

TOP PRIORITIES FOR MILITARY OPERATIONS TO COMBAT TERRORISM

*A Report of The Heritage Foundation Working Group on Military Operations*¹

Larry M. Wortzel, Working Group Rapporteur

Since the publication of the National Defense Panel (NDP) report in 1997, there have been clear warnings to the people and policymakers of the United States that the nation's homeland must be protected from terrorist attacks. Other studies also have made it clear that the U.S. armed forces, working with the Intelligence Community and Federal, State, and Local officials, must be prepared not only to identify impending terrorist attacks, but also to preempt or respond to them rapidly.²

First and foremost, the U.S. armed forces must defend the homeland and respond to catastrophic attacks, which can be the result of terrorism or counterstrikes on U.S. civilian targets by enemies, such as Iraq or North Korea, in time of war. Regardless of the origin of an attack, the armed forces must be prepared to protect the homeland and respond immediately to a catastrophe.

1. The members of the Working Group on Military Operations Against Terrorism include David Davis, Chief of Staff, Office of Senator Kay Bailey Hutchison; Colonel James P. Gibbons, USA (Ret.), former Commander, U.S. Army Land Information Warfare Activity; Major General David L. Grange, USA (Ret.), former Commander, 1st Infantry Division; Lieutenant General Patrick M. Hughes, USA (Ret.), former Director, Defense Intelligence Agency, and former Commanding General, U.S. Army Intelligence Agency; Dr. Fred Iklé, Distinguished Scholar, Center for Strategic and International Studies; General Carl E. Mundy, Jr., USMC (Ret.), former Commandant, United States Marine Corps, and former member, Joint Chiefs of Staff; General John H. Tilelli, Jr., USA (Ret.), former Commander, U.S. Army Forces Command, Vice Chief of Staff, United States Army, and Commander in Chief, U.S. Forces Korea; and General Charles E. Wilhelm, USMC (Ret.), former Commander in Chief, U.S. Southern Command. The following individuals also contributed to this report in an advisory capacity: Todd Gaziano, Director, Center for Legal and Judicial Studies, The Heritage Foundation; General Dennis J. Reimer, USA (Ret.), former Chief of Staff, United States Army; and The Honorable James Schlesinger, Special Adviser, Lehman Brothers, Inc., Washington, D.C., former Secretary of Defense.
2. For a summary of recommendations from prior commissions and studies that have not been implemented, see the table at the end of this chapter. The status of post-September 11 legislative efforts may be found in the Appendix.

In fighting terrorism, the best defense is a good offense. U.S. forces must be configured to combat the threat, and also to maintain the capabilities to fight and win conflicts against conventional armed forces. To date, the involvement of U.S. forces in military operations in Afghanistan has been conducted under an extraordinary array of circumstances that in all probability will not be a blueprint for all conflicts in the future.

In any restructuring of forces to meet a rising threat, care must be taken to ensure a continued balance between unconventional and conventional force capabilities. A number of studies have suggested how to accomplish these objectives, but their recommendations are still being debated, and many have not been systematically implemented.

This report by The Heritage Foundation Working Group on Military Operations builds on those recommendations by identifying key priorities for improving military operations and taking firm positions on how best to defend the homeland against terrorism. Specifically:

- **Priority #1: Free the National Guard and Reserves for homeland security and boost port security quickly.** The present configuration of conventional forces, special operations forces, and strategic forces will function well for military operations in support of homeland defense and for conducting a range of operations overseas, including deterrence and fighting terrorism at its roots. The National Guard and Reserves should not be the only military personnel involved in security; active force units must also be involved. But homeland security will require enhancing the capabilities of National Guard and Reserve units to respond to terrorist events, as well as freeing some units from having to add personnel for combat support and combat service support for the active forces. It also will require reinstating a port security program.
- **Priority #2: Protect U.S. borders, coasts, and critical national infrastructure with air defense and missile defense.** The threat of attack from the air—by aircraft, cruise missiles, and ballistic missiles—requires the United States to establish a robust air and cruise missile defense system now and to begin testing ballistic missile defenses on land and at sea at full design capability.
- **Priority #3: Enhance rear-area military operations to protect the homeland and prepare for terrorist attacks.** The U.S. military can assist Local, State, and Federal authorities in counterterrorism efforts by identifying and assessing security levels at critical infrastructure nodes; providing protection for critical infrastructure; providing redundant communications, command, and control systems; and procuring and maintaining equipment that would assist in responses to terrorist attacks. While many commissions have considered this approach, the Training and Doctrine Command of the U.S. Army has pulled the Army out of the mission. The Secretary of Defense should work with the

Director of the Office of Homeland Security (OHS) to have Reserve and National Guard units involved once more in homeland defense education and training and to develop active cooperation and education programs for each state.

