ammunition dump. Few members of the service in tactical units have been exposed to the CAAP. This condition could easily be remedied with professional military education. Indeed, it might be a suitable topic for the precommand course and Sergeants Major Academy.

Critical Infrastructure Protection. Critical infrastructure protection leadership is assessed as medium for the same reasons. Few officers and NCOs encounter the issue unless they work at installation headquarters or in major command headquarters that must confront the matter. Education again is the remedy, perhaps as part of the initial orientation for newly assigned personnel in jobs where CIP figures prominently. The Army should consider leaders' needs for specific types of civilian technical expertise, especially for such areas as information assurance.

Continuity of Headquarters Operations. Leadership for headquarters continuity of operations is rated high. Training, problem-solving skills, and other attributes of Army leaders seem well suited to this task area.

Cost-Effectiveness Considerations. *Force protection.* Concerns about leadership in force protection, reflected in its medium rating, involve the mental orientation that surrounds this task area. Force protection in the United States tends to address two programs: operations security (OPSEC) and subversion and espionage directed against the U.S. Army. Otherwise, most officers and NCOs conceive of force protection issues as matter for deployed forces. To earn a high rating, leadership must expand the current conception of force protection and cause Army leaders to consider the impact of an enemy campaign in CONUS on their force protection requirements.

If and when the threat becomes acute, leadership can address it by adjusting professional military education courses and the distance learning curriculum appropriately. The basic NCO course and the officer advanced courses may be appropriate venues for in-residence instruction. Leaders at all levels may eventually need instruction, however, so distance learning programs should also be contemplated.

CAAP/CIP. The medium rating reflects the lack of common understanding of critical assets and infrastructure. To overcome this rating, leadership must prepare officers and NCOs with an appropriate appreciation of the dependencies their units have on installation and civilian utilities, networks, computers, and facilities for operational success.

The costs involved in addressing CAAP are probably minimal. Curriculum adjustments in the precommand course for officers and the Sergeants Major Academy for NCOs could in short order provide a common perception of the issue and an appropriate appreciation of critical local dependencies. CIP will require a somewhat different approach. In addition to curriculum adjustments, for officials in positions involving critical infrastructure, they may need more specialized preparation. Special coursework could be designed to meet the needs of officers in CIP-related positions.

Border and Coastal Defense

Border and coastal defense are rated high because the vast majority of Army officers and NCOs are well-prepared for mainstream Army work like this.

MATERIEL

Human performance in most missions can be enhanced or undermined by the quality and readiness of the materiel supporting it. Materiel considerations appear in several task areas.

Domestic Preparedness

Evaluation. Materiel for domestic preparedness earns a medium rating because of four critical uncertainties.

The first uncertainty involves the amount of actual decontamination capability that the WMD CST brings to an incident. With a potentially modest expenditure, at least in terms of equipment, the WMD could be transformed from a rapid assessment and initial *detection* element to a rapid assessment and initial *decontamination* unit, retaining its assessment and detection capabilities, while enhancing its decontamination capabilities.

The second uncertainty involves the availability of mobility assets to move the WMD CST (and other Army response elements) to the scene of the incident. Mobility assets, predominantly Air National Guard or other Air Force airlifters probably will need to be maintained on a reasonably high state of alert, and quick, short-haul transportation will be needed to move the WMD CSTs to these mobility assets.

The third uncertainty involves the stockpiling and movement of emergency stocks of consumables that will be needed in incident responses. The uncertainty reflects the paucity of information about local stockpiles and the need for additional capabilities, provided by the Army. Site surveys to establish requirements and provisioning needs are essential to understand where, what, and how much in terms of Army stocks—if any—should be positioned to support domestic preparedness.

The fourth uncertainty is related to the first—as RDT&E yields much less costly chemical and biological detection equipment, it will be possible to distribute the equipment widely to first responders. This is likely to further blur the distinction between the WMD CST's assessment and detection capabilities and those of first responders and increasingly call into question the value of a WMD CST that has no decontamination capabilities.

Cost-Effectiveness Considerations. Because a clear picture of the cost-effectiveness of the overall (local, state, and federal) response system is lacking, it is difficult to establish whether the costs that would be incurred to address each of these areas would be worth the benefits.

