A Panel Report of the
**Defense Science Board
2007 Summer Study on Challenges
to Military Operations in Support
of U.S. Interests**

Unconventional Operational Concepts and the Homeland

March 2009

Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **MAR 2009**	2. REPORT TYPE		3. DATES COVERED **00-00-2009 to 00-00-2009**
4. TITLE AND SUBTITLE **Unconventional Operational Concepts and the Homeland**			5a. CONTRACT NUMBER
			5b. GRANT NUMBER
			5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)			5d. PROJECT NUMBER
			5e. TASK NUMBER
			5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Under Secretary of Defense,For Acquisition, Technology, and Logistics,Washington,DC,20301-3140**			8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**			
13. SUPPLEMENTARY NOTES			
14. ABSTRACT			
15. SUBJECT TERMS			

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**104**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Table of Contents

Executive Summary

This report on unconventional operational concepts and the homeland was prepared as part of the Defense Science Board 2007 Summer Study on Challenges to Military Operations in Support of National Interests. The summer study recognized that asymmetric tools of war in the hands of potential adversaries may well be employed using non-traditional concepts of operation. Moreover, the battlefield may no longer be limited to regions afar, but may include the U.S. homeland. The United States could well confront the possibility of going to war abroad in the face of significant devastation in the homeland—dividing forces between homeland catastrophe relief operations and combat abroad, or even facing the possibility that deploy and supply of U.S. military forces could be delayed and disrupted.

The capable adversary of the future will execute "one game"— attacking U.S. interests wherever the nation is most vulnerable, and that could mean the homeland. When a determined adversary succeeds in attacking the homeland at the scale imagined in this study, the nation will call on the Department of Defense (DOD) to "provide for the common defense" through both defense at home and offense abroad. DOD has, in fact, acknowledged such a future in its *2005 Strategy for Homeland Defense,* which states unequivocally that DOD must be prepared to defend the homeland:

> The Department of Defense must change its conceptual approach to homeland defense. The Department can no longer think in terms of the "home" game and the "away" game. There is only one game. … Defending the US homeland—our people, property, and freedom—is our most fundamental duty. Failure is not an option.

How well has the department progressed in turning that strategy into reality? This can be broken into three more specific questions as follows:

- How well do DOD and others understand what's expected of them? How well prepared is DOD to execute across a range of homeland defense missions?

- Given the "one game" nature of the capable adversary, can DOD have high confidence that it will be able to ensure deployment and supply in whatever set of missions it undertakes, within and from the homeland?

▪ Success, in both the current scope of homeland security and defense and the more stressing environment of the future, depends on teaming and integration unprecedented in recent history: across and among all levels of government, with and across the private sector, as well as individual actions for preparedness. Where does the nation, and especially DOD, stand in building the "one team" needed for success?

DOD Roles and Responsibilities

Overseas deployment, simultaneous with responding to a significant scale of attacks in the homeland, will stress DOD capabilities. The public expects that DOD will defend the homeland. DOD will be ordered to participate in homeland incident prevention, mitigation, and remediation through the U.S. domestic political process, regardless of the intentions of pre-incident military leadership. Legislation and directives support this approach.

However, at the next level, many responsibilities and missions are not so clearly acknowledged within DOD, resulting in the application of inadequate resources to the homeland defense mission. The problem extends beyond DOD to the interagency and response communities, where the handoffs and roles are not well understood—in part because they are not effectively exercised.

Scope of Roles and Responsibilities

Defending the homeland includes a range of activities, most often discussed in terms of support to the civil authorities. But these activities can also progress to include a leadership role in response and consequence management efforts if or when the scope of an attack is severe enough. Even in a more limited support role, DOD leadership, both civilian and military, has been slow to accept this apparently expanded scope of responsibilities. A principle reason is that these responsibilities come with significant resource demands and financial costs that are not likely to be adequately supported. As a result, the resources and capabilities that DOD has to offer have not yet been effectively applied. DOD does not really know what is expected of it and the homeland security community does not know what to expect from DOD. The transition of responsibility across the various supporting and leading roles—and the handing off of these roles from one agency to another—are not well understood among the interagency and response communities.

A focus on specifics helps to better assess progress and gaps—the approach taken in this study. Reasonable roles for DOD in homeland defense include

sharing intelligence, sharing infrastructure assurance standards (to support their mission), sharing operational doctrine and training, and providing consequence management support in case of an isolated terrorist attack or a natural disaster, such as Hurricane Katrina. Clearly DOD has lead responsibility for defense against air, missile, and maritime (with the Coast Guard) attack and for protection of its bases. DOD is in a lead role to assure the protection and resiliency of the defense industrial base, but it also must take a strong supporting role to assure protection and resiliency of other infrastructure that supports its missions (at least until a first significant attack(s) where it may be called upon to assume the lead). Roles that are not appropriate for DOD include protection of the country from internal threats like isolated terrorist attacks, production of weapons of mass destruction (WMD), or border monitoring for smuggling or illegal immigration.

To assure seamlessness among response elements and DOD, the Department must expand its concept of "jointness" to include other federal, state, regional, local, and tribal entities. This can best happen through leadership and practice. But homeland security and defense leaders, both within DOD and other agencies, need to be developed, just as DOD has so carefully developed its leaders for the "away game." Planning, exercises, and training have yet to be conducted among all actors at all levels in any meaningful way.

Force Capabilities and Capacities

The study's assessment of DOD's capabilities to execute its homeland defense roles is not a positive one. In the more traditional roles of air defense, missile defense, and maritime defense, DOD has or is developing a capability for these roles, but is far from having a well-exercised national set of capabilities. For example, while DOD maintains the best air superiority force in the world, its capabilities are not well suited to protect the nation from general aviation or unmanned aerial vehicle threats. Protection of DOD installations has been a focus of force protection programs for some time, but addressing cyber threats and WMD remain major shortfalls. In too many other cases, DOD preparedness falls woefully short. Combatant commanders, especially U.S. Northern Command, have made many of these capability requirements known, but priorities within the Department have placed resources elsewhere.

The situation is even more serious when the panel looked into force capacities that might be required to deal with a major event or adversary campaign in the homeland while also prosecuting offensive actions abroad. This

dual mission alone infers a change in the estimates of total force requirements, and only worsens when the "double counting" of the reserve component, who might also be first responders, is added to the equation. As a benchmark, ~80,000 troops were deployed in response to Hurricane Katrina, a large fraction of which were National Guardsmen. Another 33 percent of the guard was deployed simultaneously in Iraq. Further, the National Guard is counted on to support their states, other states through mutual aid agreements, and to meet federal requirements.

Currently there is no ability to track the "double counting" or the "day job" skills of guardsmen and reservists. Many are first responders. Many have critical skills from their civilian jobs that would be useful in consequence management—skills such as telecommunications and utilities. Databases with such information could help tremendously in understanding how scarce assets are being allocated or help to identify the personnel with the best skill sets in response to emergency needs.

RECOMMENDATION: DOD FORCES AND CAPABILITIES FOR HOMELAND DEFENSE

Addressing the shortfalls will require significant resources, sustained commitment, and greater involvement with other agencies, especially the Department of Homeland Security. As first steps:

The Secretary of Defense should task the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD [HD&ASA]) to revise and implement DOD policies and procedures covering homeland defense requirements.

This tasking should include clarifying relationships, roles, and missions of all elements of homeland defense (federal agencies, civilian and private sectors, state and local responders, law enforcement, and others). This information would go far to eliminate the uncertainty and/or confusion about what is expected of DOD and what others can indeed expect of DOD. The scope should expand to include the contingency where DOD assumes the lead response role in the homeland. Only those policies and procedures that lower the barriers to planning, exercising, information sharing, cooperation, and coordination across the entire homeland defense community should be approved.

Service Chiefs and the National Guard Bureau assess force requirement and adjust/adapt/expand force structure to meet the "one game" demands of the future.

Force structure should be built not just to support the regional command war plans for overseas contingencies, but also for those being developed by U.S. Northern Command. The effort will involve the development of accurate databases to understand the civilian skills and job commitments of the reserve components in order to assess and address the "double counting" issue. It will also require close planning and coordination with the service secretaries across the doctrine, organization, training, materiel, leadership, personnel, and facilities spectrum in order to ensure that shortfalls are addressed.

Assuring Deployment and Supply

This study considered two critical warfighting aspects occurring simultaneously in the homeland: defending against domestic catastrophe and ensuring deployment and supply. Domestic catastrophes can occur in an environment of large, undisciplined populations, which, can result in the destabilizing effect of violent attacks on society. On the other hand, military deployment and supply take place in a disciplined organization, trained to accomplish the mission. Yet the two are linked—military deployment and supply is critically dependent on infrastructure elements that may be destroyed or severely compromised in a domestic catastrophe. Three areas seemed most important for DOD attention: (1) critical infrastructure protection and/or resiliency, (2) logistics, and (3) family and individual preparedness. A fourth area, military installation protection and preparedness, was the subject of a recent DSB task force.

Critical Infrastructure

DOD has responsibility for not only the protection and assurance of its own military installations and facilities, but it is also the lead agency for assuring the protection and resiliency of the defense industrial base infrastructure sector. In addition, DOD has a supporting role for 14 other critical infrastructures/key resources: transportation; information technology; telecommunications; energy; chemical; commercial nuclear reactors, materials, and waste; government facilities; emergency services; public health and healthcare; drinking water and water treatment systems; dams; postal and shipping; food and agriculture; and national monuments and icons.

DOD is starting to make progress in identifying what is critical through the leadership of ASD (HD&ASA)/Defense Critical Infrastructure Program (DCIP), supported by the Naval Systems Warfare Center in Dahlgren, Virginia. Together with the combatant commanders, they have developed and are implementing a "mission assurance" process that incorporates many of the recommendations of a prior DSB study regarding risk management and mitigation.[1] The process focuses first on identifying critical functions and capabilities—command and control; ballistic missile defense; intelligence, surveillance, and reconnaissance; and power projection, for example. This step is followed by identification and assessment of those few assets or facilities necessary to ensure the functions or capabilities.

The process also provides guidance to assess a number of critical infrastructures "outside the fence" on which DOD might depend and/ or need to defend. The (classified) list of mission-critical assets appeared logical, but not complete or consistent in the application of the criteria against which criticality was judged. Further, it does not capture cascading effects and infrastructure interdependencies. Recognizing that it is still a process getting started, this study concludes that more effort must be applied to get it right and complete. The biggest gap, however, is that no one is charged with the responsibility or authority to ensure that corrective actions are taken.

Despite nearly six years since September 11, 2001, many U.S. critical infrastructures remain vulnerable. For the DOD, many critical supply chains— meals ready to eat, missiles, munitions, and fuel, for example—are not as resilient as they should be. Critical infrastructure and sources of supply are owned largely by the private sector—security and assurance is their responsibility, which is monitored by other parts of the government.

The Department of Homeland Security (DHS) has the broader mission to lead infrastructure protection across all the agencies and sectors involved. While DHS has led the interagency and the private sector councils in developing a risk-based protection approach, so much remains to be done that it is not possible to say with confidence that the nation's infrastructure vulnerabilities have been adequately addressed. In general, the department lacks the regulatory or legislated clout to direct the private sector to consistent levels of security and/or resiliency.

---

1. Defense Science Board Task Force on *Critical Homeland Infrastructure Protection*, January 2007.

DHS has, however, done a good job at leading the national planning and grant processes, as well as overseeing lead agency activities with their sectors, in order to spotlight progress and gaps. At this point, DHS has identified 36 highest priority infrastructure assets and over 2,500 next level assets on which to focus attention, and, where appropriate, investment—under the constraint that much of the infrastructure is owned privately and therefore not eligible for public funds.

Of particular concern, however, is the difficult job of information assurance. There appears to be no national improvement plan in spite of countless admonitions to, and within, the government that such a plan and its implementation is a must. An important consideration for each federal sector owner is the fact that improvements in resiliency of the infrastructure will come about largely by its private owners. Developing a public-private partnership is no more important than in this area, and some attention to incentives to the private sector for improving its posture is warranted.

Logistics

The study was pleased to learn that a number of the problems plaguing the DOD logistics community for years appear on their way to being solved—at least those within the domains of the Defense Logistics Agency (DLA) and U.S. Transportation Command. Enabled by the introduction of modern information systems, the two agencies are now able to understand inventories in their depots, and track supplies in transit to the warfighter and their delivery to transfer points to the services. Redundancy and/or alternatives exist for movement of supplies within and out of the United States.

The weak links in the system are at the start and end points, with respect to the information system "glue" that integrates it end-to-end. Strategies are not yet developed to assure the availability of materials from the private sector within the homeland and of transportation routes required for their delivery from industry to DOD facilities in the event of attacks on the homeland. In addition, many spare parts for critical weapon systems are produced either by sole source companies or by companies with limited competition. Protection of critical sources of supply has not been planned. Diversion of supplies and materiel to civil priorities has also not been planned as a contingency in the event of major incidents at home.

On the other end of the supply chain, there has not been a coordinated effort to implement a single asset visibility system for the "last tactical mile" that

would allow for tracking and reporting consumption to the DOD national provider or the end-user. The visibility inherent in the upstream steps is, at this point, lost, so that the individual requestor often does not see what has been ordered in a timely fashion, or sometimes not at all.

Cross-cutting the entire enterprise is the information management system. DLA is paying considerable attention to its network defense, but has further to go in addressing a wider spectrum of cyber threats.

Military Installation Protection

In addition to ensuring that DOD can get material for warfighters from a robust private supply and internal distribution system, DOD must also assure the security of the forces it expects to deploy. The first step is assuring the inherent security of the installation itself. Each of the military services approaches base security and force protection differently, but almost all of them plan on the support of the local community emergency response resources in a serious incident.

For example, in the Army, mission commanders establish what is mission-critical. All garrison commanders have memoranda of understanding with the local community for first response capabilities. Both garrison and mission commanders coordinate plans for deployment under catastrophic scenarios. Annual exercises and training test commanders' ability to respond to incidents.

The civilian capabilities, on which military installations rely, will not be available if the incident is an attack of a serious scale, such as an attack using weapons of mass destruction—a particular concern of this study. Consequence management is the biggest gap in dealing with weapons of mass destruction. Project Guardian provides basic response capabilities to installations—chemical, biological, radiological, and nuclear—but is not scoped for anything of major consequences to the installation or surrounding community.

The DSB Task Force on Critical Homeland Infrastructure Protection assessed best practices for protecting U.S. homeland installations and recommended various approaches to enhance security and protection of these facilities. This task force determined that DOD has many facilities that are vulnerable to the threats considered in this study, but that a rational focus should be on protecting its critical military mission capabilities and functions. It also found that the degree to which DOD facilities are dependent on non-DOD

infrastructure is not entirely known. Further, until recently DOD lacked policies and standards to guide installation commanders in securing or creating contingencies around the infrastructure on which they depend.

The critical infrastructure protection task force made many recommendations to improve DOD capabilities. This study agrees with and endorses those recommendations and, as a result, did not revisit the issue in its deliberations. But through information gathering related to installation risk assessments and management, the study believes that while progress is being made, resources remain limited and priority remains highly dependent on the installation commander.

Family and Individual Preparedness

There are many examples where individual preparedness proved pivotal in mitigating the consequences of a natural disaster (Florida's resiliency to numerous hurricanes since Hurricane Andrew versus Louisiana's response to Hurricane Katrina), and also how strong a role it played in the early days of the Cold War. In the event of coordinated asymmetric attacks in many parts of the country and/or simultaneously with a natural disaster or avian flu pandemic, emergency responders and relief organizations may not be able to move across local or state borders. Resources will be severely strained and responders will be busy dealing with or preparing to deal with disaster on their home turf.

The situation with military families deserves special attention. DOD must recognize that soldiers, sailors, airmen, and Marines will not likely be effective warfighters if they are simultaneously worried about the security of their families. While obvious steps, such as increased base protection, can be implemented, too many families live outside the installation. Instilling and promoting a culture of preparedness can provide both physical and psychological benefits to members and their families. There is much that can be done without great expense or effort to better prepare for both natural and man-made disasters.[2] Greater hazard awareness, training, home storage, and family communication/evacuation plans can provide greater peace of mind, strengthen mental resiliency, and empower DOD families to carry on through a disaster. Preparedness also reduces the impact of a crisis and likelihood that these families will have to depend only upon

---

2. Events include such things as floods, mudslides, hurricanes, tornados, fires, severe snow or ice storms, earthquakes, volcanoes, infectious disease outbreaks, severe power and fuel outages, hazardous chemical releases, nuclear or radiological incidents, and acts of terrorism and/or civil disturbance.

the emergency relief infrastructure. Self-sufficiency also empowers members and families to help others and set an example the community can follow.

RECOMMENDATION: ENSURING DEPLOYMENT AND SUPPLY

Recommendations in this section are limited to those that affect DOD, although there are many related items that DHS should address, as well.

To better ensure deployment and supply, the Secretary of Defense should direct:

- ASD (HD&ASA)/DCIP to extend the mission assurance process to the defense industrial base and recommend approaches for addressing shortfalls

- Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)) to work with defense industrial base owners to develop and implement corrective action plans

- ASD (HD&ASA)/DCIP to develop a prioritized action plan for addressing identified risks to DOD-owned assets

- U.S. Northern Command to lead implementation of actions identified by ASD(HD&ASA)/DCIP for critical function assurance

- Service secretaries to fund actions for mission assurance in owned functions

- Deputy Under Secretary of Defense for Logistics and Materiel Readiness to ensure resourcing of logistics shortfalls:

  - to assure sources of supply and movement to DOD depots

  - to eliminate the last tactical mile issues

  - to make the information management system interoperable, robust, and resilient to attack, from both within and outside

Service Chiefs should actively promote the ability of military families to shelter at home for two weeks, or evacuate on short notice. They should:

- Reinforce the message via noncommissioned officer leadership academies, on-base medical community, Armed Forces Network, unit town-hall meetings, movie/TV celebrities, veterans organizations

- Assure base commanders export this capability to adjacent civilian communities.

Building the National Team

The third dimension of this assessment of homeland defense addressed the status of the "national team" and DOD's involvement. This is not a good news story. Homeland security organizations responsible for dealing with national calamities are a diverse lot: federal agencies, state and local authorities, and private firms. DHS, as the lead agency for creating that level of response, is still in its infancy. At the state and local level, there appears to be little that is positive about the relationship with federal "partners."

DHS continues to reorganize, changes points of contact frequently, and brings to the table too much of a "we're in charge" attitude. This judgment is shared by the private sector, although DOD's relationship with the defense industrial base seems to be better than between many other sectors and their federal agency lead. U.S. Northern Command, DOD's principal operating "face" to the homeland security community, has been restrained by DOD leadership's view that the priority is—and should be—the "away game." Its low profile start has produced serious perception problems that must be overcome among the partners with whom it will be called upon to work.

The Team Members and Relationships

Interagency. In the interagency arena, a positive example of how things should work can be found in the Joint Interagency Task Force – South.[3] This pairing of military and civilian government agencies under a unified command structure provides for routine interaction between the entities that will need to work together effectively during a crisis. The DSB believes that the complex network of interdependent roles, responsibilities, and relationships demands a full-time integrated approach to homeland security and homeland defense activities through a number of similar standing operational task forces.

---

3. Joint Interagency Task Force – South has the mission of monitoring and interdiction of illicit trafficking from Latin America. Membership includes Customs and Border Patrol, Central Intelligence Agency, Drug Enforcement Agency, Department of Defense, Defense Intelligence Agency, Federal Bureau of Investigation, Immigration and Customs Enforcement, National Security Agency, and the National Geospatial Agency.

Federal-State-Local. In the case of a point attack, the first manifestation—and response—will occur locally. If or when those resources are overwhelmed, requests to the state will be made, and the governor can call out the National Guard, as well as exercise mutual aid agreements with other states for additional response resources. When those avenues of response are tapped out, appeals for federal help can and will be made. However, during its investigation, the study team heard from several state and regional response leaders that federal support can be slow in coming and what they can expect is largely unknown.