- **Priority #4: Provide intelligence support for military operations.** Effective offensive and defense operations against terrorism will require a distributed intelligence and information architecture with intelligence fusion centers that link to a network that allows any Federal agency with access (such as the U.S. Army, Federal Aviation Administration, or Central Intelligence Agency) to query a large shared database. No such database exists today, and information remains compartmentalized in different agency “stovepipes.” To win the war against terrorism, the U.S. Department of Defense (DOD) must have access to cross-referenced strategic and critical databases housed in various Federal agencies. This will require that fusion centers at the Federal, State, and Local levels, where necessary, are manned by personnel cleared for an intelligence compartment related to the war on terrorism and homeland defense.
- **Priority #5: Ensure clear command and control of overseas anti-terrorism operations.** The Department of Defense should resist calls to establish a new command to handle overseas operations against terrorism. Regardless of whether military operations are of an offensive or defensive nature, the geographic Unified Command (such as PACOM, or CENTCOM, which is directing the war in Afghanistan) must be the command-and-control headquarters for overseas military operations. In military parlance, this means that the geographic Unified Command will be the supported command and the war fighter. The United States Special Operations Command (SOCOM) should be a specified supporting command for managing counterterrorism operations and the primary force provider. The Secretary of Defense, in the Defense Guidance, must ensure that SOCOM has the requisite authority and priorities to resource the fight and to develop new systems to support the war against terrorism.

PRIORITY #1: FREE THE NATIONAL GUARD AND RESERVES FOR HOMELAND SECURITY AND BOOST PORT SECURITY.

A debate is raging among defense analysts who argue that tomorrow’s warfare will involve battles similar to today’s war on terrorism, with enemies that mount non-traditional attacks on Americans, perhaps with chemical, biological, radiologic, or nuclear (CBRN) weapons. Others argue that it primarily will involve small,

localized wars of short duration in regions that are vital to American interests. At the same time, the possibility of a major conventional war still exists.

The Working Group on Military Operations believes that the Quadrennial Defense Review (QDR) submitted to the President by Secretary of Defense Donald Rumsfeld in October correctly balances the need for counterterrorist military operations, conventional war, and operations for responding to other forms of “low-intensity conflict.” This is the right approach. The United States should continue its capabilities-based strategy to fight and win wars *and* to deter aggression and terrorism against its people, homeland, and interests.

This strategy must include a robust capability to conduct counterterrorist military operations; to protect U.S. interests should a general war break out on the Korean Peninsula, in the Middle East, or in Southwest Asia; and to respond appropriately in the Pacific region to forces of countries that employ area-denial and anti-access strategies, such as China. Such a strategy will require the Administration to take the following steps:

Key Step #1. The Secretary of Defense should add active duty personnel to current active force levels to put more combat support and combat service support elements into the active military. The Secretary of Defense should ensure that the active armed forces include additional combat and combat service support elements, particularly in the Army, so that the necessary National Guard and Reserve units are able to assume greater responsibility for homeland security. Many combat support and service support units—such as in communications, logistical support, intelligence, medical support, and food service—were moved into the National Guard and Reserves in the late 1980s and 1990s to reduce the size of the active armed forces.

Today, the U.S. Army and U.S. Air Force cannot go to war without activating large numbers of Reserve and National Guard organizations. However, these same Reserve and Guard components are the primary units to support homeland security requirements. They must be freed from their support of the active forces to defend the homeland against terrorism. Combat support and combat service support personnel that are put back in the active forces must be additions to the total active force strength.

Key Step #2. The Secretary of Defense should ensure that the National Guard has standing emergency plans to train for and work with Local authorities on homeland defense and consequence management. The National Guard Bureau, the National Guard State Area Commands (STARCs), and the State Adjutants General must be involved in all State emergency management programs. The STARCs and Continental U.S. Armies (CONUSAs) should be linked to provide

rapid communications and coordination. The STARCs are likely to be the first military responders following civilian requests for assistance in a major crisis or incident.