While the costs of transforming the WMD CST to give it decontamination capabilities could be relatively modest, the costs associated with giving the WMD CST a high enough state of readiness for 24-hour-a-day, seven-days-a-week response capabilities, and providing it with the necessary mobility assets could be quite substantial. The Army should look more closely at the missions and materiel requirements of the WMD CST.

COG

COG is rated high.

Continuity of Operations

Evaluation. *Force protection.* Force protection materiel is rated high.

Critical Asset Assurance. CAAP materiel is assessed as medium. The rating reflects uncertainty about the appropriateness of Army equipment for defending the full suite of critical assets. The uncertainty results in part from the lack of thorough understanding about the Army's dependencies.

Critical Infrastructure Protection. Critical infrastructure protection materiel rates medium according to the same logic. On one hand, JTF Computer Network Defense, a DoD asset, exercises defensive and offensive responsibility over all Defense Department networks, including the Army's. At the same time, however, great uncertainty

exists about attacker ways and means, making it very difficult to be confident that materiel for CIP is entirely adequate to the challenge. Particularly important in this arena will be RDT&E that enhances the ability to detect intrusions and execute the necessary counter-measures.

Continuity of Headquarters Operations. Materiel sufficiency in support of headquarters continuity of operations is evaluated as high.

Cost-Effectiveness Considerations. *CAAP/CIP.* Earlier reservations about the lack of full appreciation of Army dependencies manifest themselves here in a medium rating for materiel. This rating is reinforced by the lack of concrete intelligence about potential enemies and their campaign plans. The Army cannot say where it needs materiel solutions to assist in safeguarding its critical assets and infrastructure because it lacks intelligence about who might attack or what means the attackers might employ. To overcome this medium assessment, the Army must more fully understand what constitutes its critical assets and infrastructure. The Army also needs better intelligence on enemy campaign plans that target critical assets. Finally, it should consider the sorts of hedging options that can be taken in advance of an attack on critical infrastructure to weaken its consequence (e.g., enhancing stockpiles or inventories of needed consumables).

Costs in addressing the shortcomings could be relatively high. Many of the nonstate actors posited by the Defense Science Board and similar studies as future adversaries are shadowy and elusive and do not necessarily lend themselves to traditional intelligence collection techniques. In some instances, because their means of attack may be so nontraditional, knowing such basic military intelligence information as order of battle is not very helpful in understanding their campaign plans and objectives. The essential elements of information for protecting against critical asset and infrastructure attack could be quite different. For example, knowing the specific assets that are attractive targets to an enemy could demand tactical intelligence specificity at the strategic intelligence level. Only when intelligence develops in such detail can the Army understand with high confidence what the materiel requirements for safeguarding its infrastructure and other assets might be.

Border and Coastal Defense

Evaluation. Border and coastal defense materiel is rated medium. As discussed in the earlier analysis of DOTLMS for this task area, the basis for the assessment lies in the ambiguity surrounding the Army's ultimate responsibilities. For example, if policy decisions lead to a larger and more direct role in border and coastal defense, less-than-lethal weapons and specialized communications suites able to network with key civilian agencies should be explored.

Cost-Effectiveness. This task area rates a medium because of the ambiguity about the Army's role and responsibilities. To overcome the rating, the Army must have a clearer notion of exactly what type of role it will play and what specific responsibilities it might have. For example, if the Army is to play a more direct role in border and coastal defense, then materiel solutions to provide less-than-lethal weapons might be appropriate. The interagency process must first settle on a clear set of responsibilities for the Army.

The associated materiel could be substantial and could involve the sort of scale of materiel needs associated with the military involvement in the war on drugs. Nevertheless, it is not clear that the Army would incur these costs. For example, while materiel needs could include capabilities to provide long-range detection of chemical, biological, radiological, or nuclear materials before they cross U.S. borders, it seems more likely that the U.S. Customs Service, the Coast Guard, the INS, the FAA, or even the Navy or Air Force, might have a more substantial role in the employment of these technologies. In our view, the answer to this is more of a policy question that will probably reflect the preferences of the Executive Branch and Legislative Branch more than anything else.

SOLDIER SYSTEMS

Soldier systems generally appear well prepared for homeland security, with two exceptions.

Domestic Preparedness

Evaluation. Domestic preparedness soldier systems are assessed as medium. The rating results from concerns that, while most demands

on soldiers in domestic preparedness events will be similar to those they prepare for, certain events, especially those involving mass killings, may find soldiers less than fully prepared. Needs include medical readiness, psychological preparedness for operations at home, and indoctrination in a code of conduct appropriate for operations among the nation's citizens.