With respect to prevention, state and local response leaders noted how much they can contribute, provided they have adequate threat information on what they should be anticipating. In other words, a strong partnership with their federal counterparts can contribute significantly to threat mitigation and/or apprehension. Positive examples of preparation and monitoring for Y2K and state/local threat assessment centers bear out the power of such partnerships.

Public-Private. Possibly the most neglected member of the homeland security/defense team is the private sector. The private sector owns most of the infrastructure and will be the most effective in protecting (given timely and adequate threat information) and restoring its function after an attack. As such, it must be an integral member of the team alongside government actors in federal planning and information-sharing activities.

Relationships between sector owners and operators and their federal agency interfaces are uneven—a striking condition that emerged during the course of this study. In some cases, especially where there is a history of a non-regulatory partnership, like the defense industrial base and energy sectors, relationships were positive, characterized by open and frequent communication and information sharing. Others were more one-way, with the federal "partner" more controlling and didactic. The realization that the sectors have more intimate knowledge of not only their own sectors, but their ties to other sectors, has yet to be well understood and embraced at the federal level.

Leadership. Forming a truly joint homeland security and defense team starts with developing leaders with a joint perspective—both through education and career experiences—building an interagency cadre of leaders, whose understanding of homeland defense transcends their immediate position. Homeland security and defense, regardless of agency, level of government, or public or private sector, must be seen as a professional opportunity for those seeking to lead in this critical field. However, there is no recognition of the need

to develop homeland security leadership in the same manner as the nation has invested in developing national security leadership.

Plans and Exercises

While numerous doctrinal and operational plans exist, most with embedded processes for review and revision, there are no processes to ensure that the plans are practiced and capabilities measured against readiness metrics. While there are many exercises (possibly too many), the exercises are highly scripted, unconnected to each other, and typically focus on a top-down approach (where the supporting organizations are "training aids" to the senior-level players) instead of bottom-up approach (focusing on an integrated and layered response beginning with the initial event). Even the national level exercises have not been effective—more often broad than deep, where the real lessons get learned. Furthermore, these exercises often stop before the more difficult issues—transfer of command, employment of specialized assets, or unknowns such as public panic—come into play. Even more worrisome than the disjointed nature of the exercises is the lack of any process for effectively "learning from" the lessons of these exercises. This gap extends to DOD, where the numerous exercise programs do not appear to be effectively linked to national objectives.

Crisis Communications

Communications is almost always at the top of the list of recurring issues in a crisis. It can make or break a successful response. It starts with the basics of compatible equipment and language among response communities. It extends to the public-private linkage, where both the pre-emptive and response actions by private sector owners of critical infrastructure can mitigate significant problems, yet they are, more often than not, kept in the dark or not allowed access. (This was an acute problem in recovery and restoration post-Katrina.) It covers also communications to the public. Too often it is developed "real time" without benefit of factual vetting and without coordination, such that what is communicated to the public can be misleading or just outright wrong (as example, the anthrax attacks in 2001). The DSB believes that if there is only one thing that DHS and DOD ought to improve among the national team, it should be crisis communication.

RECOMMENDATION: BUILDING A NATIONAL TEAM FOR HOMELAND DEFENSE

Secretary of Defense leadership in the interagency is needed to address current deficiencies in national plans and strategies and support for domestic threat assessment. DOD needs to step up to its preparedness responsibilities in the broad set of communications issues.

To address deficiencies in plans and communications, the Secretary of Defense should:

- Promote the combination of the National Security Council/Homeland Security Council to coordinate and integrate a national strategy and response for global asymmetric engagement

- Request a national intelligence estimate on the scope of the projected threat.

  - direct the Office of Net Assessment to conduct a capabilities-based net assessment

- Request that DHS work with DOD to codify the transition from DOD support to DOD lead for a war at home

- Direct the Deputy Secretary of Defense to develop a comprehensive DOD communication system and public affairs strategy for homeland defense preparedness and crisis/consequence management.

  - develop an equipment and concept of operations architecture compliant with the National Incident Management System

  - ensure availability of DOD communication assets compatible with civilian responder community

  - work with DHS to develop messages, and coordinate and educate those who deliver them, appropriate to the full range of contingencies

The Secretary of Defense should direct U.S. Northern Command to work with the National Exercise Program at DHS to design and execute more effective exercise programs that address:

- Unified management of national capabilities

- Communication and information sharing across public and private boundaries

- Regional planning and coordination

- Interoperable and response capability shortfalls

- Transition from DOD support to DOD lead scenarios

In the layered approach to DOD's Strategy for Homeland Defense and Civil Support, one of the layers—"Enable"—is directly focused on improving domestic capabilities through sharing DOD expertise and technology. The military is recognized for its unsurpassed training, exercise, and doctrinal programs.

ASD (HD&ASA) should take the initiative to help establish a strategically-managed, interagency homeland defense/homeland security leader development program with the following attributes:

- Graduate-level, senior service DHS-sponsored "war" college developed in conjunction with the National Defense University

- An Executive Exchange Program modeled on the President's Executive Exchange Program

- Recognition as credit equivalent to senior service schools and for flag/senior executive service promotions in DOD

- Training expanded to state and local levels

Chapter 1. One Game: Defending the Homeland

The capable adversary of the future will execute "one game": attacking U.S. interests wherever and however the nation is most vulnerable, and that could mean the homeland. The Department of Defense (DOD) has, in fact, acknowledged such a future:

> The Department of Defense must change its conceptual approach to homeland defense. The Department can no longer think in terms of the "home" game and the "away" game. There is only one game. … Defending the U.S. homeland—our people, property, and freedom—is our most fundamental duty. Failure is not an option.[4]

This volume, prepared as part of the Defense Science Board 2007 Summer Study on Challenges to Military Operations in Support of U.S. Interest, focuses on the implications to DOD of adversary attacks on the homeland, as an instrument of war, with an eye toward the particular challenges that can arise if an "away" game is in progress as well.

War on the Domestic Front

The United States has long postured itself for wars to be won by assertion of its national strength—large force size and/or technological advantage. But current conflicts and the rise of asymmetric strategies and tactics are making clear the weakness of this assumption. Future adversaries, either by choice or necessity, will not follow the path leading to a conflict of strength against strength.

A series of interviews on the Chinese book *No Limit Warfare* quotes one of its authors, Senior Colonel Qiao Liang, as saying "If we were to try to use high technology to counter U.S. high technology, that would in fact land us in the U.S. trap. We could never catch up to them on that track. So for a poor and weak

---

4. *Strategy for Homeland Defense and Civil Support*, Department of Defense, June 2005. See also Appendix B for relevant excerpts of this strategy.

country to try to use high technology to counter the United States would in fact be like throwing eggs against a rock."[5]

The refusal to adopt a symmetric approach to war also goes beyond the basic issues of military strength and operational doctrine. The nations and non-state actors of the world are observing, through the current era of terrorism, that the most lucrative potential approach to war with the United States could well be through operations outside the nation's moral framework and anticipated behavioral norms. They have been able to observe the effectiveness of this approach when the conditions involve a disparity of interest. Therefore, when an adversary has a vital interest that conflicts with the non-vital interest of a strong state, the former has the greatest incentive to use asymmetric approaches.

Many scenarios come to mind where U.S. adversaries view an issue as threatening life and/or state, while the United States has relatively little at stake. Under those circumstances, adversaries will often attempt to influence U.S. foreign-based activities.[6] Simply put, they could execute innovative asymmetric approaches to shape U.S. national will in order to:

- Deter U.S. entry into any foreign affair of no perceived immediate national security impact or no perceived threat to national sovereignty by threatening disproportionate asymmetric damage to the United States.

- Halt U.S. entry or accelerate a withdrawal if the nation decides to employ forces in a foreign action.

- Delay any U.S. decision to act by executing a range of asymmetric approaches. Many unconventional homeland approaches, particularly information operations, will also be very difficult to trace. Since the U.S. political process requires a high degree of certainty for legislated action, the nation's response could be delayed and diffused until it is simply too late to act effectively.

Moreover, U.S. military leadership has had difficulty embracing the concept of a two-front war, with one of the fronts being the homeland battlefield. Since the end of the Indian Wars in 1891, the United States has treated warfare as an "away

---

5. Sha Lin, "Two Senior Colonels and No-Limit War," *Beijing Zhongguo Qingnian Bao* in Chinese, Foreign Broadcast Information Service translation, June 28, 1999.
6. Kenneth F. McKenzie, Jr., "Where Are Our Asymmetric Vulnerabilities," *The Revenge of the Melians: Asymmetric Threats and the Next QDR*, McNair Paper 62, 2000, Institute for National Strategic Studies, National Defense University, page 3.

game." Attacks on the U.S. homeland (except by symmetric capabilities of ballistic missiles and long-range bombers) have been unthinkable due to the geographical isolation of the Americas and the strength of U.S. naval and air forces. The rise of global travel, commerce, and information flows has radically changed traditional American isolation. America's sea and air power still make conventional mass invasion unlikely, but **as military modes shift from concentrated industrial warfare to distributed wars among populations, domestic disruption is likely**. Effects-based targeting, used with great success by U.S. forces to inflict maximum impact with minimum force, is similarly useful to aggressors seeking to distract the U.S. population; disrupt infrastructure, commerce, and government; and delay support to U.S. military forces operating abroad.

The homeland could be subjected to a wide range of attacks. In addition to the possibility of a serial or parallel accumulation of clearly feasible attack modes (improvised explosive devices [IEDs] and vehicle-borne IEDs, suicide bombers, and sniper attacks, for example), the attacks could employ nuclear explosives (including those designed to cause electromagnetic pulse effects), toxic chemicals, biological agents, radiological materials, and cyber means. The attacks could be from terrorists or disguised as such. They could move from isolated events to "war" campaigns. There is a distinct possibility of large loss of life and significant economic hardship. Destruction and degradation of national or local infrastructure is also possible. Military consequences of such actions on the U.S. logistics base can be severe. Civilian consequences of such actions can only be imagined but would be of major importance. **While such attacks will be (initially) a Department of Homeland Security concern, they drastically affect DOD's ability to defend the homeland and carry out military missions abroad.**

In light of these potential consequences, the United States should expect future asymmetric attacks to focus on manipulating its populace—by attacking either critical infrastructure targets or the populace directly. The attacks would generally be tactical, but with strategic effect. If the population internalizes the terror associated with future attacks and begins to believe they are at risk in the normal course of their daily lives, then the will of the nation could be shaped. Additionally, if the threat involves weapons of mass destruction (WMD), the resulting image of massive casualties would elevate the effect to even higher levels of fear. If terror is reinforced by successive events, the American people could come to believe that they have no control. Then the real intent of these attacks would surface. A perception could emerge that personal security would only be regained by a decision to withdraw from a distant conflict (with no clear connectivity to the United States). The result would be achieved. Figure 1 captures these factors.
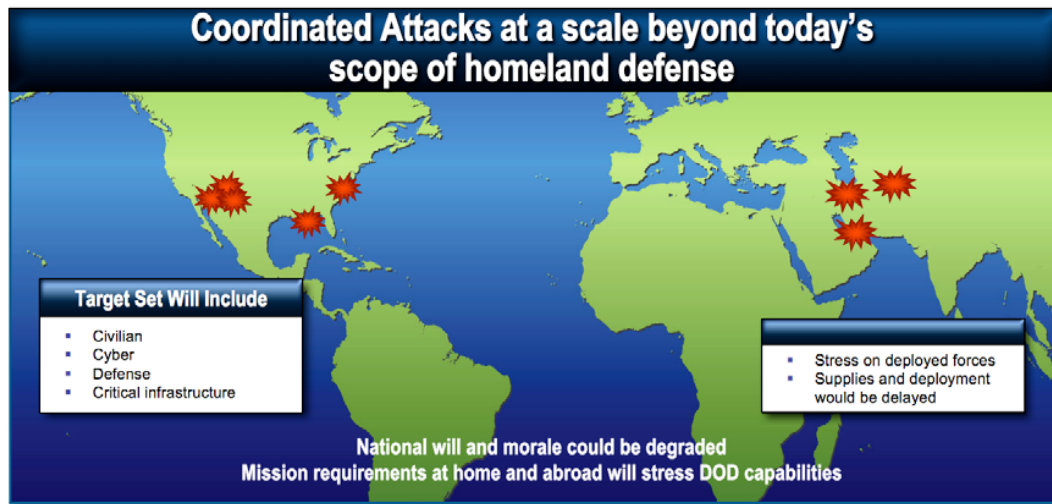
Figure 1. The "One Game" Approach of Future Capable Adversaries

As a foundation for its assessment of homeland defense, the DSB established the following assumptions. A future adversary will engage in coordinated attacks both in the U.S. homeland and in foreign theaters. With a high degree of resources and sponsorship, the attacks at home will most likely be at a scale beyond those envisioned in most current homeland defense planning, which is focused primarily on terrorist attacks. Moreover, adversaries will likely act at multiple points nearly simultaneously, or a carefully orchestrated sequence of attacks—a campaign. The openness of the U.S. society, its size, the geographical extent of its infrastructure, and its diversity will make it practically impossible to avoid all assaults. In addition, DOD will be divided between protecting the homeland from further attacks and prosecuting forward offensive operations against the adversary.

Consequences of Catastrophe

Disasters brought about by enemy action in the homeland cannot be precisely predicted, although conditions leading up to them may be generally evident. In any event, surprise should be an expected element of an attack(s). Dealing with the consequences of the attack(s) will have as much or more to do with addressing common issues as with the specific nature or cause of an attack. Planners should anticipate the breakdown of orderly society, manifested by:

- **Failure of critical infrastructure**—lack of essential goods and services (Table 1).

- **Insufficient professional resources to deal with multiple catastrophes**—response forces (Federal Bureau of Investigation, National Guard, DOD, DHS, police, fire, American Red Cross, and others) sized to handle only one or two crises at a time.

- **National will hard to focus**—public anger manifested through misguided, vigilante-style attacks.

- **Impaired ability of national, state, and local governments to govern**—lack of, or confusing, communications; fractured local authority; insufficient, disorganized emergency response.

Without adequate preparedness at all levels of government, across the private sector, and among the populace, the post-attack results could indeed become catastrophic. Some outcomes might include:

- **Flight.** Remaining in place would prove untenable for many people for actual or perceived reasons.

- **Breakdown of mutual aid agreements.** Resource-intensive incidents are typically handled through mutual aid agreements within the National Guard, first responder, and medical communities. When under attack, however, leaders in unaffected regions might opt not to support interregional common aid agreements and to conserve their resources in case they are needed locally.

- **Breakdown of civil order.** Looting, vigilante actions, gang violence, riots, and civil disobedience would further stress first responders.

- **Failure of quarantine.** Many will be reluctant to stay confined.

- **Hoarding.** People will rush to amass excess goods to stock up after the attack.

- **"Shoot your neighbor."** As people perceive the social and civil situation deteriorating, they will escalate the force they use as a first resort to protect home and family from interlopers ("shoot first, ask questions later").

- **Rampant rumors.** Media will promulgate messages from many sources without confirmation.

▪ **Population center "meltdowns."** Many U.S. population centers are located where life without infrastructure services will be difficult to sustain, such as in the desert southwest in summer and northern cities in winter.

Table 1. Examples of Consequences of Attacks on the Infrastructure

Infrastructure targets	Examples of consequences if attacked
Transportation	▪ Disruption of air traffic flow ▪ Mass transit contamination ▪ Hazmat releases from freight carrier ▪ Breakdown of supply chain essential to provide life sustaining goods and services (*e.g.* food, medical)
Oil and gas production and storage	▪ System (storage, refining, and pipeline) intrusion and degradation
Water storage and delivery	▪ Water supply contamination ▪ Interruption of availability (dams, deep public wells, etc.)
Banking and finance	▪ Data corruption ▪ Effective freezing of assets ▪ Massive stolen identity
Electrical power generation and distribution	▪ Damage to generating stations and operating systems ▪ Disruption of transmission, distribution systems, and associated fuel supply
Information and communications	▪ Lost and damaged data and information ▪ Degraded computing and telecommunications ▪ Breakdown of processing, storage, and transmission of data
Government services	▪ Loss of essential government services ▪ Overload on critical emergency services
Defense	▪ Lack of ability to execute missions from installations within the continental United States
Population	▪ Casualties and injuries at schools, malls, and other places of population/community massing ▪ Mass casualties in the event of WMD use

Responses will be further exacerbated because of the evolution of U.S. society. Dependence on "just-in-time" centrally managed, networked supplies of water, power, food, communications, and transportation leaves the United States extremely vulnerable to an effects-based attack. Additionally, over time, mobility of the American population has resulted in a breakdown of extended family and community-based societal structures that once provided informal local leadership and community organization and support. In twenty-first century society, many do

not know their neighbors, let alone have the capability or capacity to form effective support networks for long periods of time. Skepticism of authority makes governance in a disaster difficult, while the public nevertheless expects governmental assistance to mitigate the aftermath.

Implications for DOD

When a determined adversary succeeds in attacking the homeland at the scale imagined in this study, the nation will call on DOD to "provide for the common defense" through both defense at home and offense abroad. That fact is recognized in the Department's *2005 Strategy for Homeland Defense*, as noted at the outset of this chapter. The question, then, is how well the department has progressed in turning that strategy into reality. The study broke this larger question into three more specific questions, each of which is discussed in subsequent chapters:

1. How well does DOD (and others) understand what is expected of it? How well prepared is DOD to execute across a range of homeland defense missions?

2. Given the "one game" nature of the capable adversary, can DOD have high confidence that it will be able to ensure deployment and supply in whatever set of missions it undertakes within and from the homeland?

3. Success in both the current scope of homeland security and defense, and the more stressing environment of the future, depends on teaming and integration unprecedented in recent history: across and among all levels of government; with and across the private sector; down to individual actions for preparedness. Where does the nation, and especially DOD, stand in building the "one team" needed for success?

Chapter 2. DOD Roles and Responsibilities

This chapter addresses whether or not DOD roles in homeland security and defense are well understood, and how good DOD might be at executing them. Definitions taken from DOD's *2005 Strategy for Homeland Defense and Civil Support* set the stage for this discussion:

- Homeland security. "Concerted national effort to prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." DHS is the lead agency to prevent terrorist attacks within the United States. The Attorney General leads law enforcement to detect, prevent, and investigate terrorist activity with the United States.

- Homeland defense. "Protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression." DOD is responsible for homeland defense.

- Defense support to civil authorities (civil support). "DOD support for domestic emergencies and for designated law enforcement and other activities." This occurs by direction of the President or Secretary of Defense.

The establishment of U.S. Northern Command and the Assistant Secretary for Homeland Defense in the Office of the Under Secretary of Defense for Policy has provided focal points within and outside the DOD to address the Department's responsibilities within the homeland. These two organizations have done a lot to sort through the many issues for DOD in the homeland. But they have largely been on their own, given the consuming demands in the Department, on both leadership and resources, for prosecuting the "away game" in Iraq and Afghanistan. Both organizations also have to engage in an interagency effort led by DHS, which is still experiencing its own growing pains and has seen its priorities shift from prevention to preparedness in the wake of federal shortcomings in responding to Hurricane Katrina.

DOD: Support versus Lead

Engaging in an overseas deployment, while at the same time responding to a significant scale of attacks in the homeland, will stress DOD capabilities. The public will expect DOD to defend the homeland and DOD will be ordered to

participate, regardless of the intentions of the military leadership prior to the incident—engaging in incident prevention, mitigation, and remediation through the U.S. domestic political process. Legislation and directives support this approach. Further, the 2005 National Defense Strategy clearly directs the military leadership to properly shape, size, and globally posture to: 1) defend the U.S. homeland and 2) operate in and from the forward regions.