Each State must have a viable emergency plan, an operations center, and dedicated, redundant command-and-control means of communications in the event of an emergency. The relevant National Guard Bureau regulation, which was written in 1982, should be updated to reflect the new security environment. In addition, many State Adjutants General should update their state crisis action plans.

Key Step #3. The OHS Director should request the National Guard to work with Local and State officials to develop public information campaigns. An information operations plan to prevent panic and misinformation should be included in all military department press plans and consequence or crisis management strategies. This is a key component of the information war against terrorism because one goal of terrorists is to create panic and chaos.

A seamless information warfare operation should involve not only the military, but also the Director of the Office of Homeland Security. The President should appoint a national spokesman, perhaps from OHS, for the release of information about emergencies. The OHS Director should request that the National Guard and State and Local officials in each relevant area appoint spokesmen as well who will communicate with the national spokesman daily regarding any terrorist events.

Key Step #4. The Secretary of Defense, with the Secretary of Transportation and the OHS Director, should re-institute a robust port security program to check all incoming ships and containers. The Secretary of Defense should ensure that U.S. Navy ships, in conjunction with the Coast Guard, are stationed so as to protect sea approaches to key U.S. ports and waterways 12 miles from the coast, not three miles, which is the present Coast Guard standard. The most effective way to get a large weapon of mass destruction into the United States is on a ship or in a container, and joining a ship's crew offers would-be terrorists a way to enter the United States. New equipment is needed to detect smuggled nuclear devices. DOD, in cooperation with the Department of Energy, should promote the research and development of more effective equipment and sensors.

During the Cold War, as a defense against espionage, sabotage, and weapons of mass destruction (WMD), the Coast Guard and U.S. Navy—working with the Maritime Administration of the U.S. Department of Transportation—monitored all Soviet-bloc ships and crews that came into the United States, and some ports were closed for security reasons. But this program ended in the 1990s, and today the Coast Guard can inspect only 3 percent of containers that come into U.S. ports.

On the eve of the terrorist attack on the United States, there was no port security program in place that provided consistent, routine surveillance of ships, cargoes, containers, and crews. The port security system should be reconstituted. All ships entering U.S. territorial waters should be identified, and boarded and searched if authorities determine that is required. Since September 11, ships are required to give 96 hours prior notice of arrival. That notification of arrival should include crew, cargo, and passenger lists and manifests.

PRIORITY #2: PROTECT U.S. BORDERS, COASTS, AND CRITICAL NATIONAL INFRASTRUCTURE WITH AIR DEFENSE AND MISSILE DEFENSE.

As the events of September 11 showed, vital infrastructure in America's cities remains vulnerable to attack from any number of threats, including missiles launched from offshore. Most of the countries that the Department of State has identified as sponsors of terrorism are working to gain WMD and the missiles to deliver them.

Only an effective, tiered missile defense system can protect the nation's homes and people from these weapons. The President took the correct action in notifying Russia that the United States would no longer observe the 1972 ABM Treaty with the Soviet Union. It is urgent that the Department of Defense test and field a ballistic missile defense system as soon as possible.

The Department of Defense should be prepared to protect critical national infrastructure by rapidly deploying air defenses and cruise missile defenses when the need arises. The \$8 billion per year currently programmed in the Defense budget for ballistic missile defense research is adequate funding. Additional steps, however, are also necessary. Specifically:

Key Step #1. Congress should provide additional funding for the deployment of a cruise missile defense system as a component of homeland defense. At present, the United States has the technology to defend the homeland against cruise missiles, which could carry WMD or conventional blast warheads. Cruise missiles have proliferated widely around the world; they can be launched from aircraft or ships, including civilian merchant ships off the U.S. coast. But unlike ballistic missiles, which first are launched up into the atmosphere and follow a parabolic trajectory flying back down to a target, cruise missiles generally fly a straight, almost line-of-sight trajectory. Defending against them requires deploying a robust cruise missile defense system.

Key Step #2. The Secretary of Defense should deploy air defense and cruise missile defense systems to defend major U.S. cities and critical infrastructure. A layered approach to global ballistic missile defense, with both ground-based and sea-based interceptors, would help protect the homeland from ballistic missile attack. To defend against cruise missiles, defensive systems should be stationed around the U.S. coast on ships or at critical sites on land. Among the systems that would be effective are radar-directed, high-speed gun systems; laser and directed-energy weapons; and short-range, high-speed air defense missiles. The Mark 15 Vulcan-Phalanx gun system, short-range, man-portable air defense systems, and air- or ground-based lasers all offer effective and easily fielded defenses against cruise missiles.