Cost-Effectiveness Considerations. Little has been done to equip soldiers for the stresses and special conditions of supporting a mass casualties event. Soldiers are prepared for overseas deployment in part by a code of conduct that indoctrinates them in the proper treatment of combatants and noncombatants. No such code of conduct exists to guide soldiers' actions at home in dealing with civilians, police and rescue officials, and others they may encounter at the scene. In a similar way, soldiers are conditioned to the sights and sounds of the battlefield through, among other things, combined arms live fire exercises. Although these exercises have their limitations, they provide soldiers with some basic notion of what to expect in terms of noise and confusion in combat. No similar institutional preparation exists to support domestic preparedness response forces.

Overcoming today's shortfalls would be relatively inexpensive. A domestic code of conduct could be fashioned to parallel the points in today's code of conduct.

COG

COG is also assessed as high for soldier systems because current soldier systems seem well-suited to the individual soldier responsibilities in this task area.

Continuity of Operations

Evaluation. *Force protection.* Soldier systems for force protection are assessed as high. At an individual soldier level, countering subversion and espionage directed against the U.S. Army, OPSEC, situational awareness training, and medical readiness appear to be adequate.

Critical Asset Assurance. CAA earns a high rating for soldier systems. There appears to be no new demands on soldier systems from CAA responsibilities.

Critical Infrastructure Protection. CIP also earns a high rating for the same reasons CAA did.

Continuity of Headquarters Operations. Headquarters continuity of operations likewise earns a high rating.

Border and Coastal Defense

Evaluation. Border and coastal defense rates medium for soldier systems because of the uncertainty about the ultimate Army role in this task area and the demands it may or may not levy on soldier systems.

Cost-Effectiveness Considerations. This area reflects the uncertainties and ambiguities about what the Army's ultimate role and responsibilities will be for border and coastal defense. Whether the Army plays any substantial role and whether that role involves direct or standoff involvement will determine the need for additional soldier systems. The medium rating reflects the current uncertainty about future Army involvement and is not an evaluation of soldier systems used in ongoing operations in support of the Customs Service, ATF, or any other federal agency.

The costs associated with reducing the uncertainties surrounding the ultimate Army role are small. The question of the type and degree of Army involvement is a policy issue, to be decided within the parameters of the law.

ASSESSING THE ADEQUACY OF ARMY CAPABILITIES

Table 9.1 summarizes the homeland security task areas and the types of Army units most likely to be useful in responding to contingencies in each task area.

Given our understanding of the current threat (low), the ambiguity surrounding the requirements for support, and the limited amount

Table 9.1
Units Useful for Homeland Security Contingencies

Task Area	High-Value Units	Other Supporting Units
Domestic Preparedness	NBC Engineer Medical Infantry	Explosive ordnance disposal Mortuary services Casualty reporting
Continuity of Operations	Similar units to those damaged or destroyed	
Force Protection	Intelligence Air defense NBC Medical Military police Infantry	Other units on the same installation
Critical Asset Assurance	LIWA	Signal Engineer
Critical Infrastructure Protection	Military police Engineer Infantry	Other units adjacent to critical infrastructure
Department of the Army Headquarters Continuity of Operations	Major Command Headquarters	
Continuity of Government	Individual staff officers Signal Intelligence	Any secure facility
Border and Coastal Defense	Intelligence Aviation Air defense	Infantry Cavalry

of information on the cost-effectiveness of alternatives, it is difficult to provide a highly detailed assessment of the adequacy of capabilities in the current Army force structure.

That said, Table 9.2 summarizes the main units available in the active-duty and reserve component Army force structure of interest for the repertoire of homeland security tasks. We believe that, given these resources, there is no reason at present for the Army to assign or earmark additional units for homeland security task area contingencies. Nevertheless, as discussed earlier, since many of these units

may be low-density and dual-missioned to homeland security and warfighting, additional planning may be required to deconflict competing claims for the same resources.

Table 9.2
Available Units in Army Force Structure

Type of Unit	Number in the Army
Medical brigade	13
Medical group	11
Hospital	78
Chemical battalion	12
Air defense battalion	46
Military police battalion	36
Military intelligence battalion	49
Signal battalion	94
Engineer battalion (combat)	91
U.S.-based maneuver divisions	14

SOURCE: Association of the U.S. Army, 1999.