Homeland defense currently includes a range of activities in the continental United States (CONUS). Often, DOD will be called on to provide support to the civil government, but its activities can also progress to a leadership role in response, and consequence management efforts if and when the scope of attack is sufficiently severe. The concept described is notionally depicted in Figure 2, in which the transition from a supporting role by principally DOD reserve component forces shifts to one of leadership at significant attack levels involving reserve and active duty forces.
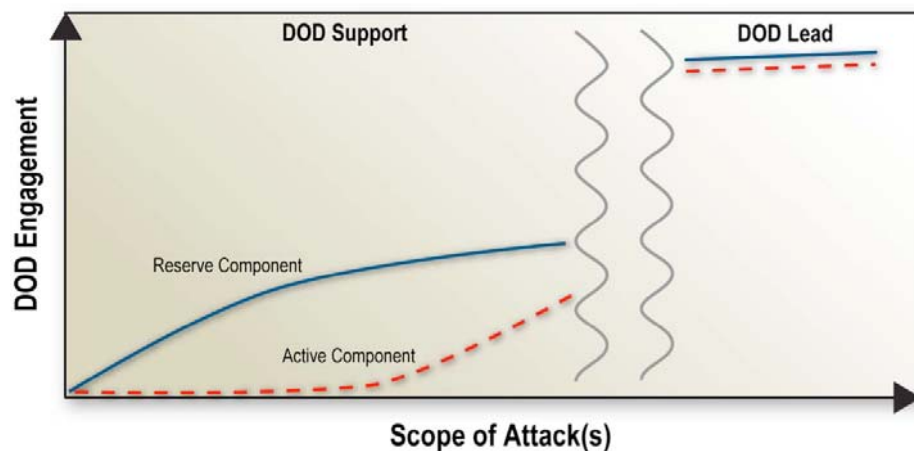
Figure 2. Notional Transition of DOD Forces from Support to Lead

Under coordinated global aggressive action from a capable adversary, the military response will involve actions that could be described as "at war within the homeland." In other words, an active layered defense must stretch across the integrated global battle space—extending from the forward regions, to the approaches to the United States, and the homeland itself.

When defense of the homeland transfers to the military, it implies a hardening of the target—which, in and of itself, can act as a deterrent to an

adversary. At that time, an adversary has to recalculate the overall benefit of his actions. The U.S. Northern Command Homeland Defense Plan recognizes this potential deterrent effect and outlines a robust range of actions in CONUS—ranging from sustained deterrence and enhanced deterrence, both targeted to deter threats and support civilian law enforcement agencies; to contingencies for the escalation of asymmetric activities at the severe end of the scale, described as decisive operations.

Unfortunately, DOD has applied inadequate resources to these homeland defense missions. The first step to resolving this situation is to acknowledge and communicate the roles and missions throughout the chain of command. Additionally, the portion of the Homeland Defense Plan addressing "decisive operations" has not been integrated and coordinated with the appropriate range of agencies and government entities. Therefore, the resources and capabilities that DOD has to offer are not yet effectively applied. DOD does not really know what is expected of it and the homeland security community does not know what to expect from DOD. The transition of responsibility from supporting to leading roles among the various agencies involved—and the handoff of these roles from one agency to another—are not well understood among the interagency and response communities. Although improving, this confusion extends to deterrent operations due to the immaturity of the DOD/DHS interface, but certainly is not yet addressed under "decisive operations" scenarios.

This interdependent and interactive problem is a difficult one to resolve and will need a great deal of attention. The relationships between all homeland partners, including state and local governments, will vary and depend on the type of asymmetric attack. The roles will be very different for ballistic, kinetic, WMD, and cyber approaches. Therefore, "jointness" beyond DOD must be pursued, with all the commensurate requirements in leadership, planning, training, and exercises fully resourced.

Legislation and Directives

The study found nothing in legislation, directives, or other documents to prevent a more aggressive posture and engagement by DOD. On the contrary, the documents set expectations for DOD preparedness, whether as supporting agency (expected in most situations) or supported agency (shift to homeland defense). Starting with the Constitution, the federal government is to "provide for the common defense." The Stafford Act allows for use of the military for disaster relief operations at the request of the state governor, and further defines

three scales of involvement: essential assistance (up to 10 days), emergency, and major disaster.

The Posse Comitatus Act is typically viewed as a restriction on DOD engagement since it punishes those who "…except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully use any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws…." A statutory exception to posse comitatus allows the President or other key government officials special authorizations for engaging the military in domestic situations. That authority has been exercised sparingly; examples include granting the U.S. Coast Guard law enforcement authorities and allowing the military to share information and equipment with civilian law enforcement, while prohibiting its ability to make arrests or conduct searches and seizures.

The Homeland Security Act gave DHS the lead for homeland security. DOD continues to maintain the lead for defense of the homeland. The Homeland Security Presidential Directives (HSPDs), issued by the White House since the establishment of DHS, provide further guidance for DOD's roles in civil support (HSPD 5), its lead responsibilities as the infrastructure sector "owner" for the defense industrial base (HSPD 7), and responsibilities for emergency preparedness (HSPD 8).

DOD has also recognized its responsibilities, through formal directives, in which it should be prepared to take the lead and/or act pragmatically:

- in support of natural disasters (its immediate assignment of resources in the aftermath of the 1906 San Francisco earthquake; its immediate deployment (unrequested) of a hospital ship to New Orleans after Katrina)

- to preserve public order where other options are unavailable or overwhelmed in order to carry out governmental operations

- in sudden and unexpected civil disturbances, disasters, or catastrophes when civil authorities can no longer maintain control

- to provide catastrophe relief without or before imposition of the Stafford Act, on a temporary basis

- to undertake some specific law enforcement activities

The Board's assessment is that there is sufficient breadth and flexibility in the relevant legislation to allow DOD to take on a wide range of roles. Those roles should be clearly understood at all levels so that all stakeholders can plan accordingly.

DOD Capabilities for Homeland Security and Defense

After the incidents on September 11, 2001, the nation was forced into a new level of national preparedness against attack on the homeland. The Department of Homeland Security was created to take the lead role in homeland security. As described previously in this chapter, DHS and DOD have either lead or support roles in protecting the homeland, depending on the type and scale of attack. The creation of DHS, while clearly adding to the preparation and focus of the country on improving homeland security, has also added some confusion regarding roles and missions for DOD in homeland defense. The Board believes this confusion comes from general statements about roles and responsibilities, in contrast to specific statements about DOD's roles and missions that tend to alleviate disputes or uncertainties.

Nonetheless, DOD leadership, both civilian and military, has been slow to accept this apparently expanded scope of responsibilities because with it comes significant resource demands and financial costs that are not likely to be adequately supported. The study determined that a focus on specifics was needed in order to motivate the Department's leadership to focus on priorities. Table 2 offers an illustrative list of those specific roles and missions that are generally accepted as DOD responsibility and those that are not.

As the table notes, typical roles expected of DOD are sharing intelligence, sharing infrastructure assurance standards (to support their mission), sharing operational doctrine and training, and providing consequence management support in case of an isolated terrorist attack or a natural disaster such as Hurricane Katrina. Clearly, DOD has lead responsibility for defense against air, missile, and maritime (with the Coast Guard) attack and for protection of its bases. DOD is in a lead role to assure the protection and resiliency of the defense industrial base, but also must take a strong supporting role to assure protection and resiliency of other infrastructure that supports its missions (at least until a first significant attack(s) where it may be called upon to assume the lead). Roles that are not appropriate for DOD include protection of the country from internal threats like isolated terrorist attacks, production of WMD, or border monitoring for smuggling or illegal immigration.

Table 2. DOD Responsibilities for Homeland Defense

Reasonable	Unreasonable

• Share intelligence
• Protect against air, missile, and maritime threats
• Protect designated civil infrastructure after first attack
• Provide consequence management after attacks
• Meet infrastructure assurance standards for DOD facilities and contractors
• Prepare to protect U.S. homeland from large scale attack
• Develop doctrine and plans to assure supply during attack of U.S. homeland
• Train with federal agencies and state and local authorities
	• Protect against or detect in U.S. homeland
	  • Production of WMD
	  • Terrorists
	• Protect civil infrastructure against initial attack
	• Constant surveillance of land and maritime borders
	  • Smuggling weapons, for example

Table 3 provides a rough assessment of the key capabilities DOD should have in order to execute the responsibilities listed in Table 2. The assessment includes not only a "grade" and trend (in the far right column labeled "How Good"), but also a breakdown to better highlight progress (or lack thereof).

The bottom line of this assessment is not a positive one. In the more traditional roles of air defense, missile defense, and maritime defense, DOD has or is developing a capability for these roles, but is far from having a well-exercised set of national capabilities. For example, while DOD maintains the best air superiority force in the world, its capabilities are not well suited to protecting the nation from general aviation or unmanned aerial vehicle threats. Protecting DOD installations has been a focus of force protection programs for some time, but addressing cyber threats and WMD remain major shortfalls. In too many other cases, DOD preparedness falls woefully short. Combatant commanders, especially U.S. Northern Command, have made many of these capability requirements known, but priorities within the Department have placed resources elsewhere.

Table 3. Capability of DOD to Perform Expected Roles

Assessment of DOD Status	Expertise	Think They Have Role	Has a Plan	Has Necessary Capability	Exercised and Ready	How Good
Ballistic Missiles		LEAD				↑
Cruise Missiles		LEAD				
Aircraft/UAS		CO-LEAD		NCR Emphasis		↑
Maritime		CO-LEAD				↑
Conv. Explosive (IED)						
• Road/Rail		No				
• Market-School		No				
• Critical Infrastructure		No				↑
• DOD Installation						↑
• Defense Industrial Base						
Cyber Attack						
• Commercial Target		No				
• Critical Infrastructure		No				
• DOD Installation						
• Defense Industrial Base						
Combating WMD						

DOD Capacities for Homeland Security and Defense

The study next turned to the issue of how chaos in the homeland would affect the military's ability to deploy and effectively prosecute offensive actions abroad. One important concern is whether DOD has sufficient capacity to support the "one game" envisioned in this study—whether DOD's role in the homeland and abroad implies a change in total force requirements. Lacking scenarios or plans for the "one game," the study considered the level of DOD support to Hurricane Katrina as a surrogate for force sizing for a single major event. Katrina drew a total of nearly 80,000 troops plus equipment, principally through the National Guard, but also from specialized active components, as shown in Table 4.

In a generic model of response to a catastrophic event, the initial response will come from traditional first responders—fire, police, and medical support. Based on the magnitude of the event, additional state resources could respond, including National Guard forces. Support from the National Guards in other states could be requested under Emergency Management Assistance Compact (EMAC) arrangements. For catastrophic events, federal resources, including DOD forces, could be deployed to support the response. In addition, depending on the number

of incidents and the expectation of further attacks, DOD forces (active and reserve component) could support other homeland protection missions (for example, guarding critical infrastructure nodes to prevent follow-on attacks).

Table 4. DOD Support to Hurricane Katrina

Support	Logistics
Search, Rescue, and Evacuation Approximately 15,000 residents of the Gulf coast were rescued and 80,000 others evacuated. **Medical Assistance** Ten thousand medical evacuations by ground and air; medical treatment of more than 5,000 patients; more than 3,000 beds in field hospitals, installations, and aboard U.S. Navy ships. **Mosquito Abatement** C-130s treated over 2 million acres. **Mortuary Affairs** Thirteen mortuary teams supported local authorities in the systematic search, recovery, and disposition of the deceased	**Personnel** Over 72,000 title 10 and National Guard forces. **Aviation** 293 helicopters and 68 fixed-wing aircraft. **Maritime** 23 naval ships. **Commodities** DOD delivered more than 30 million meals (24.5 million meals ready to eat) and 10,000 truckloads of ice and water. **Medical** Over 2,000 health care professionals deployed to the area. **Installations** Nine DOD installations in Alabama, Florida, Georgia, Louisiana, and Mississippi served as mobilization centers or staging areas for the Federal Emergency Management Agency (FEMA).

The intended outcome is a layering or cascading of support to the homeland, which has the potential to involve significant numbers of military forces. This layering should ensure that the appropriate level of support is provided at each level. The situation will be further exacerbated in the case of multiple events in the homeland. At the same time, military forces (including active duty, National Guard, and reserve forces) will be deployed to conduct military operations outside the homeland. At each layer of support, in the homeland or abroad, individuals will be filling critical positions and functions—their availability will be essential to the successful conduct of these missions and functions. The same individual cannot support multiple critical functions at the same time.

Despite the logic of this statement, the study came across several anecdotal indications (but not much hard data) that many individuals are filling multiple roles in the cascade. This is most apparent for the National Guard and reserves:

- Estimates suggest that 10–15 percent of the National Guard are also first responders.

- Fifty percent of forces in Iraq in 2006 were guardsmen.

- Thirty-three percent of the National Guard deployed in Iraq or for Katrina in September 2005.

More accurate data were not available because the data are not collected on a systematic basis. Absent specific data, the full extent of the impact cannot be quantified. However, it is likely that local communities, state leaders and planners, and DOD planners could be counting on the same individuals to fill two or even three roles at the same time within a global asymmetric warfare situation.

The "worst case" model would be the local first responder to a specific incident, who is then activated by the state governor as a member of a National Guard unit (to respond to the same incident, another incident in the state, or under EMAC to another state), and whose unit is subsequently called to federal status to provide homeland support or to engage in military operations overseas. Figure 3 illustrates the dilemma. As a result, it is critical to planning at every level that the extent of "double counting" be quantified at a higher level of resolution, and its effects on planning assumptions understood.

One Individual, Many Possible Roles

National Guard unit could be activated by government to:
Support the incident
Support incidents in other parts of the state
Support other states under EMAC

National Guard unit could be federalized to:
Support the incident
Support other incidents
Be deployed overseas

First responders including:
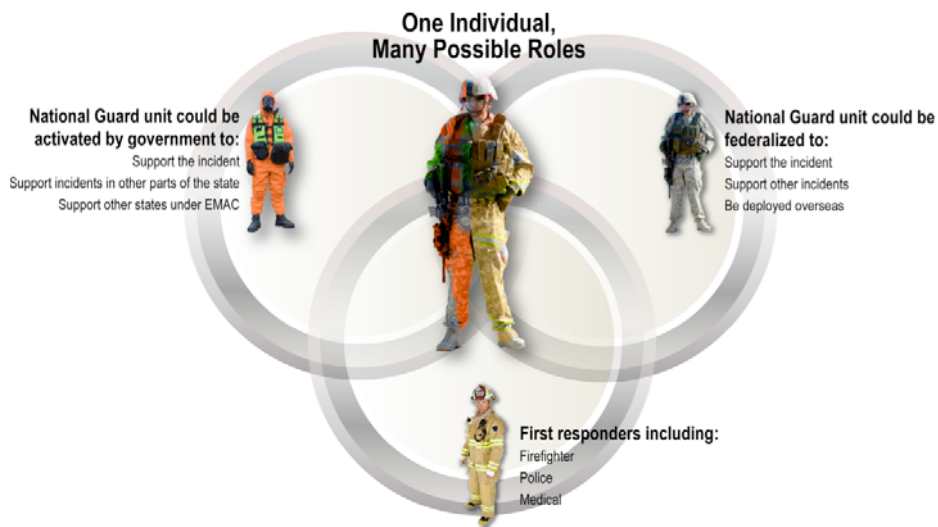Firefighter
Police
Medical

Figure 3. Double and Triple Counting of the Reserve Components

RECOMMENDATIONS: DOD ROLES AND RESPONSIBILITIES

Addressing the shortfalls identified in this chapter will require significant resources, sustained commitment, and greater involvement on the part of DOD with other agencies, especially with DHS. To begin the process, the Board recommends the following:

1. **The Secretary of Defense task the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD [HD&ASA]) to revise and implement DOD policies and procedures covering homeland defense requirements.** This tasking should include the clarification of relationships, roles, and missions of all the elements (federal agencies, civilian and private sectors, state and local responders, and law enforcement) of homeland defense at a level of specificity highlighted in this chapter. Clarification of this sort would go far to eliminate the uncertainty and/or confusion about what is expected of DOD and what others can indeed expect of DOD. The scope should include contingencies where DOD assumes the lead response role in the homeland. Only those policies and procedures that lower the barriers to planning, exercising, information sharing, cooperation, and coordination across the entire homeland defense community should be approved.

2. **Service Chiefs and the National Guard Bureau assess force requirements and adjust, adapt, and/or expand force structure to meet the "one game" demands of the future.** Force structure should be built not just on the regional command war plans for overseas operations, but also on those being developed by U.S. Northern Command for homeland operations. The effort will involve the development of accurate databases to understand the civilian skills and job commitments of the reserve components in order to assess and address the "double counting" issue. It will also require close planning and coordination with the Service Secretaries across the spectrum of doctrine, organization, training, materiel, leadership and education, personnel, and facilities in order to ensure that shortfalls are addressed.

Chapter 3. Assuring Deployment and Supply

One of the critical issues facing the military in time of war is deploying forces to the battle site and providing supplies of all sorts (from meals to fuel to weapons). If the homeland is under attack, then the primary base of support and the supply chain may be significantly impacted. One concept for addressing this concern is "resilience."

Merriam-Webster's on-line dictionary defines resilience as: 1) the capability of a strained body to recover its size and shape after deformation caused especially by compressive stress; 2) an ability to recover from or adjust easily to misfortune or change. The concept of resiliency with respect to the nation's critical infrastructure and DOD logistics supply chain goes beyond protection and hardening of potential targets to include redundancy as well as rapid response and recovery.

This chapter examines how well the nation is prepared to meet the simultaneous demands of fighting a war both in the homeland and abroad. The assessment is based on the resiliency of the nation's critical infrastructure and functions, DOD processes and status for ensuring resiliency, DHS processes and status for protecting the nation's critical infrastructure, DOD preparedness (supply, logistics, installations), as well as family and individual preparedness.[7]

Critical Functions and Infrastructure

The nation must be prepared for a future adversary who conducts clandestine and well-executed attacks on the U.S. homeland, while simultaneously executing overt military actions at great distance from the United States. Can DOD defend the homeland if required to deploy? Can DOD deploy if the homeland is under attack? Answering these questions must start with addressing more basic ones:

- What military missions and functions must be assured from the homeland?

- What assets and operations are critical to that assurance?

- How do we figure that out?

---

7. Relevant excerpts from DOD's Strategy for Homeland Defense and Civil Support can be found in Appendix B.

- Who is responsible for doing what (DOD, DHS, others with key infrastructure responsibilities), and do we understand how the system expects to function under stress?

- What will be the availability of critical national assets and capabilities?

- What competing demands will be made on the military and National Guard?

- How do DOD and the nation measure its preparedness—or readiness?

The United States has transitioned to a global economic power with an agile, but fragile, set of interconnected and interdependent infrastructures. In the 1800s, the nation consisted primarily of a distributed collection of communities in rural areas, cities, and states with somewhat independent supply, social, and governing structures. In the 20th century, national networks emerged to unify these local systems, which became dependent upon each other. The consequence is a system that is economically focused on high performance at the lowest possible cost, which leads to a highly efficient system, but one with few redundancies. Lack of redundancy opens the structure to multiple vulnerabilities, especially single node failures, with large-scale (national and international) economic impact.

For purposes of this discussion, the study assumed a multi-point attack on the United States that is severe enough for the President to declare the nation "under attack," with federal authorities in overall control. Under such conditions, national resources will be stretched to the point where demands for national and international requests will go unmet. Local resources will also be overwhelmed and could face societal panic, if people feel localities are unable to provide law and order, medical care, municipal services (water, refuse), food, energy, trade, transportation, information system availability, and protection from the elements.

Under such a scenario, two critical warfighting requirements occur simultaneously: defending against domestic catastrophe and ensuring deployment and supply. Domestic catastrophes occur in an environment of a large, undisciplined population, and these violent attacks can have a destabilizing effect on society. On the other hand, military deployment and supply take place in a disciplined organization, trained to accomplish the mission. Yet the two are linked—military deployment and supply is critically dependent on infrastructure elements that may be destroyed or severely compromised in a domestic catastrophe. Furthermore, both missions will draw on many of the same people and equipment, as discussed in the previous chapter. The protection challenge for the U.S infrastructure is significant, as illustrated in Table 5.