PRIORITY #3: ENHANCE REAR-AREA MILITARY OPERATIONS TO PROTECT THE HOMELAND AND PREPARE FOR TERRORIST ATTACKS.

The use of the military in homeland defense against terrorism has limitations. The first priority must be to stop a terrorist act before it can cause catastrophic damage through quick actions. Unless a terrorist event takes place on a military installation, however, Local, State, and Federal law enforcement agencies and medical and emergency services personnel—not the U.S. military—will be the front-line troops, or “first responders,” in dealing with terrorist attacks on the homeland.³

What the U.S. Military Can and Cannot Do. The U.S. military can assist Local, State, and Federal agencies in homeland defense by identifying and assessing security levels at critical infrastructure nodes; providing protections for critical infrastructure; providing redundant communications, command, and control systems; and procuring and maintaining equipment that would assist Local and State responses to terrorist incidents. The Department of Defense can also provide military assistance to civil authorities to help them respond to certain situations involving chemical or biological weapons of mass destruction and nuclear materials.⁴

Neither the Posse Comitatus Act nor other statutes seek to deny, limit, or condition the President's use of the armed forces to respond to a catastrophic terrorist attack on the United States.⁵ However, active-duty armed forces and reserves, while in Federal service, are prevented by the Posse Comitatus Act from engaging directly in most law enforcement functions. The Posse Comitatus Act (18 U.S.C. § 1385)

3. Separate statutes allow the President to use the military to keep the peace in an emergency or disaster not prohibited by the Act—such as a hurricane, riot, or earthquake—and Congress has authorized the use of the military for specific immigration and drug enforcement tasks. Military personnel, moreover, are required to enforce the military justice system on military bases, including making arrests that involve military personnel and others. For more on first responders, see chapter on Civil Defense and chapter on Intelligence and Law Enforcement.

was enacted in 1878 to end certain military practices in the post-Civil War reconstruction era. It does not apply when a governor utilizes the National Guard in state service. In its current form, the Act provides that the Army and Air Force may not be used to “execute the laws” unless “expressly authorized by the Constitution or Act of Congress.”⁶ The Act acknowledges that the President retains some constitutional authority to use the military in certain circumstances. By declaring an emergency in the event of attack, riot, or other major disaster, or the threat thereof, the President can utilize federal armed forces to maintain order and protect life and property.

Military personnel can act decisively to stop a catastrophe or terrorist act occurring in their presence. The Department of Defense may make available military personnel or equipment or provide technical assistance in many situations; thus, the courts have not interpreted the Posse Comitatus Act as prohibiting all assistance to Local, State, and Federal law enforcement operations.

To enhance military operations in homeland defense beyond the scope mentioned above, the Secretary of Defense should clarify command and control. Specifically:

Key Step #1. The Secretary of Defense should make the Commander in Chief (CINC) of the Joint Forces Command also the CINC for military operations to defend the homeland against terrorism.⁷ At present, the U.S. Army is the executive agent for military support for homeland defense operations; its emergency operations center initially receives, processes, and prioritizes the requests that come in from civilian authorities for military support. The Joint Forces Command in Norfolk, Virginia, is DOD’s commander and manager for homeland security and for responses to terrorist incidents or incidents involving weapons of mass destruction. It tasks the service components (the Army, Navy, Marine Corps, Air Force, and Coast Guard

-
4. For a comprehensive discussion of the Posse Comitatus Act, see Charles Doyle, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*, Congressional Research Service, CRS Report 95-964, June 1, 2000. For the relevant laws on military assistance to civil authorities in WMD-related incidents, see 10 U.S.C. Section 382, *Emergency Situations Involving Chemical or Biological Weapons of Mass Destruction*, and 18 U.S.C. 831, *Prohibited Transactions Involving Nuclear Materials*. Department of Defense Directive 3025.15, *Military Assistance to Civil Authorities*, requires that requests for assistance to civil authorities be evaluated against six criteria: compliance with law; potential use of lethal force by or against DOD forces; safety of DOD forces; impact on DOD budget; and impact on DOD’s readiness to perform its mission.
 5. See Paul Schott Stevens, “U.S. Armed Forces and Homeland Defense: The Legal Framework,” Center for Strategic and International Studies, *CSIS Report*, October 2001, p. 3.
 6. This language creates some ambiguities and exceptions. For example, federal appellate courts disagree as to whether the Act applies to the Navy and Coast Guard, and a logical argument can be made that it should not apply on the high seas.

components assigned to it in DOD's Unified Command Plan) to respond to events around the United States.

The CINC for homeland defense operations must be a Unified Command that has a strong staff familiar with the National Guard and land and maritime operations. It cannot be a highly specialized specified command that is expert at a single facet of warfare (such as air or space defense). At present, the Joint Forces Command has the assets and experience its commander needs to function effectively as CINC for homeland defense.

The Army Forces Command and the Air Force Air Combat Command are component commands of the Joint Forces Command, with subordinate organizations that they train, equip, and control in the United States. The Naval Service elements of the Joint Forces Command (the Atlantic Fleet and the Marine Forces, Atlantic) train, equip, and control organizations east of the Mississippi River. (They work through lateral and higher headquarters to task organizations west of the river.) In the case of the Navy and Marine Corps, the Chief of Naval Operations and the Commandant of the Marine Corps should be responsible for operational support to the CINC Joint Forces Command. This will permit those service chiefs to direct forces throughout the United States.

The Joint Forces Command established the Joint Task Force Civil Support (JTF-CS) at Fort Monroe in Hampton, Virginia, to provide command and control over DOD forces in support of lead Federal agencies—those agencies held responsible by the President under Presidential Decision Directive (PDD) 63 for managing consequences of WMD or other incidents in the United States, its territories, or its possessions. Examples of lead Federal agencies are the Centers for Disease Control and Prevention (CDC) for medical or biological incidents, the Federal Emergency Management Agency (FEMA) for consequence management in major disasters, the Federal Aviation Administration (FAA) for airline crashes, and the Federal Bureau of Investigation (FBI) for criminal investigations. Broadening the mission of the Joint Forces Command, which handles incidents using weapons of mass destruction, to make its commander the CINC for homeland defense is a sensible course of action that takes advantage of that expertise.⁸

-
7. In discussion with some members of the Working Group, an alternative approach was also suggested. Since the U.S. Army Forces Command now controls or coordinates with all Army National Guard elements in the United States, Continental U.S. Armies (CONUSAs), State Area Commands, and State Adjutants General, a logical alternative to designating Joint Forces Command as CINC Homeland Security would be to vest that responsibility in Forces Command and make it a unified command with the responsibility for homeland defense.
 8. The Joint Forces Command will likely require relief from some of its NATO-related responsibilities if this course of action is adopted.

Key Step #2. The Secretary of Defense should use the deliberate planning process to establish a refined list of military responses to terrorist acts in the United States. One approach that has been used in some Unified Commands is the establishment of Standing Joint Task Forces (SJTFFs) to respond to contingencies. But such organizations tend to burden apportioned military staffs with additional personnel, logistics, and administrative requirements, and they can build up staffs that take on a life of their own. It is noteworthy that a number of Federal agencies—FEMA, the Environmental Protection Agency (EPA), CDC—and many military organizations already have pre-planned deployment lists of people and equipment to move in case of emergency, and plans on how to load equipment for transport to respond to crises. This should be the model for establishing military component responses and planning. In fact, DOD uses the same approach for war planning very effectively.

Key Step #3. The Secretary of Defense, in cooperation with the OHS and the Cabinet, should require the development of an interactive network of operations, command, and control centers and service mobilization directorates linked with key Federal and State response agencies. All military and civilian authorities at the Federal and State levels should be able to communicate with each other through redundant but secure systems. The Secretary of Defense, in consultation with Cabinet members and the OHS, must ensure that the operations, command, and control centers in the Joint Chiefs of Staff (JCS) and the service mobilization directorates are tied into the State emergency management operations centers, the STARCs, FEMA, the CDC, and other first responders using dedicated and redundant command, control, communications, and computer (C4) networks. The military departments and Joint Staff support operations should communicate with and involve civilian authorities through directorates of military support in their operations centers. Representatives of other Federal agencies should be co-located in the centers.