Table 5. Size Indicators of Some Critical Infrastructure and Key Assets

Agriculture and food	1,912,000 farms; 87,000 food-processing plants
Water	1,800 federal reservoirs; 1,600 municipal waste water facilities
Public health	5,800 registered hospitals
Emergency services	87,000 U.S. localities with 30,000 fire departments (80% volunteer); 18,000 law enforcement agencies
Defense industrial base	250,000 firms in 215 distinct industries
Telecommunications	2 billion miles of cable
Energy	▪ *Electricity:* 2,800 power plants ▪ *Oil and natural gas:* 300,000 producing sites
Transportation	▪ *Aviation:* 5,000 public airports ▪ *Passenger rail:* 22,000 miles ▪ *Freight rail:* 120,000 miles of major railroads ▪ *Highways, trucking, and busing:* 590,000 highway bridges ▪ *Pipelines:* 2 million miles of pipelines ▪ *Maritime:* 300 inland/costal ports ▪ *Mass transit:* 500 major urban public transit operators
Banking and finance	26,600 FDIC insured institutions
Chemical industry and hazardous materials	66,000 chemical plants
Postal and shipping	137 million delivery sites
Key assets	▪ *National monuments and icons:* 5,800 historic buildings ▪ *Nuclear power plants:* 104 commercial nuclear power plants ▪ *Dams:* 80,000 dams ▪ *Government facilities:* 3,000 government owned/operated facilities ▪ *Commercial assets:* 460 skyscrapers

Source: *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003

DHS has the interagency lead for critical infrastructure protection, and has assigned each infrastructure sector to its most logical federal "owner" or sector-specific agency (SSA). An important consideration for each SSA is the fact that improvements in infrastructure resiliency will come about largely by the efforts of its private owners. The development of the public-private partnership is no more important than in this area. (The next chapter addresses the public-private partnership in more detail.) The SSA works with the private sector via its Sector Coordinating Council (SCC) to develop a sector-specific risk mitigation and resiliency improvement plan. That plan helps prioritize federal investments, as well as focus private efforts for business continuity. The SSA joins with other interested federal agencies to form a Government Coordinating Council (GCC) where cross-sector issues can be addressed.

DOD has responsibility for not only the protection and assurance of its own military installations and facilities, but it is also the SSA for the defense industrial base infrastructure sector. In addition to leading the GCC for the defense industrial base sector, DOD has a presence on 14 Critical Infrastructure/Key Resource National Sector GCCs: transportation; information technology; telecommunications; energy; chemical; commercial nuclear reactors, materials, and waste; government facilities; emergency services; public health and healthcare; drinking water and water treatment systems; dams; postal and shipping; food and agriculture; and national monuments and icons.

DOD Approach and Progress for Assuring Defense Critical Functions

DOD is beginning to make progress in identifying what is critical through the Defense Critical Infrastructure Program (DCIP) within ASD (HD&ASA), supported by the Naval Surface Warfare Center in Dahlgren, Virginia. Together with the combatant commanders, a "mission assurance" process is being developed and implemented—a process that incorporates many of the recommendations of a prior Defense Science Board (DSB) study regarding risk management and mitigation.[8] The process focuses first on identifying critical functions and capabilities, followed by identifying and assessing those few assets or facilities necessary to ensure the functions or capabilities. The process also provides guidance to assess a number of critical infrastructures "outside

---

8. *Report of the Defense Science Board Task Force on Critical Homeland Infrastructure Protection,* January 2007.

the fence" on which the combatant commanders might depend and/or need to defend. Figure 4 illustrates the mission assurance process, which proceeds as follows:

- Combatant commanders identify critical capabilities, missions, and functional networks (41 have been identified as in the most critical tier 1 category; several hundred are in the tier 2 category).

- The critical capabilities, missions, and functional networks are decomposed into defense critical assets that are assessed against threats, hazards, and vulnerabilities (risk assessment). Risk of loss is assessed and mitigation actions are proposed (protect/harden, duplicate/backup, re-locate, and others).

- The Services then analyze the results and the proposed mitigation actions (N.B.: The Department is at this stage now).

- Finally a senior group (the Deputies Advisory Working Group or its equivalent) adjudicates differences and prioritizes for resource allocation.
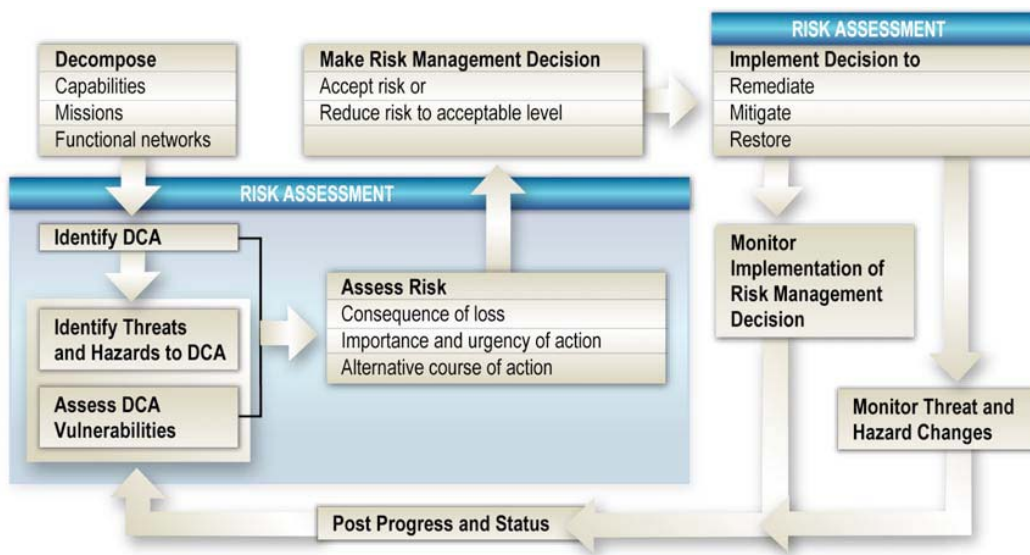

Figure 4. DOD Mission-Assurance Process for Critical Infrastructure Protection

Specifics are classified, but examples of DOD mission critical functions and related assets include:

- command and control
- ballistic missile defense
- intelligence, surveillance, and reconnaissance
- power projection

The study judged that the list appeared logical, but neither complete nor consistent in the application of the tier criteria.[9] Recognizing that it is a process in its early stages, the DSB nonetheless believes that more effort must be applied to get it right and complete.

With respect to the defense industrial base, efforts led by ASD (HD&ASA)/DCIP are underway to work in a similar fashion with defense industrial base owners through National Guard assessment teams, but this too is a work in progress. Some initial positive outcomes (classified) are notable, but the process has not yet enjoyed widespread visibility. There is also the question of how far the private sector will go to meet what it may view as DOD special assurance needs over and above business continuity to support other customers. In that respect, DOD will have to address what incentives it might be able to offer.

One factor contributing to the relatively slow progress at DOD is the recent reorganization in the Office of the Under Secretary of Defense for Policy, which decimated the staff devoted to this area. This will make it extremely difficult to implement the inspired proposal to create a Deputy Assistant Secretary of Defense for "mission assurance," which would consolidate policies, programs, and procedures for CBRNE (chemical, biological, radiological, nuclear, and high-explosive), anti-terrorism, consequence management, critical infrastructure protection, and continuity of operations in one office. The biggest gap, however, is that no one is charged with the responsibility or authority to ensure that corrective actions are taken, either within DOD or nationally through DHS.

---

9. Tier 1 Task Critical Asset (TCA), loss or disruption will cause failure of multiple assigned strategic missions (determined by combatant commander); Tier 2 (TCA), loss or disruption will cause failure of a single assigned strategic mission or cause severe disruption to mission accomplishment of several assigned missions (determined by combatant commander); Tier 3 (TCA), loss or disruption will cause severe disruption to mission accomplishment of a single assigned strategic mission (determined by combatant commander). These TCAs are then analyzed by the Joint Staff, and TCAs that support multiple combatant commanders are considered to be Defense Critical Assets (DCAs).

The result is that despite nearly seven years since 9/11, many U.S. critical infrastructures remain vulnerable, and for DOD, many critical supply chains—to include meals ready to eat, missiles, munitions, and fuel—are not as resilient as they should be.

DHS Process and Status for Critical Infrastructure Protection

DHS has a related but different approach to identifying critical national functions. It focuses on 17 sectors called Critical Infrastructure/Key Resources. The Homeland Security Act of 2002 provides the basis for DHS roles and responsibilities. HSPD-7 outlines the national approach. Other key documents and plans include the *National Strategy for Homeland Security*, the *National Strategy for Securing Cyberspace*, the *National Strategy for the Physical Protection of Critical Infrastructure/Key Resources*, and several other HSPDs.

With these strategies and directives as a basis, DHS has led the development of the National Infrastructure Protection Plan (NIPP). The NIPP's overarching goal is to "Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR (critical infrastructure/key resources) to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency." The DHS approach for managing risk is that "Sectors that are primarily dependent on fixed assets and physical facilities may use a bottom-up, asset-by-asset approach, while sectors (such as Telecommunications and Information Technology) with diverse and logical assets may use a top-down business or mission continuity approach."

Sector-specific plans (SSP) support the NIPP by establishing a coordinated approach to national priorities, goals, and requirements for critical infrastructure and key resource protection. The SSPs provide the means by which the NIPP is implemented across all critical infrastructure and key resource sectors, as well as a national framework within which each sector can address its unique characteristics and risk landscape. This coordinated approach allows federal funding and resources to be applied in the most effective manner to manage risk. DHS has focused, so far, on assets and facilities versus operations and functions. DHS coordinates and provides guidelines, but cannot edict standards for security across sectors (although it should be promulgating best practices). At this point,

the DHS has identified 36 "Tier 1" assets and over 2,500 "Tier 2" assets.[10] These include several identified by DOD. How the tier criteria are developed and applied were not clear (to this study team, at least) nor were the processes by which the SSAs or SCCs influenced choices.

The DSB discovered inconsistent involvement by private sector owners and operators in the DHS process. The DHS Office of Infrastructure Protection is redirecting the National Infrastructure Simulation and Analysis Center to provide analytical support to sectors and agencies, and to characterize interdependencies among sectors, so that a more consistent and carefully analyzed set of priorities can be established. Significant private sector engagement will be required to achieve a rigorous and robust analytic capability. In the view of the DSB, information assurance, highlighted in the accompanying side bar, is probably the most pervasive issue in infrastructure protection.

Information Assurance

Pervasive to critical infrastructure/key resource assurance is information assurance (corroborated by both the technology and counterforce panels of this study, and explicitly highlighted in the following section on logistics). Two of the most significant recommendations of the Defense Science Board *2006 Summer Study on Information Management* were to: 1) identify the DOD information management system as a weapon system and treat it with all the same processes as that implies for readiness assessments and for use in exercises and in training; and 2) develop and fund robust information assurance efforts to lessen the vulnerability of the system to attack, improve its resilience and assure ability to operate with a degraded system. In part II of this current study, concepts of testing and operations to improve information assurance are recommended. Yet, the DSB believes that more should be done to not only protect the military system but commercial cyberspace as well. All facets of the U.S. economy are critically linked to efficient transmission of information. Therefore, a whole new look is required.

Finding. The number and complexity of cyber transactions on today's Internet are well beyond those conceived at the initial design stages of ARPANET. A new look at network design, operation, and traffic flow protocols is needed with a fresh insight in light of the enormous information exchange impact of the Internet today.

Recommendation. The Defense Advanced Research Projects Agency should assemble a small group of the brightest commercial and academic minds in the area of Internet operation to review current status and develop a plan for next generation Internet operation and protocols, building on, but not limited to, the National Science Foundation Genie Program. This group should recommend both short- and long-term enhancements to the Internet in all areas of operational effectiveness and security including recommendations for adequate development funding and realistic time scales for implementation.

---

10. Criteria for Tier 2 are sector-specific. Criteria for Tier 1 are more severe: (1) make the Tier 2 list and (2) satisfy at least two of the following: prompt fatalities greater than 3000; economic impact of $50B or more; psychological impact requiring mass evacuations with prolonged absence; or loss of governance or mission execution that disrupts multiple regions for more than one week, resulting in loss of necessary public services.

Logistics

The DOD logistics system has shown significant improvement in its ability to produce a rapid and precise response (Figure 5). Examples include:

- improved materiel availability
- implemented state-of-the-art commercial logistics information technology (IT) systems
- improved asset visibility
- designation of U.S. Transportation Command (TRANSCOM) as the distribution process owner

The TRANSCOM designation has, in turn, facilitated planning and coordination of DOD's supply chain. However, much more needs to be accomplished.
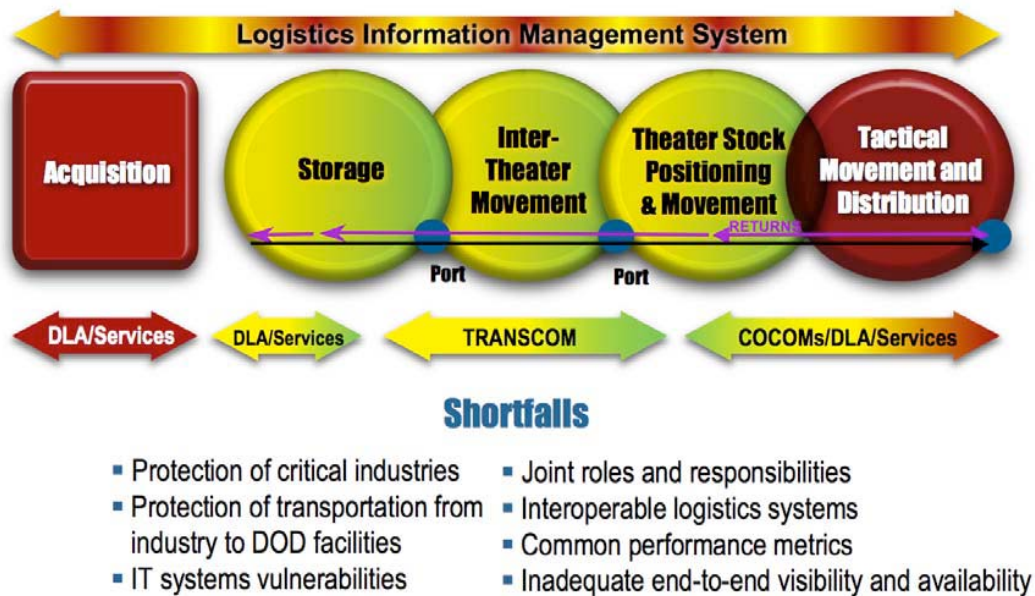

Figure 5. Assessment of Robustness of DOD's Supply Chain

The U.S. industrial base produces the vast majority of the material required to support the Department of Defense. There are many critical commodities and items that are essential for DOD to accomplish its mission, both abroad and at

home. Examples include: meals ready to eat, subsistence, medical, fuel, and spare parts for critical weapon systems. Many of these items (especially critical spare parts) are produced by sole-source companies or by companies with limited competition. Strategies have yet to be developed to assure the availability of these materials in the event of attacks on the homeland. Such a strategy should include:

- a comprehensive list of critical commodities and items, updated and (re)prioritized on a routine basis

- assessment and assurance of transportation routes required for their delivery from industry to DOD facilities

- assessment and assurance of the sources of the critical commodities and items (for example, through developing alternative sources of supply for these items by contracting for the capability, but not necessarily the actual production)

This strategy has been used successfully for a limited number of medical items, and should be expanded significantly.

Each military service and the Defense Logistics Agency have either implemented or are in the process of implementing state-of-the-art commercial logistics information technology systems. However, no organization has been given the leadership role to ensure that these systems are interoperable and secure. These new logistics IT systems remain vulnerable to attacks because, by design, they must remain accessible to the commercial industrial base. DOD needs to develop a team of experts from both within DOD and the commercial sector to address this vulnerability.

At a higher level, as the DOD supply chain becomes more and more joint, the roles and responsibilities of the military services, combatant commanders, Defense Logistics Agency, the Joint Staff, and the Office of the Secretary of Defense need to be reviewed and clarified. Additionally, the Office of the Deputy Under Secretary of Defense for Logistics and Materiel Readiness (ODUSD (LM&R)) needs to develop common performance metrics for the entire supply chain.

The weakest segment of the DOD supply chain is often described as the "last tactical mile." In the logistics context, this represents the tactical movement and distribution of material once in-theater to its actual use by the warfighter. There has not been a coordinated effort to implement a single asset visibility system for the "last tactical mile" that would track and report consumption to

the DOD national provider or to the end user. ODUSD (LM&R) should coordinate this effort. Visibility of material in the "last tactical mile" must be an element of a joint logistics enterprise-wide visibility system, which uses a common data architecture, has authoritative sources of data, and is available 24 hours a day, 7 days a week.

Military Installation Protection

In addition to ensuring supplies from a robust private supply and internal distribution system, DOD must also assure the security of the forces it expects to deploy. The first step is assuring the inherent security of the installation itself. The military services each approach base security and force protection differently, but almost all of them plan on the support of local community emergency response resources in a serious incident (this being a consequence of outsourcing in this domain).[11] These civilian capabilities will not be available if the incident is an attack of a serious-enough scale. In particular, the study worries about the consequences of a WMD attack in terms of both the technical and operational shortfalls in both military and civilian communities.

A previous DSB task force assessed best practices for protecting U.S. military installations and recommended various approaches to enhancing security and protection of these facilities.[12] Principal findings included:

- DOD has many facilities that are vulnerable to the threats considered in the study, but a rational focus should be on protecting its critical military mission capabilities and functions (as opposed to installations and facilities).

- Interdependencies of DOD facilities upon non-DOD infrastructure are not entirely known.

- DOD, until recently, lacked policies and standards to guide installation commanders in securing, or creating contingencies around, infrastructure on which they depend.

---

11. For example, the Army has consolidated installation management under a single command, as did the Navy earlier. Mission commanders establish what is critical and each garrison commander takes measures within his/her resources to protect and/or assure the critical function; special needs are funded by the mission command. Garrison and mission commanders coordinate plans for deployment under catastrophic scenarios. All garrison commanders have memoranda of understanding with the local response community for mutual aid. Plans are tested through training and annual exercises.
12. Report of the *DSB Task Force on Critical Homeland Infrastructure Protection*, January 2007.

- DOD Directive 3020.40, "Defense Critical Infrastructure Program," signed August 2005, assigns DCIP responsibilities at all levels across the department.

As a consequence of those findings, the task force recommended that:

- ASD(HD&ASA)/DCIP lead efforts to characterize defense sector infrastructure dependencies, develop risk mitigation guidance, and establish uniform DCIP standards (which is now underway, as outlined previously in this chapter).

- Services develop and implement plans to mitigate risk across owned installations; provide annual update to the Deputy Secretary of Defense.

- Installation commanders develop local assessment of dependencies and implement risk mitigation plans consistent with guidance and standards.

- Commander, U.S. Northern Command develop understanding of dependencies and risk mitigation by Services in the continental United States; other combatant commanders do the same in their respective areas of responsibility.

- DOD through ASD(HD&ASA)/DCIP monitor, collect, and share examples for installation preparedness as a basis for judging risk mitigation decisions within the previously recommended risk management program.

The study team was updated on some programs for installation risk assessments and management and came to believe that these prior findings and recommendations remain largely valid. With the exception of the start of the mission assurance process developed by ASD(HD&ASA)/DCIP, little has been done beyond earlier force protection programs.

Family and Individual Preparedness

Every mission begins at home.[13]

No amount of planning, training, and exercising can totally protect against homeland attacks. The second line of defense, as discussed in the previous sections of this chapter, must be to harden government and civil organizations

---

13. Quantico Marine Corp Base, sign at entrance to military housing.

and critical functions against the effects of an attack and/or to assure an orderly recovery. The third line must be preparation of individuals and their families to withstand the impacts of a national catastrophe.

The study team was reminded of the many examples where individual preparedness proved pivotal in mitigating the consequences of a natural disaster, and the strong role it played in the early days of the Cold War. The effectiveness with which Florida is able to contend with hurricanes, having learned valuable lessons from Hurricane Andrew, especially when compared to Louisiana's inability to deal with Katrina, shows how state and local preparation can blunt a disaster's impact. The preparedness of the Swiss population to hunker in place during military emergencies is another good example of preparedness. More often, however, unless catastrophe is a near-term reality, most major domestic preparedness programs are likely to fail because of competing, short-term resource needs. Katrina was widely and credibly forecast for many years, yet Louisiana remained poorly prepared (Table 6).