In many cases, the geographical areas of responsibility within the United States differ for various agencies with homeland security or consequence management responsibilities. For example, the FEMA, FAA, and Continental U.S. Army (CONUSA) regions and the sub-regions of responsibility for other federal agencies do not always coincide. To resolve the inevitable confusion that results from such differences, the CINC for homeland defense and the Director of the Office of Homeland Security should conduct regular exercises and training sessions that involve all Federal agencies and the States.

Key Step #4. The service branches should ensure that active-duty members, reservists, and National Guard personnel understand how to correctly apprehend suspected terrorists. The service members who are out protecting some locations are basically infantrymen. They usually have little or no instruction in the rules of collecting

evidence, apprehension of suspects, cursory legal searches, or the legal seizure of contraband, weapons, or evidence. Their goal should be to prevent a catastrophic terrorist act.

Key Step #5. The service branches should provide training for the National Guard, FEMA, and other Federal and State agencies on incident response and mitigation.

In many cases, the U.S. armed forces have specialized knowledge and training on planning for and conducting these types of operations, as well as instruction on maintaining, budgeting for, and sustaining equipment. This knowledge can be transferred to first responders at the Local and State levels by including the National Guard, FEMA, and other Federal agencies in the military's formal training programs and exercises on incident response and mitigation.

Key Step #6. The Secretary of Defense should ensure that all components of the Joint Forces Command can directly task units around the United States to respond to incidents. The Navy and Marine Corps components of the Joint Forces Command are essentially only responsible for direction, training, staffing, and equipping of organizations east of the Mississippi River. They should be able to task organizations throughout the United States in a rapid manner without requiring lateral coordination with Navy and Marine Corps headquarters west of the Mississippi. All the components of the Joint Forces, in particular the Navy and Marine Corps, should be able to respond to a terrorist incident or requests for support without passing the mission to another headquarters. The Chief of Naval Operations and the Commandant of the Marine Corps, not a subordinate headquarters with limited regional authority, should be the force provider.

PRIORITY #4: PROVIDE INTELLIGENCE SUPPORT FOR MILITARY OPERATIONS.

Effective military operations depend on timely and accurate intelligence about enemy forces, movements, capabilities, and intentions. Real-time, all-source intelligence fusion centers are required for effective counterterrorism military operations and for homeland defense.

As discussed in the chapter on Intelligence and Law Enforcement, the Director of the OHS, with the Director of Central Intelligence (DCI), should foster the development of an all-source intelligence fusion center for providing information to authorities on a need-to-know basis about the potential terrorists, including where their cells are located and their plans, activities, and stated intentions. The database should be interactive and networked, linking Federal agencies and sophisticated collation and analysis methods to develop intelligence on terrorists.

Five of the terrorists who attacked the United States on September 11 were on the watch lists of different U.S. government agencies. Three of the five were on a CIA watch list. Of the 13 terrorists in the United States on visitors' visas, three were here on expired visas. Thus, information about many of those terrorists and their movements existed in federal databases before that tragic day. However, these databases were not integrated or linked for common retrieval of information. Thus, no single agency—not the FBI, the Department of Defense's intelligence units, the Federal Aviation Administration, the Immigration and Naturalization service, nor the CIA—was able to query all the databases to fuse, collate, and assess the quality of that information.⁹ While it is impossible to say what might have happened had authorities apprehended and questioned the five people on the federal watch lists or the three with expired visas, integrated databases and fusion centers would facilitate such action. To achieve this goal, two key steps must be taken:

Key Step #1. The Defense Department should institute local, low-level counterintelligence source operations for force protection near military installations. Defense counterintelligence agencies (elements funded under DOD's Foreign Counterintelligence Program) should work with Local, State, and Federal law enforcement personnel to develop an information network on potential terrorists or military surveillance in an area. Military police, military intelligence officials, and DOD counterintelligence and security personnel could approach retired military annuitants in the vicinity of military installations to develop a counterintelligence source network.