Whatever measures are taken to deal with domestic catastrophes, they all must have intrinsic value—improved efficiency, greater safety, better level of service, less cost. Government should not be the principal source of resources, but should lead in encouraging improvements, providing guidelines, and offering the venues for educating and practicing how well prepared communities are—or should be. DOD's success in assuring the deployment and supply of expeditionary forces, or defense against domestic catastrophe, is utterly dependent upon the military community's ability to function adequately in a post-attack or pandemic environment. Homeland security and the ability to continue military operations in a hostile environment at home is a capability supported by three pillars: government, private sector, and individuals and families. If any of these are weak, the system, like a three-legged stool, is unstable, and seriously degraded, at best. The sentiment was best summed up by Jim Schwartz, Arlington County Fire Chief, Incident Commander, Pentagon 9/11: *"A prepared society lessens the burden on DOD to do its warfighting job."*

Table 6. Progress Toward Preparedness

In the aftermath of Katrina, President Bush demanded that "we find out the lessons, that we learn them, and that we fix the problems, that we take every action to make sure America is safer, stronger, and better prepared." The lessons referenced were those enumerated in The *Federal Response to Hurricane Katrina Lessons Learned*, 2006. These included planning, resource management, evacuation, situational awareness, communications, and coordination. These lessons are not new; in fact they have been repeatedly observed and stated:	**Hurricane Andrew, 1992** The Committee heard substantial testimony that the post-disaster response and recovery to Hurricane Andrew suffered from several problems, including: Inadequate communication between levels of government concerning specific needs;
Hurricane Katrina, 2005	▪ Lack of full awareness of supply inventories and agency capabilities;
Command centers in the Department of Homeland Security (DHS) and elsewhere in the Federal government had unclear, and often overlapping, roles and responsibilities that were exposed as flawed during this disaster … This lack of coordination at the Federal headquarters-level reflected confusing organizational structures in the field. … Furthermore, the Joint Field Office (JFO) staff and other deployed Federal personnel often lacked a working knowledge of National Incident Management System (NIMS) or even a basic understanding of ICS.	▪ Failure to have a single person in charge with a clear chain of command; and ▪ Inability to cut through bureaucratic red tape. *Governor's Disaster Planning and Response Review Committee Final Report, 1993:60* These shortfalls in communications are repeatedly identified in a multitude of after-action reports. Recent catastrophic events have resulted in many legislative actions and directives to address these problems:
The Federal Response to Hurricane Katrina Lessons Learned, 2006:52	▪ Homeland Security Act of 2002
September 11, 2001	▪ Homeland Security Presidential Directive-5 – Management Domestic Incidents
It is a fair inference, given the differing situations in New York City and Northern Virginia, that the problems in command, control, and communications that occurred at both sites will likely recur in any emergency of similar scale. The task looking forward is to enable first responders to respond in a coordinated manner with the greatest possible awareness of the situation. …. Emergency response agencies nationwide should adopt the Incident Command System. When multiple agencies or multiple jurisdictions are involved, they should adopt a Unified Command. Both are proven frameworks for emergency response.	▪ Homeland Security Presidential Directive-7 – Critical Infrastructure Identification, Prioritization & Protection ▪ Homeland Security Presidential Directive-8 – National Preparedness ▪ Post Katrina Emergency Management Reform Act of 2006 ▪ Intelligence Reform and Terrorism Prevention Act of 2004
The 9/11 Commission Report, 2004:315,397	▪ Implementing Recommendations of the 9/11 Commission Act of 2007
Oklahoma City Bombing, 1995	As evidenced by the enormous scope of the recent 9/11 legislation, it is widely perceived that little progress has been made in addressing these problems. Why don't we learn? Why are these problems a challenge to military operations?
The Integrated Emergency Management System (IEMS) and Incident Command System (ICS) were weakened early in the event due to the immediate response of numerous local, state and Federal agencies, three separate locations of the Incident Command Post (ICP), within the first few hours, and the deployment of many Mobile Command Posts (MCPs), representing support agencies.	
After Action Report: Alfred P. Murrah Federal Building Bombing, 2003:3	

Resiliency

According to FEMA, there have been over 1,700 federal disaster declarations issued since 1953, with an annual average of 31 events per year. The number of events during the last decade has exceeded this average (Figure 6). A capable enemy could take advantage of any one of these annual events as an opportunity to launch an attack while U.S. resources are strained and leadership distracted.

Americans have been conditioned over many decades to assume disaster relief assistance will come from communities adjacent to military installations and that other federal and state assets will be available. Firefighters and emergency medical technicians (EMT), for example, call for mutual aid when local systems are stretched beyond their limits, and major disasters routinely draw from resources across the nation including the National Guard.
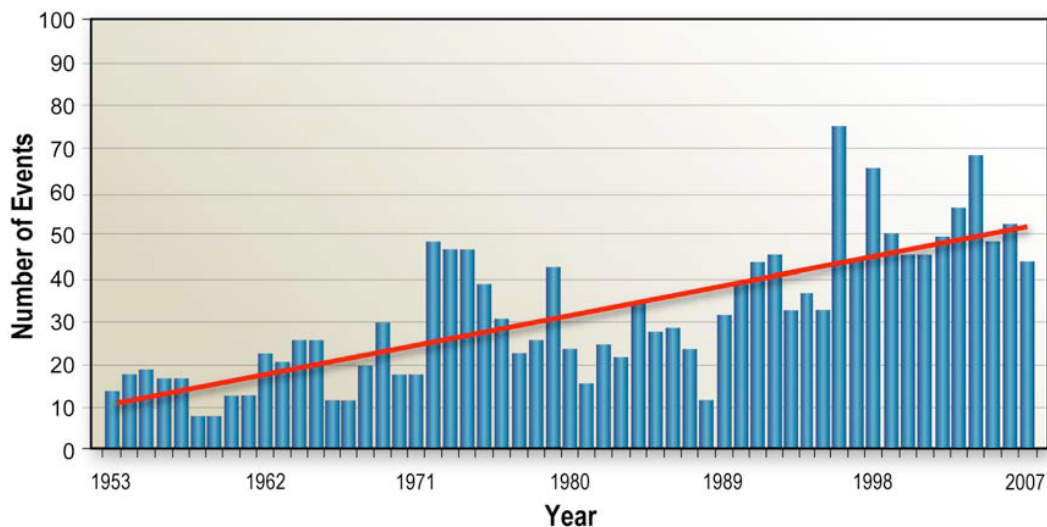
Source: FEMA, August 2007; http://www.fema.gov/news/disaster_totals_annual.fema

Figure 6. Number of U.S. Disaster Declarations

In the event of coordinated asymmetric attacks in many parts of the country and/or simultaneously with a natural disaster or avian flu pandemic, emergency responders and relief organizations may not be able to move across local or state borders. Resources will be severely strained and responders will be busy dealing with or preparing to deal with disaster on their home turf.

This reality has a sobering consequence. Even in the best of worlds, with all public and private emergency response and recovery systems operating as designed, help may not be there when military members and their families desperately need it. Evidence of this has been dramatically illustrated during countless disaster relief operations. To cite one example, in January 1998, the worst ice storm in New York State's recorded history paralyzed an area in a northern region of the state the size of Vermont, affecting over 18 million acres.[14] Twenty thousand utility poles had collapsed, the power grid was out of service for weeks, fallen trees made most roads impassable, and citizens were left to survive in the sub-freezing temperatures with only the food, water, and other supplies they had on hand.

For most of them, especially those with children, the experience was a terrible ordeal. Tragically, some did not survive. But for a few, the experience was no more than an inconvenience. These were usually older people who had grown up in a time when self-reliance was an accepted way of life. They had stockpiles of water, food, fuel for woodstoves, and medicines. One elderly couple replied to a rescue team that came to their home to offer assistance, "Go help somebody else, we're good here until Spring."

For military families, it comes down to one simple truth: the ability to function during or after a terrorist attack, pandemic, or natural disaster will reflect the quality of individual planning and preparations. Relying totally on traditional government responsive means of support in times of crisis is a strategic blunder with potentially dire outcomes.

A Culture of Preparedness

Instilling and promoting a culture of preparedness can provide both physical and psychological benefits to members and their families. There is much that can be done without great expense or effort to better prepare for both natural and man-made disasters.[15] Greater hazard awareness, training, home storage, and family communication and evacuation plans can provide greater peace of mind, strengthen emotional resiliency and empower DOD families to carry on through

---

14. Federal Emergency Management Agency. *New York Ice Storm Final Report*, January 1998. Retrieved on August 13, 2007 from http://www.fema.gov/news/newsrelease.fema?id=10489

15. Events include such things as floods, mudslides, hurricanes, tornados, fires, severe snow or ice storms, earthquakes, volcanoes, infectious disease outbreaks, severe power and fuel outages, hazardous chemical releases, nuclear or radiological incidents, acts of terrorism and/or civil disturbance.

a disaster. Preparedness also reduces the impact of a crisis and likelihood that these families will have to depend only upon the emergency relief infrastructure. Self-sufficiency also empowers members and families to help others and set an example the community can follow.

Most emergency preparedness guidelines encourage a minimum of 72 hours worth of supplies per individual for use until authorities are able to restore order and marshal emergency services.[16] However, experience has shown, and future disaster estimates (such as for a pandemic flu) indicate, that individuals should be prepared for much longer periods (two weeks to several months). Over time, individuals and families can build up their own home storage supply of food, water, medicines, and other necessary items including financial reserves and prudent debt avoidance.

Fortunately, preparedness at the individual and family level is the cheapest and perhaps most achievable of strategies to enable the nation's military community to continue operations during times of adversity. The idea of individual and family preparedness was reinforced by a group of noncommissioned officers (NCOs) with whom a part of the study team met: "We can't protect our country if we can't protect ourselves."

DOD must recognize that soldiers, sailors, airmen, and Marines will not likely be effective warfighters if they are simultaneously worried about the security of their families. While obvious steps, such as increased base protection, can be implemented, too many families live outside the installation. Having them educated and prepared for self sufficiency for up to two weeks would have immense morale, as well as actual, impact. The idea is not new in the homeland security context, but DHS's programs have been poorly funded and not well publicized.

---

16. Helpful Resources: DHS Be Ready, http://www.ready.gov/; FEMA, http://www.fema.gov/areyouready/, http://www.pandemicflu.gov/plan/tab3.html; Citizens Corps, http://www.citizencorps.gov/; CDC, http://www.bt.cdc.gov/; Florida Division of Emergency Management, http://www.floridadisaster.org/bpr/family%20preparedness/ index.htm

RECOMMENDATIONS: ENSURING DEPLOYMENT AND SUPPLY

The recommendations offered here are restricted to those that affect DOD, although there are many related items that DHS should address, as well.

The first set of recommendations is associated with ensuring deployment and supply. Toward that end, the Secretary of Defense, should direct:

- OSD ASD (HD&ASA)/DCIP to extend the mission assurance process to the defense industrial base and recommend approaches for addressing shortfalls.

- Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)) to work with defense industrial base owners to develop and implement corrective action plans.

- OSD ASD (HD&ASA)/DCIP to develop a prioritized action plan for addressing identified risks to DOD owned assets.

- U.S. Northern Command to lead the integration and analysis of defense agency critical functions, within the framework identified by ASD (HD&ASA)/DCIP, to enhance mission assurance, and to be the principal advocate for prioritized resource needs and shortfalls.

- Service secretaries to fund actions for mission assurance in owned functions.

- DUSD (LM&R) to ensure resourcing of logistics shortfalls:

  - to assure sources of supply and movement to DOD depots

  - to eliminate the last tactical mile issues

  - to make the information management system interoperable, robust, and resilient to attack, from both within and outside

An important additional aspect, not highlighted in the recommendations above, is that **DOD should also continue to carefully assess those parts of the infrastructure outside the defense industrial base on which it depends (telecomm, transportation, and others) to understand its robustness and availability in the environments characterized in this report.**

In the area of family preparedness, the Service chiefs of staff should actively promote the ability of military families to shelter at home for two weeks, or evacuate on short notice. They should:

- ▪ Reinforce message via NCO leadership academies, on-base medical community, Armed Forces Network, unit town-hall meetings, movie/TV celebrities, veterans' organizations, and other similar venues.

- ▪ Assure base commanders export this capability to adjacent civilian communities.

These recommendations were crafted on the strong advice of the NCOs consulted. They stated that the most effective way to achieve this capacity is through leadership, rather than by an administrative order. Families should not be "ordered" to prepare since orders could be politely ignored or even counterproductive, and impossible to enforce. Instead, leadership should help them understand why it is important and how to do it. Leadership should help them want to do it by implementing an education and outreach campaign. This should cascade from the chiefs down through example and encouragement to the individual unit level.

This message could be reinforced through NCO leadership academies, on-base medical community (pan-flu education), Armed Forces Network, unit town-hall meetings, celebrity endorsements, motivational speakers, promotional sales (at cost) via commissaries, as well as veteran and community organization involvement. DOD could also partner with other organizations such as the DHS-sponsored Citizens Corps on how best to prepare and educate members and their families.[17] According to FEMA, there are over 2,200 Citizens Corp Councils serving areas containing 75 percent of the total U.S. population.[18] Commissary stocks of long shelf-life items should also be increased. A significant collateral benefit (according to the NCOs) would be enhanced morale for members serving in assignments that separate them from their families.

---

17. American Red Cross, Center for Disease Control, Community Emergency Response Team, Department of Homeland Security, Federal Emergency Management Agency, Medical Reserve Corps Program, Neighborhood Watch/USAonWatch, and Volunteers in Police Service.
18. Citizens Corps, (2007). Retrieved on August 13, 2007 from http://www.citizencorps.gov/

Chapter 4. Building the National Team

"One Team"

The third dimension of the study's assessment of homeland defense addressed the status of the "national team" and DOD's involvement. As stated in Chapter 1, success in both homeland security and defense, whether against terrorism or more stressing peer-generated environments, demands a level of partnership and integration between and among all levels of government as well as with the private sector. In its investigation, **the study team found an almost exclusive focus in national strategy and plans on terrorist attacks**, most often a single event, even if distributed in nature (as a bio or cyber attack might be), **rather than on the more capable adversary envisioned in this study**.

In spite of the wake-up call provided by Katrina, progress toward an integrated national system is painfully slow, and the leaders who will have to act in those situations are choosing not to take full advantage of the training opportunities presented to them. Transitions in command from local to federal authorities, or from DHS to DOD, are not practiced. Most important, in the view of the DSB, is the lack of the homeland security/defense professional—either civilian or military. Academic programs are starting in several universities, but the government professional development track in homeland security and homeland defense, akin to those of other accepted prime missions of federal departments, has not yet been created.

The Homeland Security Team

Homeland security organizations responsible for dealing with national calamities are a diverse group: federal agencies, state and local authorities, and private firms. Some are new, some long-standing, and many, with principal and/or historic missions elsewhere, are included because of their special expertise or location. This community, in its present form, was hastily assembled following the 9/11 attacks on New York and Washington. Its "pick-up" nature has meant that homeland security and defense leaders often lack sufficiently broad perspectives across the numerous capabilities and equities participating in the homeland security mission. Some of the organizations do not fully appreciate what other team members (such as private firms that operate critical infrastructures) can offer. Many homeland security leaders—police and fire,

Coast Guard, FEMA, Federal Bureau of Investigation (FBI), National Guard, and others—have extensive experience in organizations with long histories of disaster response, recovery, and relief, but little experience working in a unified command environment. In today's threat environment, the planning and coordination needed for effective, timely response to national emergencies is greater than ever before in the nation's history. However, DHS, as the lead agency for creating that level of response, is still in its infancy.

At the state and local level, the DSB heard little that was positive about their federal "partners." DHS continues to reorganize, changes points of contact frequently, and brings to the table too much of a "we're in charge" attitude. This judgment is shared by the private sector, although the relationship between DOD and the defense industrial base seems to be better than with other sectors and their federal agency lead. With respect to U.S. Northern Command, DOD's principal operating "face" to the homeland security community, the command has been restrained by the view among the Department's leadership that the priority is—and should be—the "away game." Its low profile start has produced some serious perception problems that must be overcome with the many partners it will need to work with in a national emergency.

Possibly the most neglected member of the team is the private sector. The previous chapter discussed the importance to DOD (and of course, the nation) of critical infrastructure protection. The private sector owns most of the infrastructure and will be the most effective in restoring its function after an attack. As such, it must be as integral to the national team as government actors.

The real challenge to the nation's leaders is to ensure that the right agency, with the appropriate authorities and capabilities, is postured to lead a response at the appropriate time and with the necessary capabilities, from its own resources and/or from other supporting agencies and qualified contributors.

Interagency

The major departments of the federal government responsible for coordinating the elements of national power in the defense of the nation—the Departments of Defense, Homeland Security, Justice, and State, as well as the intelligence community—have varying degrees of authority and responsibility under different circumstances. Coordinating these efforts in remote theaters where roles and responsibilities are well understood is very difficult. The challenges are even more acute in the homeland. As the agency charged with protecting the

United States from terrorist attacks, DHS is responsible for leading the federal effort to prevent attacks and to respond to domestic events, whether man-made or natural. The Department of Justice, however, is the law enforcement agency with the lead for domestic terrorist incidents. The DOD has significant responsibilities in support of civil authorities and assurance of critical infrastructure, especially as it relates to the defense infrastructure base.

Under the National Response Framework, DOD is a primary agency for urban search and rescue and a support agency for nearly every other identified emergency support function: transportation, communications, firefighting, emergency management, mass care, emergency assistance, housing and human services, public health and medical services, oil and hazardous materials response, agriculture and natural resources, energy, public safety, long-term community recovery, and external affairs. The Army Corps of Engineers is the coordinator and primary agency for public works and engineering. Furthermore, DOD is identified as the coordinating agency for cyber incidents and as a cooperating agency for every other identified incident, including biological, nuclear, radiological, and terrorism law enforcement investigation. As discussed in previous chapters, DOD may also find itself in the lead should events become serious enough.

The *2005 DOD Strategy for Homeland Defense and Civil Support* recognizes the importance of the interagency: "Given that we face an emerging global, multi-dimensional threat, how should we prepare ourselves to operate 'jointly' across the interagency in a way that increases our effectiveness and decreases our vulnerabilities along the seams?"

An example of the effectiveness of a cooperative interagency construct is the Joint Interagency Task Force (JIATF)–South. This organization offers a unique model for day-to-day interagency operations. JIATF-South conducts counter-illicit trafficking interdiction operations, intelligence fusion, and multi-sensor correlation to detect, monitor, and handoff suspected illicit trafficking targets. It also promotes security cooperation, as well as country team and partner nation initiatives in order to defeat the flow of illicit traffic.

As a true interagency organization, membership in JIATF-South includes Customs and Border Patrol, Central Intelligence Agency, Drug Enforcement Agency, Department of Defense, Defense Intelligence Agency, Federal Bureau of Investigation, Immigration and Customs Enforcement, National Security Agency, and the National Geospatial-Intelligence Agency. This pairing of military and civilian government agencies under a unified command structure provides

for routine interaction between the entities that will need to work together effectively during a crisis.

Taking a lesson from the success of JIATF–South, the panel believes that the complex network of interdependent roles, responsibilities, and relationships demands a full-time integrated approach to homeland security and homeland defense activities through a number of such standing operational task forces. Some specialized examples, such as the National Maritime Intelligence Center, operated jointly by the Coast Guard and Navy, or the FEMA-DLA memorandum of understanding for DLA logistics support in national emergencies, are a good, but incomplete, start. For DOD, this means that U.S. Northern Command must step up—and in some cases, be allowed to step up—to a more proactive role in the interagency forum.

Federal-State-Local

In the case of a point attack, the first manifestation—and response—will occur locally. If or when those resources are overwhelmed, requests to the state will be made. At that point, the governor can call out the National Guard, as well as exercise mutual aid agreements with other states for additional response resources. When those avenues of response are tapped out, appeals for federal help can and will be made. However, the study heard from several state and regional response leaders that federal support can be slow in coming and what they can count on is largely unknown. In fact, the leader of one of the largest state emergency response offices stated that he plans for no federal help at least for three days after a major event. Interesting, as well, were comments from local and state responders that, by and large, they didn't need more "stuff" as provided by the DHS grant programs, but rather support for regional planning, training, and exercising.

With respect to prevention, state and local response leaders noted how much they can contribute, provided they have adequate threat information to recognize a threat when observed. In other words, a strong partnership with their federal counterparts can contribute significantly to threat mitigation and/or apprehension.

Several examples, positive and negative, highlight the power of effective federal-state-local partnerships.

Y2K Information Reporting and Communications

During Y2K, an Information Coordination Center was established by Executive Order 13073 and implemented through a system for reporting information from the local level to federal, as well as the provision of information of interest to state and local entities. The Information Coordination Center was the federally operated central point for gathering, analyzing, and summarizing information on systems operations during the Year 2000 date rollover. The guiding principles for its development and operation were:

- common, consistent operational picture to the President and decision-makers

- owners to fix their own problems at the lowest level

- use of existing agencies and capabilities; supplement where needed

- federal assessment, assistance where national interest, life, and safety merit

- Federal Response Plan used as the model

- individual agencies required to validate data they supplied

- information content planned, templated, routinely transmitted; significant events transmitted on an exception basis

- one voice to the nation

The model for the operation of the Information Coordinating Center is captured in Figure 7. The interagency and intergovernmental coordination and teamwork leading up to the rollover and immediately thereafter was commendable, and could provide a valuable model for information-sharing in high alert and/or crises for today's homeland security and homeland environment.

Figure 7. Y2K Information Flow

Response to Katrina

The failings of government at every level in the response to Hurricane Katrina have been the subject of many studies and treatises, both within and outside the government. This study turned to the experience of its members as well as outside sources to better understand specifics of the response. Clearly, state and local agencies and officials had inadequate planning and preparation to deal with the scope and scale of the event, but problems occurred at every level. The federal-state-local shortcomings, as developed independently for the Homeland Security Council, are summarized as follows:[19]

- Key decision-makers were unfamiliar with response plans.

- Federal agencies were slow to respond to the unprecedented requirements for federal support and coordination.

- Federal multi-agency coordination centers were not established in the field until after the height of the crisis.

- Critical public affairs structures were not operating at full capacity until weeks after landfall.

---

19. GEN Dennis Reimer, USA (ret.), DFI International Government Services, Analysis for the Homeland Security Council.

- The delayed establishment of key federal coordination mechanisms (such as a joint field office) exacerbated management problems and confusion in the field.

- The joint field office should have been fully resourced and pre-positioned prior to the event.

- Key federal, state, and local personnel, especially state National Guard leaders, should have been co-located to facilitate joint planning and decision-making.

- The military played a critical role in the response to Hurricane Katrina, but overall coordination was lacking.

- DOD's mission assignment process proved cumbersome and delayed the delivery of some resources.

- Greater operational planning is needed for specific defense support to civil authorities missions.

- Greater integration between U.S. Northern Command and the National Guard would have enhanced coordination and response.

- Equipment, personnel, and training shortfalls affected the National Guard response.

- DOD needs a greater understanding of the types of support that will be expected during a domestic disaster.

- DHS officials need greater awareness of the capabilities and authorities of DOD; conversely, key DOD personnel should be trained on the National Response Plan, the National Incident Management System, and the Incident Command System.

State and Local Intelligence Fusion Centers

Since 9/11 many state and local jurisdictions have established "fusion" centers for the purpose of collecting information on terrorist threats from a wide range of sources—including criminal investigations, the media, and tips from the public. Major metropolitan areas like Los Angeles and New York City pioneered these efforts. In 1996, Los Angeles County established the Terrorism Early Warning Group as an interdisciplinary group in which local, state, and federal agencies work together to share information and combine resources to enhance the ability to identify and respond to acts and threats of terrorism. Today at least

46 states and the District of Columbia have operating fusion centers to create a fuller picture of potential threats in their area.

In December 2005, President Bush directed federal agencies to "develop a common framework" for sharing security information with other levels of government and the private sector. The Departments of Homeland Security and Justice grants have helped fund many of the centers. DHS contributions have amounted to $380 million so far. There are several examples of how these centers have proven effective in apprehending suspects wanted by the federal government. But there is growing concern that without a plan to identify and allocate state funding to keep these centers operating, they could be in jeopardy. Many of these centers are voluntary endeavors and funding profiles vary greatly from state to state.

Public-Private

As discussed previously, DHS has been tasked with significant leadership responsibilities for identifying and protecting the nation's critical infrastructure and key resources. In addition to the Government and Sector Coordinating Councils (GCCs/SCCs) it has organized to facilitate the process, DHS has established the Critical Infrastructure Partnership Advisory Council (CIPAC) to support the National Infrastructure Protection Plan (NIPP). Through CIPAC, DHS coordinates federal infrastructure protection programs with infrastructure protection activities of the private sector and state, local, territorial, and tribal governments, and facilitates interaction among the stakeholders in each sector.[20] Because CIPAC meetings are customarily closed to the public, participants can more comfortably share security-sensitive information about threats, vulnerabilities, and protective measures.

During the course of this study, the DSB heard from representatives of the healthcare, defense industrial base, energy (electricity), information technology, communications, and emergency services sectors, and from three transportation sub-sectors (mass transit, oil and natural gas, and railroads). The consensus among these sectors suggested that the GCC/SCC "partnership" concept is good because it provides an opportunity to build trust among all stakeholders. However, the concept is not uniformly applied across all sectors.

---

20. CIPAC is exempt from the Federal Advisory Committee Act [P.L. 92-463].

For example, DHS and other sector-specific federal government agencies (SSA) worked with SCCs to produce sector-specific plans (SSP) required by the NIPP.[21] But the experience of the sectors was dependent upon the relationship with the SSA. The information technology sector, whose SSA is the cyber security component of DHS, was very satisfied with the experience, as was the oil and natural gas sector, whose SSA is the Department of Energy. Success was attributed to strong relationships and information sharing between the private and public principals.

On the other hand, where the Transportation Security Administration (TSA) is the SSA, some transportation sub-sectors have reported unsatisfactory experiences. Some sector representatives said DHS has the classic "left hand/right hand" problem and the "partnership" concept is contradicted at times by the regulatory responsibility and mind-set of some of its agencies, especially TSA. DHS must institute a consistent approach across all its components, and persist with other SSAs in reinforcing the importance of sector "partnership." To build trust, DHS must treat all sectors as full partners, not as subordinates. Rather than try to control the sector, DHS must facilitate security efforts of the sectors.

In spite of these problems, critical infrastructure owners and operators independently have taken steps to protect their assets and enhance the resiliency of their systems based upon their own risk assessments.[22] In many instances, however, they say they are not doing all they could be doing to protect their facilities and employees because of competing interests or issues.[23] For example, companies are chartered to fulfill a fiduciary responsibility to their shareholders for continuity of operations, but in some cases the activities needed for them to best protect their employees are counter to the activities to provide the best continuity of operations. Also, if they actually envisioned the kinds of scenarios contemplated in this study, it could put them on uncertain legal ground regarding risk disclosure and could result in a misperception on Wall Street that could negatively impact shareholders.

Another problem voiced by the private sector is that it does not have a full understanding of the threat since it does not have access to the same level of

---

21. Sector-specific plans appear to be programmatic plans to guide the DHS grant process vice operational plans for sectors.
22. DHS grants legislatively are restricted to public entities.
23. Comments by representatives of the defense industrial base sector.

information DHS has. Intelligence flow, at an appropriate level, to the private sector is limited due to the more commonly held principle of "need to know" vice "need to share." Therefore, business continuity plans are more often based upon a company's own evaluation of risk, which may or may not be consistent with DHS's assessment. A robust information flow from DHS and the responsible SSA would support effective deployment of limited private resources for business continuity and resiliency, and additional critical infrastructure protection that the government or military might require. Absent that, businesses are likely to limit security investment to the level judged prudent for business continuity.

A related intelligence issue is the private sector's view that even when DHS intentions are good, it does not always recognize when a sector has a "need to know" due to complex interdependencies with other sectors, unfamiliarity with sector operations, and co-location of infrastructures. As an example of this problem, DHS did not notify the railroad sector of the 2006 Iraq chlorine vehicle-borne IED incidents even though the industry has cleared personnel and a DOD-cleared facility.[24] Although the attacks in Iraq involved chlorine trucks and not rail tank cars, detailed information about the Iraq attacks is very relevant because of the volume of chlorine transported by rail and because the railroad industry is in the process of designing the next-generation chlorine tank car.

Perhaps the best example of this complex problem occurred in August 2004, when DHS raised the alert level to Orange for the financial services sector in New York City, Northern New Jersey, and Washington, D.C., and issued direct warnings to specific entities in those regions, including the Citigroup buildings in the New York City area; the New York Stock Exchange Building in New York City; the International Monetary Fund and the World Bank Buildings in Washington D.C.; and the Prudential Insurance Company of America in Newark, New Jersey. DHS did not, however, issue warnings to the owner and manager of the Citicorp Center, Boston Properties. At that time, Citicorp did not own, manage, or even occupy a majority of the Citicorp Center. Nor did DHS issue warnings to owners and operators of other critical infrastructure located adjacent to or under these buildings. This left mass transit operators, water, gas pipeline,

24. After a similar incident in 2007 was reported in the press, the industry sought more information by submitting a list of Industry Information Requirements to DHS. As of this writing, DHS has not fully answered the industry's information requirements.

telecommunications, and electric companies unaware of the potential danger to their operations.[25]

The assignment of sector subject matter experts to the DHS intelligence unit (Homeland Infrastructure Threat and Risk Analysis Center [HITRAC]) would go a long way toward closing the intelligence sharing and analysis gap. However, the clearance process and the DHS requirement for full-time vice part-time personnel are impediments to progress.

In the late 1990s, many sectors established Information Sharing and Analysis Centers (ISAC) at the urging of the federal government.[26] ISACs were tailored to the needs of the individual sectors. Some sectors received federal funding for their ISACs; other ISACs were self-funded. But DHS ended federal support for sector-established ISACs and established the Homeland Security Information Network (HSIN), a "one-size-fits-all" approach. The level of satisfaction with HSIN depends upon the constituencies of the SCCs. For example, where the previous ISAC was not well supported, HSIN is a step forward. However, where SCCs are safety and security standard-setting organizations for their industries, and where sectors are network industries, more robust information sharing within the sector is traditional and indeed required for safety (such as the emergency management and railroad sectors). HSIN does not measure up to their standards for timely and useful information. The panel questions whether a single system could ever meet the diverse needs of the many sectors it is attempting to support.

Leadership for the National Team

Response to national catastrophes requires close cooperation among leaders and their organizations, which, in turn, depends on leaders with a sound vision of the team operation and relationships with other team members. This concept is the homeland defense equivalent of "jointness" as practiced within the DOD. The federal government is in the unique position to unite the homeland team.

Forming a truly joint homeland security and defense team starts with developing leaders with a joint perspective—both through education and career experiences—building an interagency cadre of leaders, whose

---

25. "Public-Private Sector Intelligence Coordination," National Infrastructure Advisory Council, July 11, 2006.
26. Pursuant to Presidential Decision Directive 63, Protecting America's Critical Infrastructures.

understanding of homeland defense transcends their immediate position. Carrying out homeland defense requires "joint operations" teamwork; leading such operations requires a truly joint leadership team. Homeland security and defense—regardless of agency, level of government, or public or private sector—must be seen as a professional opportunity for those seeking to lead in this critical field.

The DSB saw no such recognition of the need to develop homeland security leadership in the same manner as the nation has invested in developing national security leadership. The military and civil service education, training, and advancement processes for the latter could and should serve as a model for a parallel track for homeland security.

Plans and Exercises

There appear to be numerous doctrinal and operational plans, with embedded processes for review and revision of the plans. **But processes to ensure that the plans are practiced and capabilities measured against readiness metrics are lacking.** While there are many exercises (possibly too many), the exercises are highly scripted, unconnected to each other, and typically focus on a top-down approach (where the supporting organizations are "training aids" to the senior-level players) instead of bottom-up approach (focusing on an integrated and layered response beginning with the initial event). Even the national-level exercises have not been effective—more often broad than deep, where the real lessons get learned. They are often stopped before the more difficult issues of transfer of command, or employment of specialized assets, or unknowns (like public panic), come into play. Figure 8 is a compilation of the top two levels of national exercises planned for the next five years. Surprisingly, this chart represents the first time that all such exercises were captured in one place. The DSB, and the DHS program manager responsible, note the lack of connection and integration among them.

More worrisome than the disjointed nature of the exercises is the lack of any process for effectively "learning from" the lessons of these exercises. While there are mechanisms for capturing observations and documenting problem areas identified during the exercises, there are no mechanisms to promulgate the lessons to the wider homeland security and homeland defense community, or to implement, track, and record corrective actions taken as a result of the lessons. DHS has recognized the problem and is standing up the "National Exercise Program" to put more discipline into their processes. But the discipline inherent in DOD is lacking in the homeland security community, so that promulgating lessons learned will be a much more difficult task.
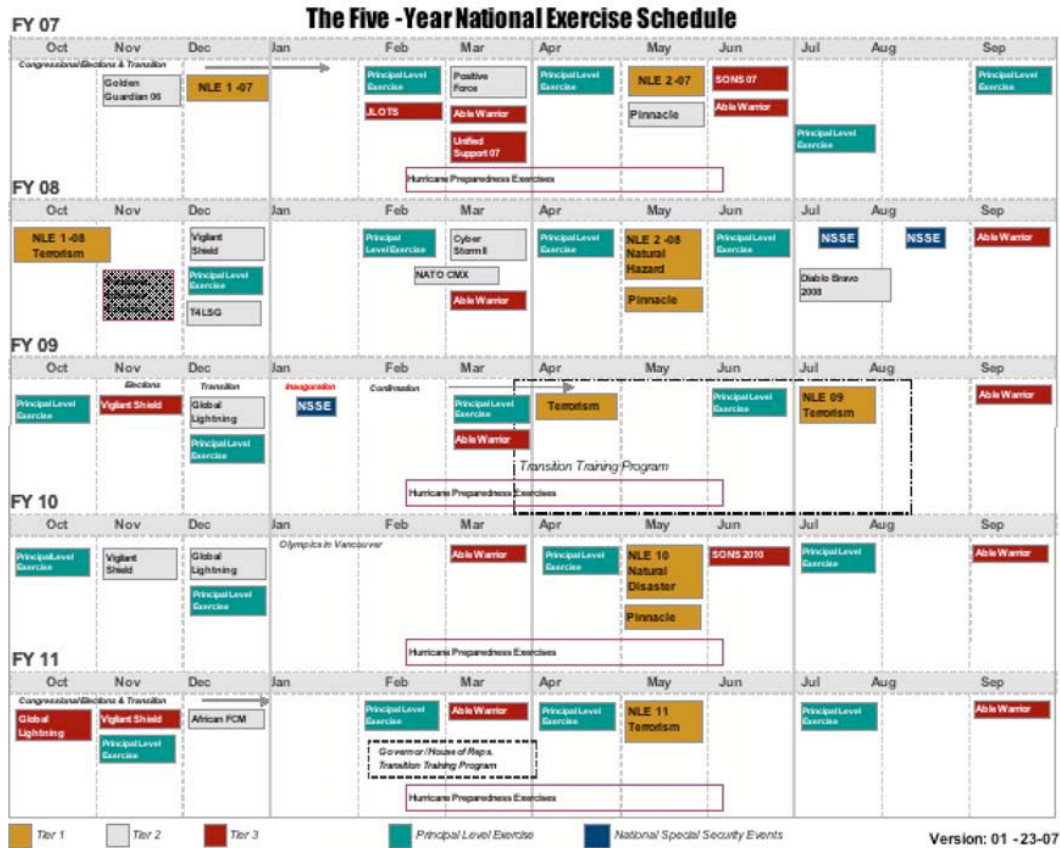
Figure 8. The Five Year National Exercise Schedule

The gap extends to DOD, where relevant exercise programs do not appear to be effectively linked to national objectives. For example, the Joint Forces Command (JFCOM) Noble Resolve exercises, initiated in the current year, are an experimentation series designed to address homeland scenarios. These are not yet linked to DHS' National Exercise Plan, nor do the JFCOM personnel involved seem aware of the official DHS scenarios or of existing tools and models already developed. The DSB was quite dismayed to learn that the maritime intercept scenario of Noble Resolve-1 was artificially limited to avoid interagency handoff or coordination issues.

Northern Command's Ardent Sentry exercise series is a move in the right direction to involve local and regional responders, but its objectives appear to be overly broad and shallow, in that there are too many players with disparate goals

and exercise objectives. One reason appears to be that many of the players may be using the exercises as their primary means of training, rather than using the exercise as a "capstone" event to validate plans and training and to assess interactions with other participants.

The Defense Threat Reduction Agency and DHS experience from exercises such as BioNet (military-civilian response to a bio attack in the San Diego region) and with U.S. Pacific Command (military-civilian response to a nuclear event on Oahu) provide numerous pointers for military-civilian combined operations associated with WMD events. A key lesson learned from these experiences is the importance of exercising mutual aid responsibilities anticipated in plans, including coordinated approaches to public information and interoperable communications for response elements. The exercises also highlight operational and technical shortfalls in planning for WMD consequence management and multiple, major events. However, it is not clear what impact these exercises have had beyond the participants themselves—in other words, these lessons have not informed the homeland security and homeland defense community at large.

Stepping back, the DSB concluded that most of the exercise examples lacked realistic design and planning, interagency integration, and application of lessons learned. Exercises appeared in many instances to be a collection of activities artificially aggregated into an exercise construct. It is difficult to conduct a good exercise, whereby "good" means: (1) provides answers to questions established prior to the exercise and (2) effectively meets objectives for all participants. If the homeland defense community is ever to run meaningful and useful tests that give answers as to the value and shortcomings of U.S. homeland defense operations, six rules, derived from work on design of experiments, should be followed:

- **The exercise must have an objective.** It must be designed to stress specific elements of the operations plan (in many homeland security and homeland defense cases, a unified operational plan) in ways that result in lessons that will improve the plan and participants' actions. Exercises are learning (not training) opportunities.

- **There must be a model for the exercise.** If the objective of the exercise is to test operations in response to a specific event, there must be a model for that response beforehand against which to evaluate the results of the exercise. This model may or may not be a computer model, but it should be easy enough to understand that anyone involved in, or reviewing, the exercise can clearly understand the exercise.

- **The exercise design should allow observation based on the model.** If the exercise is designed to produce a given result, the result should be well understood, observable, and comparable to that from the model.

- **The data obtained by early observations should be such that they can be analyzed quickly** so that the model, which is bound to be wrong in some respects, and the modeling methods can be changed prior to the next phase of the exercise.

- Exercise design and execution must provide a comprehensive, objective, and accurate **after-action reporting mechanism**, coupled with a corrective action plan and a **commitment to resource** implementation by all parties.

- Regardless of the importance of the exercise in providing answers related to new operations, **the exercise should also provide teaming opportunities for the participants** to work together with other members of the homeland security/defense team.

Why Can't We Learn?

With the current preparedness system and exercise program, the involved agencies at all levels of government unfortunately end up training on real world events. The history of major disasters shows the same lessons observed, over and over again. The list invariably includes:

- communications
- leadership
- logistics
- planning
- situational awareness
- operations
- resource management

Learning from these lessons is much less evident. During each new event solutions found earlier are often re-invented. When asked about specific threats and exercises, a representative of the International Association of Fire Chiefs indicated little training to address enemy attacks on the homeland, but "I'm sure if it happens, we'll find a way to get it done."