Key Step #2. The Director of OHS and the Director of Central Intelligence should ensure the creation of all-source fusion centers for collecting and sharing information about terrorist cells, plans, activities, and intentions. As discussed in more detail in the chapter on Intelligence and Law Enforcement, a national fusion center for intelligence and information on the threat to the homeland is vital to protecting the homeland and deploying resources efficiently and effectively. Local, State, and other Federal personnel who require access to this information must undergo necessary background investigations by Federal authorities. In addition, States and Localities will have to build information storage and processing facilities and systems that meet federal standards for the handling of classified national security information.¹⁰

9. With respect to the terrorists that attacked the United States on September 11, whenever the FBI places a suspected terrorist on a watch list, it circulates that person's photo to local police, immigration officers, or customs agents. Though some of the hijackers were on U.S. intelligence agency watch lists when they boarded the planes on September 11, the intelligence/information was not shared with the FAA, which could have used it to alert the airlines.

PRIORITY #5: ENSURE CLEAR COMMAND AND CONTROL OF OVERSEAS ANTI-TERRORISM OPERATIONS.

The Department of Defense and the Joint Staff have an effective and functional Unified Command Plan that sets out the responsibilities of the U.S. Armed Forces to conduct war and defend the United States. It would be a mistake to attempt to reorganize that structure in the middle of any war, including the current war on terrorism. The Administration should rely on the Unified Command Plan and the geographic Unified Commands (PACOM, EUCON, SOUTHCOM, CENTCOM) to fight the war on terrorism overseas.

Key Step #1. The Secretary of Defense should keep SOCOM as a force provider (supporting CINC), not the major war fighter, and assure that SOCOM has adequate resources to carry out its mission. The Secretary of Defense should resist calls to establish a command to handle overseas operations against terrorism. In war fighting, the U.S. military employs a geographic Unified Command structure as the supported CINC to direct and control overseas combat, covert actions, and military intelligence-gathering operations. This structure provides the necessary command, control, communications, computer, and intelligence (C4I) capabilities for coordinating operations. It also has the logistics support infrastructure necessary for conducting operations. In addition, each Unified Command has an integrated special operations organization and liaison officers from within the U.S. Intelligence Community.

Thus, the geographic Unified Command remains the best-equipped and best-structured organization to control major military operations. The Special Operations Command (SOCOM) should be a specified command for managing counterterrorism operations so that it can direct training and operations, properly resource the fight, and develop new systems to support the fight.

The major war fighter, or supported CINC, should be the geographic Unified Command. Some defense analysts have suggested that SOCOM should become the supported command (the war fighting CINC in charge of all forces, support, and operations) in the war on terrorism. There also have been calls for a major increase in the number of special operations forces. But there are practical limits on the number of personnel that can be recruited and trained for special operations. These limits are a function of the demanding mental, physical, technical, and linguistic requirements for participating in special operations, as well as the relatively small number of people who volunteer for such duty. An expanded armed force, however,

10. For detailed descriptions of the information to be collected and the process for disseminating it, see chapter on Intelligence and Law Enforcement.

would provide a larger base of personnel from which to draw such dedicated volunteers.

As the main campaign against the al-Qaeda network in Afghanistan achieves its goals, the war against terrorism will likely shift to other areas of the world, where clandestine infiltration and exfiltration as well as unilateral direct actions could become the more common methods of destroying terrorist cells. Rather than increase funding for more special operations personnel, the Administration should focus on ensuring that a healthy mix of CIA and Special Operations Command personnel are on the staffs of the geographic CINCs and that the JCS headquarters and CIA are appropriately cross-staffed to permit proper coordination of such operations.

SOCOM must be able to direct the training and operations, prepare the budgets to resource the fight, and develop surveillance and reconnaissance systems like Predator and Global Hawk to support the fight. SOCOM should not have to compete for resources in the Unified Command Plan with the Unified Commands for specialized resources or assets. To ensure that SOCOM's acquisitions and budget requirements are properly prioritized, the Secretary of Defense must make sure that the Defense Guidance specifically charges SOCOM with those responsibilities. In addition, the Under Secretaries of Defense must provide the political leadership to ensure that the service bureaucracies do not simply return to business as usual.

Key Step #2. The commander in chief for homeland defense should prepare pre-planned force packages for initiating rapid responses to contingencies. The geographic CINC should plan for the movement and arrival of forces with dedicated movement packages and notional time-phased force deployment lists. The service component commands and the headquarters of the Unified Commands should use the deliberate planning process and time-phased force deployment lists to plan for forces that can rapidly respond to contingencies. The creation of numerous standing joint task forces is not recommended, since it could tax the staffs of the component commands and create more bureaucracy in the Unified Commands.