The Department of Homeland Security sponsored a workshop soon after Katrina to examine why the emergency response community finds it difficult to learn certain lessons. This workshop uncovered several barriers to learning and achieving change. These findings were echoed by many responders, homeland security professionals, and private sector representatives with whom the study met. In summary, they are:[27]

- lack of motivation for change
- ineffective review and reporting processes
- unproductive learning and teaching
- poorly planned and executed exercises
- resource constraints

Motivation for Change

Several barriers to effective resolution of these issues exist. First and foremost is motivating the sustained energy required to achieve lasting change. Organizational change is extremely difficult, especially in the emergency response area. Memory is short-lived and the ability to garner the political will to make well-thought out and rational changes in the national response system is often short-changed due to other pressing matters such as failing schools, high fuel prices, and other economic calamities. Even when important lessons do result in calls for change, the disparate emergency response community at all levels of government lacks a shared vision of what to do about those lessons.

Another barrier to sustaining motivation for change is the irregular nature of significant events. In general, the longer lasting effects of even very large events are confined to a relatively small geographic region. To improve response on a national level, agencies and organizations must be willing to learn from events even if they were not directly affected. This calls for organizations to think collectively and be willing to learn from each other. The attitude that "it won't happen here or it won't happen again" is pervasive. When asked after her Katrina experience in Louisiana "What can the federal government do to help you the next time such an event occurs?," a local emergency response director replied, "Hold me accountable." The need for effective leadership and

---

27. A more detailed report can be found in *Homeland Security Affairs, The Journal of the Naval Postgraduate School Center for Homeland Defense and Security,* Volume II, Issue 2, July 2006.

accountability at all levels of government is critical to motivate change and implement the necessary elements to sustain it.

Review and Reporting Process

The process of learning begins with identifying lessons. In the areas of emergency response, homeland security, and homeland defense, this is often achieved through after-action reports. Such reports could be of immense value to many emergency response agencies at all levels of government, but there is no universally accepted approach to the development or content of such reports. It is not uncommon for multiple reports to emerge from any given incident. These reports differ and often conflict because perspectives and experiences vary dramatically.

Worse than conflicts and possible inaccuracies, concern about attribution and retribution often constrains an open and frank dialogue concerning lessons learned. Meaning is also confused by the lack of common terminology. After-action reports tend to focus on what went wrong with little to no attention on what went right. As a result, there is precious little documentation on good solutions and best practices or "near misses." To achieve this kind of reporting requires an additional analytical step; those preparing the reports need to understand not only what happened, but also why it happened and what corrective action would have improved the circumstances.

Given that such reports could be prepared, the next step is to assure effective distribution. Most dissemination is either tightly controlled or achieved through informal mechanisms. This is particularly true for state and local agencies that may not have access to controlled distributions and often do not have the necessary resources to establish their own repositories, such as the Center for Army Lessons Learned.

Learning and Teaching

There are many theories on organizational learning behaviors, and most agree on four essential phases, such as those described by Kolb in Figure 9.
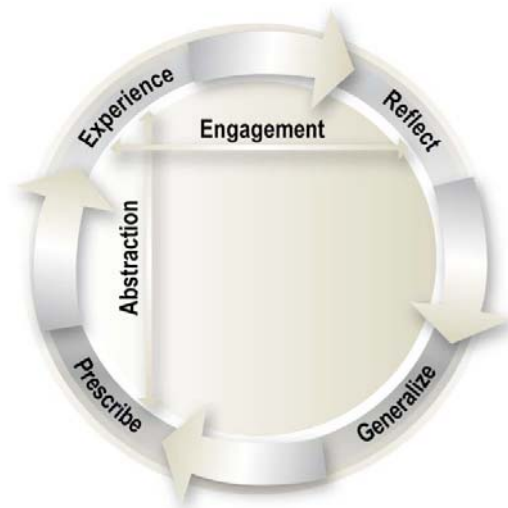
Figure 9. The Learning Cycle

The scope of Kolb's model applies to individuals and organizations who aim to learn from experience, which includes both working and training situations. There are four stages to the cycle: (1) active experience of some specific task and context; (2) reflective review to assess the significant events and relationships of that experience; (3) generalization of the lessons learned from the experience; and (4) prescription of how future activities will be modified given the lessons learned. These stages correspond with two dimensions: abstraction (from the concrete to the conceptual) and engagement (from active participation to reflection). The same dimensions underlie the "learning styles" inventory used to assess the individual approaches to problem solvers. Kolb's model is particularly evident in techniques used to train collaborative decision-making—a key element of an effective unified incident command.

In many cases, particularly in civilian emergency response, failure to learn is due, in part, to the lack of common and accessible systems to identify and disseminate lessons. Learning begins with analysis to identify the causal process that underlies the lesson. One workshop participant put it this way: "We don't study lessons carefully enough and apply them in a serious way. We don't drill down into the details of what changes are really required to address lessons." This dilemma is intensified by the fact that civilian emergency response disciplines lack a common operating doctrine. Agencies often lack a systems view and will tend to consider individual incidents and/or particular lessons in isolation in much the same way as current exercise plans and objectives are developed in various stovepipes.

After action reports often identify lessons and occasionally appropriate remedies, which can easily lead to a false sense of security that we have actually learned the lessons before they are properly included in a training program. Practice is often short-changed. In absence of an effective training program and opportunities to practice, change is not embedded in the system and often the same mistakes occur on the next exercise or incident.

Planning and Executing Exercises

One of the most important elements of the learning cycle is the inclusion of effective exercises to ensure that new behaviors are instilled in the organization. Unfortunately, the current process for design and execution of disaster exercises is woefully inadequate. Creating an exercise scenario that is believable, even for events that have a low probability of occurring but high consequence should an event transpire, is critical to engaging a level of play and experiential learning that will be long lasting. Lack of realism both with respect to scenarios and what can be expected of the response community exist at all levels of government. Often exercises are designed such that true complexities in actual response operations and incident management are never uncovered. Everything works nicely, no one makes mistakes, or if they do, it doesn't really affect the outcome. Lastly, the fear of failure in our current exercise programs is a very real impediment to getting the right people to the table and the design of a realistic exercise environment.

Often participants who have not been engaged in the planning, do not understand either the performance expectations or exercise objectives. As stated above, even in large "national-level" exercises many groups come together with their own exercise objectives, and while these groups play "in parallel," they often do not integrate their exercise objectives into a single unified exercise scenario. The scenarios become unwieldy and result in exercises consisting of, for example, 5000 players and 2000 exercise objectives (Ardent Sentry 2007). As a result, these exercises are grossly expensive and highly scripted and participants get "one shot" at their part and never get a chance to learn from their mistakes and try again.

Resource Constraints

Providing the necessary funding for sustaining corrective action and continued engagement, in a world of many distractions and competing priorities, is a challenge that must be overcome, especially in the large civilian response community critical to both homeland security and homeland defense missions. DOD has many resources that could support preparedness in the homeland

security environment and enhance its effectiveness when the operational environment transitions from supporting civil authorities to homeland defense. Overcoming the fundamental challenges of long-term resource commitment and achieving the organizational discipline required to engage interagency, intergovernmental, and private sector communities will be necessary. The civilian emergency response community is very diverse, often fractured, and consists of a large volunteer force (especially in firefighting). Even when federal grant dollars are being spent, procurement decisions are often made at the local level, which makes adoption of a common operational doctrine, not to mention interoperable or incompatible equipment, a difficult task to achieve.

Crisis Communications

Communications is almost always at the top of the list of recurring issues. It can make or break a successful response. It starts with the basics of compatible equipment and language among response communities. There has been significant improvement across the United States in recent years, especially through the Urban Area Security Initiative and other DHS grant programs and through the efforts of DHS's Office for Interoperability and Compatibility and its SAFECOM program.

However, progress is inconsistent and slow, and seems to be hampered as much by the will to change as by resources. It extends to the public-private linkage, where both the pre-emptive and response actions by private sector owners of critical infrastructure can mitigate significant problems, yet they are more often than not kept in the dark or not allowed access. (This was an acute problem in recovery and restoration post-Katrina.) It also covers crisis communication to the public. Too often it is developed "real time" without benefit of factual vetting and without coordination, such that what is communicated to the public can be misleading or just outright wrong (*e.g.,* anthrax attacks in 2001). **The DSB came to believe that if there were only one thing that DHS and DOD ought to improve among the national team, it should be to develop a common doctrine and an enabling unified command with an interoperable, survivable communication infrastructure.**

RECOMMENDATIONS: BUILDING THE NATIONAL TEAM

As with other recommendations in this study, the recommendations related to building the national team focus on what DOD should do. Secretary of Defense leadership is needed in the interagency to address current deficiencies in national plans and strategies and support for domestic threat assessment. DOD must step up to its preparedness responsibilities in the broad set of communications issues.

To address deficiencies in plans and communications, the Secretary of Defense should:

- Promote the combination of the National Security Council/Homeland Security Council (NSC/HSC) to coordinate and integrate a national strategy and response for global asymmetric engagement.

- Request a National Intelligence Estimate on the scope of the projected threat.

  - Direct the Office of Net Assessment to conduct a capabilities-based net assessment.

- Request that DHS work with DOD to codify the transition from DOD support to DOD lead for a war at home.

- Direct the Deputy Secretary to develop a comprehensive DOD communication system and public affairs strategy for homeland defense preparedness and crisis/consequence management.

- Develop an equipment and concept of operations architecture compliant with the National Incident Management System (NIMS).

- Ensure availability of DOD communication assets compatible with civilian responder community.

- Work with DHS to develop messages, and coordinate and educate those who deliver them, appropriate to the full range of contingencies.

The one game nature expected from future adversaries will demand seamless decision-making, starting with the White House, hence, the recommendation for a joint HSC/NSC strategy. The request for a national intelligence estimate will illuminate the shortfalls in intelligence and therefore allow a better focus of effort. Recognizing that intelligence will always be limited, the estimate should be complemented with a capabilities-based net assessment to enable the DOD community to plan and hedge in a reasonable and balanced manner. National

policy is necessary to better understand when and how a transition from DHS to DOD response leadership would occur. And the critical nature of timely, accurate communications during a crisis requires considerable preparation— something that DOD understands and knows how to do better than any other agency. Thus, DOD may be called upon to lead, given the diversity of capabilities, resources, and generally fractured nature of the civilian emergency response community.

The Secretary of Defense should direct U.S. Northern Command to work with the National Exercise Program at DHS to design and execute more effective exercise programs that address:

- unified management of national capabilities

- communication and information sharing across public and private boundaries

- regional planning and coordination

- interoperable and response capability shortfalls

- transition from DOD support to DOD lead scenarios

In the layered approach to DOD's *Strategy for Homeland Defense and Civil Support*, one of the layers—"Enable"—directly focused on improving domestic capabilities through sharing DOD expertise and technology. The military is recognized for its unsurpassed training, exercise, and doctrinal programs. An integrated National Exercise Program should:

- train and exercise to a common set of goals and objectives

- build from the bottom up—including all relevant players

  - maximize value of involvement: make it worthwhile

  - exercise what is important at the strategic and policy level

  - exercise what is important in sufficient depth

  - provide unified management of national capabilities

- follow through with effective corrective actions both in policy and practice

- structure to identify interoperable and response capability shortfalls

- address transition from homeland security to homeland defense operations (transition from DOD support to DOD lead scenarios)

- aggressive red teaming to identify interoperable and response capability shortfalls

As a part of this recommendation, DOD could enable a National Emergency Response Lessons Learned Institute. DOD has capabilities and expertise that can enable analysis and dissemination of lessons learned. The national civilian emergency response infrastructure lacks sufficient discipline and consistency in critical capabilities necessary to manage large-scale or simultaneous incidents. One of the challenges in achieving such a capability is the promulgation of an unbiased, standardized, and readily accessible reporting system. Leveraging capabilities such as the Center for Army Lessons Learned, U.S. Training and Doctrine Command, and the Lessons Learned Information Sharing web site, this institute could be at the foundation of a new national doctrinal institute. Engaging such an activity will also enable DOD to better understand what resources it may be required to provide in defense of asymmetric attacks on the homeland. Furthermore, these lessons learned should drive continuous improvement of the national training and exercise programs.

To support regional planning and coordination, FEMA and DLA, as an aspect of their memorandum of understanding and in collaboration with state homeland SCCs, should jointly plan for and deploy pre-positioned materials in support of emergency response operations. These cached materials should be tailored to regional needs and could be coordinated with local private sector suppliers. These caches should include emergency communications equipment, specialized protective equipment, and medical supplies that may be needed for WMD events; they should also take into consideration the current capabilities and threat environment (including natural disasters) of the region they are intended to support. For example, regions subject to flooding events, will likely expect federal government support for water rescue.

Other potential ideas could include FEMA working with other federal agencies, including DOD, to provide for more flexible and streamlined procurement and legal guidelines to obtain needed resources in real time, and standardizing credentialing capability for access of critical personnel to disaster areas. Delegation of authority in acquisition matters should be at the lowest level possible. DOD might also advocate for a one-stop shopping mechanism like GSA to enable and encourage state and local governments to work together for the purpose of making "bulk" purchases. This kind of arrangement will likely provide a powerful incentive for state and local regions to maintain interoperable and compatible equipment and concepts of operations.

ASD (HD&ASA) should take the initiative to help establish a strategically-managed, interagency homeland defense/homeland security leader development program with the following attributes:

- graduate-level, senior service DHS-sponsored "war" college developed in conjunction with the National Defense University

- an Executive Exchange Program modeled on the President's Executive Exchange Program

- recognition as credit equivalent to senior service schools and for promotion to flag officer rank and the senior executive service in DOD

- training expanded to state and local levels, and the private sector

---

One of the most significant conclusions of this study is the realization that DOD's success in prosecuting future wars against capable adversaries will likely depend on the success of other agencies of the government—at all levels—and on the private sector to succeed at their missions in the face of attacks on the homeland. As such, DOD must take much more seriously its own strategy statements that "failure (in the homeland) is not an option."

Success will require the department to step up to a much more active role in the interagency arena, to engage the local and regional communities on which they depend at home more consistently and deeply, and to carefully examine its own mission critical needs and ensure their availability in times of attack. Lots of homework and relationship-building outside the historic mainstream of DOD activities will be required. As with all new things, the ability to attract good people to this critical work must come with the incentives for career progression and recognition.

While many of these activities are difficult to contemplate in the current and near future environment of Operation Iraqi Freedom, Operation Enduring Freedom, and the major recapitalization bills these campaigns will demand, a number of these activities require relatively inexpensive efforts in planning, training, and exercising. **The key ingredient will be leadership commitment to chart and sustain the path.**

Appendix A. Relevant Legislation and Directives for DOD in Homeland Security and Defense

There are numerous legislative and executive directives defining DOD's roles and responsibilities with regard to homeland defense and support to civil authorities.

Article II of Constitution

Article II, Section 2 of the Constitution specifies that "the President shall be commander in chief of the Army and Navy of the United States, and of the militia of the several states, when called into the actual service of the United States." In this role as Commander in Chief, he is authorized to utilize both the active duty military as well as the National Guard (militia) in support of the national defense.

Stafford Act

This act provides statutory authority for employing the U.S. armed forces for domestic disaster relief. Permitted operations include debris removal and road clearances; search and rescue; emergency medical care and shelter; provision of food, water, and other essential needs; dissemination of public information and assistance regarding health and safety measures; and the provision of technical advice to state and local governments on disaster management and control. The Stafford Act does not authorize the use of Federal military forces to maintain law and order.

DOD doctrine (DOD 3025) allows commanders to provide resources and assistance to civil authorities without, or prior to, declaration under the Stafford Act when a disaster overwhelms the capabilities of local authorities and necessitates immediate action "to prevent human suffering, save lives, or mitigate great property damage."

Posse Comitatus Act

The Constitution does not expressly bar the use of military forces in civilian situations or in matters of law enforcement, but the United States has traditionally refrained from employing troops to enforce the law except in cases of necessity. Congress has provided for a number of statutory exceptions to the Posse Comitatus Act explicitly by vesting law enforcement authority directly in a military branch, or indirectly by authorizing the President or another government official to call for assistance in enforcing certain laws.

Homeland Security Directive #5. Management of Domestic Incidents

The heads of federal departments and agencies shall adopt the National Incident Management System (NIMS) within their departments and agencies, and shall provide support and assistance to the Secretary of Homeland Security in the development and maintenance of the NIMS. All Federal departments and agencies will use the NIMS in their domestic incident management and emergency prevention, preparedness, response, recovery, and mitigation activities, as well as those actions taken in support of state or local entities. The heads of Federal departments and agencies shall participate in the National Response Plan (NRP), shall assist and support the Secretary of Homeland Security in the development and maintenance of the NRP, and shall participate in and use domestic incident reporting systems and protocols established by the Secretary.

The Secretary of Defense shall provide military support to civil authorities for domestic incidents as directed by the President or when consistent with military readiness and appropriate under the circumstances and the law. The Secretary of Defense shall retain command of military forces providing civil support. The Secretary of Defense and the Secretary of Homeland Security shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments.

Homeland Security Directive #8. National Preparedness

The Department of Defense will provide to the Secretary of Homeland Security information describing the organizations and functions within the Department of Defense that may be utilized to provide support to civil authorities during a domestic crisis.

Homeland Security Presidential Directive #7. Critical Infrastructure, Identification, Prioritization & Protection; Department of Defense Directive 3020.40, August 2005

DOD is the sector-specific agency for the Defense Industrial Base (DIB). The term "sector-specific agency" means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resource category.

Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with state and local governments and the private sector to accomplish this objective.

Federal departments and agencies will ensure that homeland security programs do not diminish the overall economic security of the United States.

Federal departments and agencies will appropriately protect information associated with carrying out this directive, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

Federal departments and agencies shall implement this directive in a manner consistent with applicable provisions of law, including those protecting the rights of United States persons.

NSPD 51, HSPD 20, National Continuity Policy

The Secretary of Defense, in coordination with the Secretary of Homeland Security, shall provide secure, integrated, continuity of government communications to the President, the Vice President, and, at a minimum, Category I executive departments and agencies.

Enforcement of the Laws to Restore Public Order (aka "The Insurrection Act")

Congress has delegated authority to the President to call for the military during an insurrection or civil disturbance (10 U.S.C. 331-335). The Insurrection Act has been used to send the armed forces to quell civil disturbances a number of times during U.S. history, most recently during the 1992 Los Angeles riots.

The 109th Congress included in the Defense authorization bill for FY2007 a provision that is intended to explicitly cover instances of "domestic violence" where public order is disrupted due to a national disaster, epidemic or other serious public health emergency, terrorist attack, or incident. This revision of 10 U.S.C. 333 authorizes the President to employ Federal troops to "restore public order and enforce the laws of the United States without a request from the governor or legislature of the state involved, when he/she determines that local authorities are unable to maintain public order."

Military Support for Law Enforcement Agencies

Congress has also authorized the armed forces to share information and equipment with civilian law enforcement agencies, although it has prohibited the use of armed forces personnel to make arrests or conduct search and seizures.

DODD 5525.5 Cooperation with Civilian Law Enforcement Officials

This directive defines DOD's responsibilities to cooperate with civilian law enforcement officials consistent with the needs of national security and military preparedness. This directive applies to OSD, the military departments, the Organization of the Joint Chiefs of Staff (OJCS), the unified and specified commands, and the defense agencies (hereafter referred to collectively as DOD components). The term "military service," as used herein, refers to the Army, Navy, Air Force, and Marine Corps.

Responsibilities enumerated in this directive include, but are not limited to:

- Coordinate with civilian law enforcement agencies on long-range policies to further DOD cooperation with civilian law enforcement officials.

- Provide information to civilian agencies and the National Narcotics Border Interdiction System (NNBIS) to facilitate access to DOD resources.

- Coordinate with the Department of Justice, the Department of Transportation (U.S. Coast Guard), and the Department of the Treasury (U.S. Customs Service) and represent DOD on interagency organizations regarding matters involving the interdiction of the flow of illegal drugs into the United States.

- Review training and operational programs to determine how and where assistance can best be provided to civilian law enforcement officials.

- Implement procedures for prompt transfer of relevant information to law enforcement agencies.

- Implement procedures for establishing local contact points in subordinate commands for purposes of coordination with Federal, state, and local civilian law enforcement officials.