For lower-intensity operations overseas that require close coordination with the Intelligence Community, and for other covert activities, the geographic CINC should continue to be the supported CINC. Having a CIA liaison in each geographic Unified Command also will facilitate coordinated operations.

Key Step #3. The Secretary of Defense should ensure that the Defense Guidance sets out the nation's clear priorities regarding the conduct of the war against terrorism. These priorities—especially surveillance, reconnaissance, logistics, communications, and intelligence support for the fight—must be reflected in Defense research and

acquisitions plans, policies, and budgets to ensure that any bureaucratic inertia or parochial interests do not hinder the effort.

CONCLUSION

Any attempt to completely reorganize the armed forces in the middle of the war on terrorism would be a mistake. The current Unified Command Plan will work well in fighting the war on terrorism overseas and defending the homeland. The United States Special Operations Command needs the responsibility and political backing in budget battles to acquire the proper new intelligence and reconnaissance systems as well as other assets for this fight against terrorism. For the defense of the homeland, the National Guard Bureau must update its own regulations and begin to train and work closely with civilian first responders at the Local level in responding to crises.

Information operations are a necessary component of the war on terrorism to prevent panic among the U.S. population. The United States, which is now defenseless against ballistic missiles, must deploy defenses against both ballistic and cruise missile attacks. And the Department of Defense must establish a linked, searchable, and interactive intelligence database so that information acquired by different government agencies can be exploited to ensure the war's success.

Table 6

**Status of Key Unimplemented Commission Recommendations
for Counterterrorist Military Operations and Structures**

Recommendation	Name of Commission	Status
<p>Terrorist Attacks: Detection and Attribution Capabilities. Invest in capabilities to detect CBRN attacks and attribute them to likely aggressors. Credible retaliatory capability, essential for deterrence, depends on strong attribution capabilities to identify perpetrators and their supporters. Such capabilities will include laboratory facilities, equipment, and personnel necessary.</p>	Defense Science Board	Current detection and attribution capabilities are insufficient. The Department of Defense has made no known proposals to increase its capabilities with regard to the events of September 11.
<p>Warning Capability. Strengthen warning capabilities. Facilitate rapid communications for conveying information concerning a terrorist warning and preemptive strikes. Conduct a lessons-learned study of U.S. government warning across the entire intelligence cycle.</p>	Defense Science Board	Current warning capabilities are insufficient. The Department of Defense has not yet implemented plans for increasing warning capabilities.
<p>Annual Net Threat Assessment. Develop an “annual net threat assessment of the foreign and domestic threat of CBRN attack and terrorism.” Provide Federal planners with the basis for assessing the emerging risk of such attacks and develop an integrated analysis structure for planning U.S. programs and response.</p>	Defense Science Board	Current threat assessment is insufficient. GAO reports recommend re-evaluating the role of threat assessment for homeland security. No vehicle for the implementation of such assessment capabilities is known to exist.
<p>Defense Review. Congress and the Secretary of Defense should move the Quadrennial Defense Review to the second year of a presidential term.</p>	Hart–Rudman Commission	The Department of Defense has made no public proposal to move the Quadrennial Defense Review to the second year of any President’s term.
<p>Acquisition System. The Secretary of Defense should establish and employ a two-track acquisition system, one track for major acquisitions and a second “fast track” for a limited number of potential breakthrough systems, especially those for command and control.</p>	Hart–Rudman Commission	No known vehicle exists for implementation of a two-track acquisition system.
<p>Prototyping and Testing. The Secretary of Defense should foster innovation by directing a return to the pattern of increased prototyping and testing of selected weapons and support systems.</p>	Hart–Rudman Commission	Current strategy is ineffective. No vehicle exists for increased prototyping and testing.
<p>Expeditionary Capabilities. The Defense Department should devote its highest priority to improving and furthering expeditionary capabilities.</p>	Hart–Rudman Commission	Current strategy is ineffective and insufficient. Requires continued support and improvement.
<p>National Guard. The Secretary of Defense, at the President’s direction, should make homeland security a primary mission of the National Guard, and the Guard should be reorganized, properly trained, and adequately equipped to undertake that mission.</p>	Hart–Rudman Commission	National Guard is currently underutilized in homeland security. Requires reorganization of State Area Command (STARC) units to be able to mobilize more quickly and effectively.
<p>Note: Information on the reports issued by these commissions may be found in the bibliography.</p>		