DODD 3025 Military Assistance for Civil Disturbances

This directive provides for DOD officials to take emergency action without prior authorization in cases where: "sudden and unexpected civil disturbances (including civil disturbances incident to earthquake, fire, flood, or other such calamity endangering lives) occur, if duly constituted local authorities are unable to control the situation and circumstances preclude obtaining prior authorization by the President."

Appendix B. Selected Excerpts from the "Strategy for Homeland Defense and Civil Support," June 2005

The Department of Defense must change its conceptual approach to homeland defense. The Department can no longer think in terms of the "home" game and the "away" game. There is only one game. The Strategy for Homeland Defense and Civil Support is a significant step toward this strategic transformation. Defending the U.S. homeland—our people, property, and freedom—is our most fundamental duty. Failure is not an option.

Key Definitions

Homeland security, as defined in the National Strategy for Homeland Security, is "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." The Department of Homeland Security is the lead Federal agency for homeland security. In addition, its responsibilities extend beyond terrorism to preventing, preparing for, responding to, and recovering from a wide range of major domestic disasters and other emergencies. It is the primary mission of the Department of Homeland Security to prevent terrorist attacks within the United States. The Attorney General leads our nation's law enforcement effort to detect, prevent, and investigate terrorist activity within the United States. Accordingly, the Department of Defense does not have the assigned responsibility to stop terrorists from coming across our borders, to stop terrorists from coming through U.S. ports, or to stop terrorists from hijacking aircraft inside or outside the United States (these responsibilities belong to the Department of Homeland Security). Nor does DOD have the authority to seek out and arrest terrorists in the United States (these responsibilities belong to the Department of Justice).

Homeland defense is the protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and

aggression, or other threats as directed by the President.[28] The Department of Defense is responsible for homeland defense.

DOD Activities, Objectives, and Core Capabilities	
Lead	**Achieve Maximum Awareness of Threats** ▪ Maintain agile and capable defense intelligence architecture ▪ Analyze and understand potential threats ▪ Detect, identify, and track emerging threats in all operational domains ▪ Ensure shared situational awareness within DOD and with domestic and foreign partners **Deter, Intercept, and Defeat Threats at a Safe Distance** ▪ Deter adversaries from attacking the U.S. homeland ▪ Intercept and defeat national security threats in the maritime and air approaches and within U.S. territory **Achieve Mission Assurance** ▪ Ensure force protection, to include DOD installations, especially against the threat of CBRNE attacks ▪ Prepare and protect defense critical infrastructure ▪ Ensure preparedness of the Defense Industrial Base ▪ Prepare to protect designated national critical infrastructure ▪ Ensure DOD crisis management and continuity preparedness
Support	**Support Consequence Management for CBRNE Mass Casualty Attacks** ▪ Manage consequences of CBRNE mass casualty attacks
Enable	**Improve National and International Capabilities for Homeland Defense and Homeland Security** ▪ Effective interagency planning and interoperability ▪ Improved Federal, state, and local partnership capacity and effective domestic relationships ▪ Improved international partnership capacity and effective defense-to-defense relationships

Defense support of civil authorities, often referred to as civil support, is DOD support, including Federal military forces, the Department's career civilian and contractor personnel, and DOD agency and component assets, for domestic emergencies and for designated law enforcement and other activities. The

---

28. Homeland defense includes missions such as domestic air defense. The Department recognizes that threats planned or inspired by "external" actors may materialize internally. The reference to "external threats" does not limit where or how attacks could be planned and executed. The Department is prepared to conduct homeland defense missions whenever the President, exercising his constitutional authority as Commander in Chief, authorizes military actions.

Department of Defense provides defense support of civil authorities when directed to do so by the President or Secretary of Defense.

Defense Critical Infrastructure

Related to its force protection responsibilities for DOD facilities, the Department of Defense has the responsibility to assure it has access to defense-critical infrastructure. This is defined as DOD and non-DOD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide. When these infrastructures are located on Department of Defense installations, their protection is the responsibility of the installation commander or facility manager. In some instances, however, critical defense assets are located at public or private sites beyond the direct control of DOD. In either case, the protection of designated defense critical infrastructure must be assured on a priority basis.

In some scenarios, assurance of non-DOD infrastructures might involve protection activities, in close coordination with other Federal, state, local, tribal, or private sector partners. This could include elements of the Defense Industrial Base, which is a worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapons systems, subsystems, components, or parts to meet military requirements. These defense-related products and services are essential to mobilize, deploy, and sustain military operations. Moreover, defense critical infrastructure could also include selected civil and commercial infrastructures that provide the power, communications, transportation, and other utilities that military forces and DOD support organizations rely on to meet their operational needs.

In addition, the President or the Secretary of Defense might direct U.S. military forces to protect non-DOD assets of national significance that are so vital to the nation that their incapacitation could have a debilitating effect on the security of the United States.

Core Capability: Preparedness and protection of defense critical infrastructure

Because resources are constrained, it is not possible to provide uniform protection of all defense-critical infrastructure. The Department must prioritize the protection of assets based on their criticality to executing the National Defense Strategy and seek to minimize the vulnerability of critical assets in

accordance with an integrated risk management approach. To this end, the Department will devise a strategy to:

- identify infrastructure critical to the accomplishment of DOD missions, based on a mission area analysis

- assess the potential effect of a loss or degradation of critical infrastructure on DOD operations to determine specific vulnerabilities, especially from terrorist attack

- manage the risk of loss, degradation, or disruption of critical assets through remediation or mitigation efforts, such as changes in tactics, techniques, and procedures; minimizing single points of service; and creating appropriate redundancies, where feasible

- protect infrastructure at the direction of the President or the Secretary of Defense where the nature of the threat exceeds the capabilities of an asset owner and civilian law enforcement is insufficient

- enable real-time incident management operations by integrating current threat data and relevant critical infrastructure requirements

The military departments, defense agencies, and other DOD components are now implementing the Protective Risk Management Strategy through modifications to their programs and budgets.

Core Capability: Preparedness of the Defense Industrial Base

The *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (2003) notes that, without the important contributions of the private sector, DOD cannot effectively execute core defense missions. Private industry manufactures and provides the majority of the equipment, materials, services, and weapons for the U.S. armed forces. The President recently designated DOD as the sector-specific agency for the DIB. In this role, DOD is responsible for national infrastructure protection activities for critical defense industries, as set forth in Homeland Security Presidential Directive-7.

To assure that mission-critical supplies and services are available, DOD contracts are being modified to ensure that protective measures are in place at key facilities and that DOD can assess the security of the DIB. In addition, the DLA and other DOD contracting activities are revising the contract process to ensure that civilian defense contractors are able to operate for the duration of a national emergency. Defense contractors must be able to maintain adequate

response times, ensure supply and labor availability, and provide direct logistic support in times of crisis. DOD program managers will be held accountable for ensuring the protection of supporting infrastructure, including key suppliers. DOD base and installation commanders, and those who contract for non-DOD infrastructure services and assets, will monitor assurance activities through compliance with contract language that clearly identifies reliable service availability, priority of restoration, and asset protection.

Core Capability: Preparedness to Protect Designated National Critical Infrastructure

The Department has historically focused on preventing unauthorized personnel from gaining access to DOD installations and protecting those installations from traditional military attacks. In the post-September 11, 2001 era, DOD is expanding the traditional concept of critical asset protection to include protection from acts of trans-national terrorism. Countering terrorist reconnaissance activity is central to the successful defense of critical infrastructure.

As outlined in the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (2003), DOD bears responsibility for protecting its own assets, infrastructure, and personnel. At the Department's request, domestic law enforcement may protect DOD facilities. For non-DOD infrastructure, including private and public assets that are critical to the execution of the National Defense Strategy, DOD's protection role is more limited. The initial responsibility for protection of non-DOD infrastructure rests with asset owners. Civilian law enforcement authorities augment and reinforce the efforts of asset owners, creating a second tier of protection.

Should protection requirements exceed the capabilities of asset owners and civilian law enforcement, state authorities provide an additional layer of defense. In addition to a governor's authority to employ National Guard forces in a state active duty status, recent changes to Title 32 of the U.S. Code may provide an additional, expeditious means to use National Guard forces under the control of the governor, with the approval of the Secretary of Defense, using Federal funding to perform homeland defense activities. To achieve critical infrastructure protection in the most serious situations, the Department of Defense maintains trained and ready combat forces for homeland defense missions.

Terms of Reference

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

FEB 0 2 2007

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board 2007 Summer Study on
Challenges to Military Operations in Support of National Interests

The United States capability in conventional warfare is unmatched by any other
state for now and the immediate future. The success in Operation DESERT STORM
followed by even greater success a decade later in the initial phases of Operations
ENDURING FREEDOM and IRAQI FREEDOM demonstrate an overwhelming ability
to continually grow conventional capability and outmatch opponents.

However, the same overmatch does not exist across the conflict spectrum and is
unlikely to exist in the conventional space forever. For example, the Soviet Union
threatened the existence of the United States along nuclear and ideological lines and
seriously threatened U.S. interests with conventional arms. Russia retained sufficient
nuclear capability to threaten U.S. existence, but that threat is no longer coupled with the
same ideological and conventional threat. The growing proliferation of nuclear weapons
may challenge U.S. conventional forces in some regions or thwart U.S. interests. Finally,
we have to expect WMD proliferation, e.g., biological, in general. Will WMD
proliferation transform unexpected adversaries into challengers sufficiently capable to
threaten the existence of the U.S. or at least thwart U.S. interests?

Asia's economic growth may enable several states to compete along conventional
lines if they so choose. An important part of Asia's growth is driven by globalization of
technology and manufacturing prowess that discounts historical DoD advantages in these
areas. The worst-case scenario results in a technologically inferior U.S. vis a vis an
opponent. There are also indications that opponents may not choose to confront the U.S.
head to head with conventional forces: asymmetric warfare is the province of states as
well as of terrorists and insurgents, e.g., the recent conflict in Lebanon demonstrated gaps
in conventional vs. asymmetric forces. Finally, the U.S. may choose capabilities and
resultant force structures that provide opponents unrecognized vulnerabilities for their
exploitation. Although these types of challenges may not threaten the existence of the
United States, they may prove sufficiently challenging to justify serious consideration and
planning to mitigate the effect on U.S. interests.

In addition, the U.S. Armed Forces will likely face: continuing and long lasting stabilization and reconstruction operations; an increasing number of humanitarian missions driven by epidemics and AIDS, climate change, famine and water shortages, religious and tribal strife; and more instances of domestic catastrophe support, like Katrina. These responsibilities will inevitably detract from capabilities for deterring and defeating competitors who could challenge military operations.

Further, nowadays competition is intrinsically global. On one hand, we need the capability for very swift deployment anywhere on Earth to counteract "blitzkreig" tactics, capability for decisive deployment of massive force to counteract a peer, and capability for sustained deployment for operations that might take years. On the other hand, attacks on our homeland must be not only anticipated but expected; and the very same resources needed for foreign expeditions, e.g., the Reserve, might be needed for protection at home.

As the world evolves in the 21st century, the Department of Defense must anticipate future stressing wars. What would a challenger look like and how would it successfully challenge military operations? Will states attempt to achieve peer status in a conventional force-on-force conflict, or will some other strategy prove successful? If not, what will they attempt to enable them to maintain their interests? Under what circumstances might a coalition or transnational group successfully challenge military operations? What are the metrics for success in this environment? Are there innovative technologies, systems or operational concepts that can be applied to this subject before it becomes a national crisis?
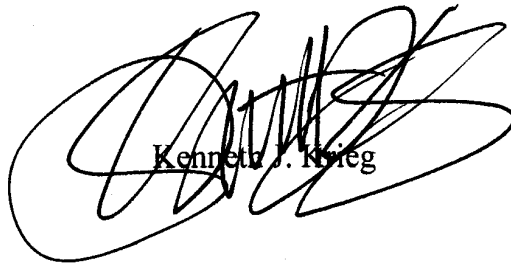
Specifically the Summer Study should:

(1) Review previous and ongoing studies regarding stressing wars;

(2) Identify defining parameters for challenges to military operations (e.g., physical size, population, technological prowess, and denial and deception);

(3) Assess capability gaps;

(4) Identify possible solutions. At a minimum, the Summer Study should assess technological, operational, and policy oriented solutions.

The study will be co-sponsored by the Under Secretary of Defense for Acquisition and Technology and the Under Secretary of Defense for Policy. Dr. Craig Fields and Mr. Rich Haver will serve as Chairmen of the Task Force. Mr. Todd Lowrey, OUSD(P) will

serve as Executive Secretary; and Commander Cliff Phillips, USN, will serve as the DSB Secretariat Representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of title 18, U.S. Code, section 208, nor will it cause any member to be placed in the position of acting as a procurement official.

Kenneth J. Krieg

Panel Participants

DEFENDING AGAINST DOMESTIC CATASTROPHE IN WAR TIME PANEL

Chairs	
Dr. Bill Howard	Private Consultant
Mr. Robert Nesbit	MITRE
Members	
Mr. Jerry Buckwalter	Northrop Grumman
Mr. Evan Wolff	Hunton & Williams LLP
Government Advisors	
COL Joseph Bassani	U.S. Northern Command
Mr. Jim Caverly	Director, Partnership & Outreach Division
Mr. John Humpton	HQDA ODCS G-3/5/7

ENSURING DEPLOYMENT AND SUPPLY PANEL

Chairs	
Dr. Miriam John	Private Consultant
Dr. Ronald Kerber	Private Consultant
Members	
Dr. John Cummings	Sandia National Laboratories
Maj Gen John Fenimore V, USAF (Ret)	J.H. Fenimore & Assoc, LLC
LtGen Rick Kelly USMC (Ret.)	LMI
Dr. Duane Lindner	Sandia National Laboratories
VADM Keith Lippert, USN (Ret.)	Accenture National Security Service, LLC
Ms. Nancy Suski	Lawrence Livermore National Laboratory
LTG David Teal USAF (Ret.)	Accenture National Security Services
Ms. Nancy Wilson	Association of American RR

Government Advisors	
COL Joe Bassani, USA	NORTHCOM
Mr. Bill Bryan	OSD(P)/ASD/HD
Mr. James Caverly	DHS
Mr. G. Gurvais Grigg	FBI
Mr. Lacey Hughes	HQDA DCS G-4
Mr. John Humpton	Department of the Army, G3

DSB REPRESENTATIVE

Maj Charles Lominac, USAF	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics

STAFF

Julie Evans	Strategic Analysis, Inc.
Brian Keller	Private Consultant
Carla King	Strategic Analysis, Inc.
Kelly Frere	Strategic Analysis, Inc.

Presentations to the Panels

Ensuring Deployment and Supply
Defending Against Domestic Catastrophe in War Time
Joint Panel Meetings

Name	Topic

FEBRUARY 9, 2007

Name	Topic
Mr. Don Latham	2003 DSB SS on DOD Roles & Missions in Homeland Security
Mr. Bob Stephan, DHS, Assistant Secretary for Infrastructure Protection	DHS Critical Infrastructure Approach
Dr. Miriam John/Dr. Ronald Kerber	Report of the DSB Task Force on Critical Homeland Infrastructure Protection

MARCH 20, 2007

Name	Topic
Mr. William Bryan, DCIP OASD (HD&ASA)	Update on DOD Defense Critical Infrastructure Program
Mr. Bob Nesbit, MITRE	DSB 2005 Summer Study on WMD
Maj Gen Tim Lowenberg, TAG for the State of Washington	National Guard Discussion
Ms. Nancy Wilson, American Association of Railroads	Partnership for Critical Infrastructure Security
GEN (R) Reimer, DFI International	Katrina Lessons Learned

APRIL 24, 2007

Name	Topic
Mr. Merrick Krause, DHS	National Infrastructure Simulation and Analysis Center and Critical Infrastructure Protection-Decision Support System
Maj Gen Fenimore, Private Consultant and Dr. Nancy Suski, Sandia National Laboratory	Citizen Preparedness
COL Joseph Bassani, USA, USNORTHCOM	NORTHCOM
Mr. Jim Kish, DHS	National Exercise Program
AD Dr. Vahid Majidi, FBI	FBI WMD Program

MAY 24, 2007

Gen (R) Mike Carns, USAF, Private Consultant	DSB Energy Strategy Task Force
MG (R) Barry Bates, NDIA	Panel of Corporate Security Execs from Defense Industrial Base
Ms. Alane Andreozzi, DTRA	A Kele Exercise
Mr. Carl Brown, DTRA	BioNet
Colonel Joseph Bassani, USNORTHCOM	NORTHCOM

JUNE 11, 2007

LTG C. V.Christianson, J-4 COL Ed Hatch, JFCOM Mr. Alan Banghart, DLA	OCONUS Deployment & Sustainment Panel
Mr. Ronald Krisak, IDA	Noble Resolve
Healthcare: Mr. Chris Lake, BLU-MED Response Energy: Mr. Stan Johnson, Manager Situation Awareness & Infrastructure Security, North American Electric Reliability Corporation IT: Mr. Guy Copeland, CSC; Mr. Michael Aisenberg (EWA-IIT); Mr. Paul Nicholas (Microsoft); Liesyl Franz (ITAA). Emergency Services: Ms. Ann Davison, Int'l Assoc of Fire Chiefs & Mr. Tom Rhatigan, National Sheriff's Assoc. Homeland Security Program Manager	Sector Coordinating Council Representatives: PCIS Panel: Energy, IT, Commo, Healthcare, Emergency Services

JUNE 12, 2007

Dr. Til Jolly, Office of Health Affairs, DHS	Pandemics: Community Mitigation and Implications to Planners
Mr. Bill Bryan, Director, DCIP OASD (HD&ASA)	Update on DOD 41 Critical Infrastructure
Mr. Philip Sakowitz, Executive Director, US Army Installation Management Command (Accompanied by Mr. Clay Davis, Mr. Don Stout, Mr. Gordon Rogers)	Installation Preparedness
Oil & Natural Gas: Mr. Gary Forman, NiSource Inc. Highways & Motor Carriers: Martin Rojas, American Trucking Assoc. Railroads: Nancy Wilson, Assoc of American Railroads Transit: Mr. Tom Yedinak, American Public Transportation Association	PCIS Panel: Transportation Sectors

JUNE 19, 2007

LTG (R) Peter Kind, USA	Y2K Information Coordination Center
Mr. Brandon Wales, DHS	Tier 1 and 2 CI/KR Update
BG Peter Aylward, J34 Antiterrorism and Homeland Defense	WMD Insights
Mr. Jim Schwartz, Arlington County Fire Chief Mr. Marko Bourne, FEMA Dr. Helen Miller, OR-1 Disaster Medical Assistance Team (National Disaster Medical System) Mr. Matt Bettenhausen,California Office of HLS	Panel of State and Local Authorities

JULY 17, 2007

Mr. Allan Banghart, DLA Colonel Dennis D'Angelo, TRANSCOM Mr. Alan Estevez, OSD(LM&R)	Logistics Panel: Ensuring Deployment and Supply
LtCol Stephen Hall, USAF, Joint Task Force Civil Support (JTF-CS)	JTF-Civil Support

Glossary

ASD (HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
CBRNE	chemical, biological, radiological, nuclear, and high explosive
CI/KR	critical infrastructure/key resources
CIPAC	Critical Infrastructure Partnership Advisory Council
CONUS	continental United States
DCA	defense critical asset
DCIP	Defense Critical Infrastructure Program
DHS	Department of Homeland Security
DLA	Defense Logistics Agency
DOD	Department of Defense
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
EMAC	Emergency Management Assistance Compact
EMT	emergency medical technician
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GCC	Government Coordinating Council
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
IED	improvised explosive device
ISAC	Information Sharing and Analysis Centers
JFCOM	U.S. Joint Forces Command
JIATF	Joint Interagency Task Force
NCO	noncommissioned officer
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NSC	National Security Council
NSPD	National Security Presidential Directive
ODUSD (LM&R)	Office of the Deputy Under Secretary of Defense for Logistics and Materiel Readiness

SCC	Sector Coordinating Council
SSA	sector-specific agency
SSP	sector-specific plans
TCA	task critical asset
TRANSCOM	U.S. Transportation Command
TSA	Transportation Security Administration
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology & Logistics
WMD	weapons of mass destruction
Y2K	Year 2000