Report of the
Defense Science Board

Defense Imperatives for the New Administration

August 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Imperatives for the New Administration	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 & Logistics,Defense Science Board,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)**	**72**	

This report is a product of the Defense Science Board (DSB).

The DSB is a federal advisory committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report was prepared by the DSB Task Force on Future Perspectives; the task force completed its information gathering in June 2008.

This report is unclassified and cleared for public release.

Defense Imperatives for the New Administration

THIS REPORT DESCRIBES... THOSE ISSUES THAT THE NEXT SECRETARY OF DEFENSE SHOULD PLACE AT THE TOP OF THE AGENDA—ISSUES THAT WILL REQUIRE THE ATTENTION OF THE COMMANDER-IN-CHIEF, AND, IF LEFT UNRESOLVED, COULD LEAD TO FUTURE MILITARY FAILURE.

It has been more than two generations since the presidency transitioned with American troops engaged in significant combat operations—a deployment begun in the aftermath of the September 11, 2001 attacks.

Beyond the current military engagements in Iraq and Afghanistan, the nation faces other equally important national security challenges. These include nuclear proliferation, the potential for other regional conflicts into which we could be drawn, and the spread of militarily relevant technology even beyond nation-states.

The incoming leadership must be prepared to deal with the most pressing issues facing the Department of Defense today. The pressing issues described herein are daunting and may seem all-inclusive, but they are only a fraction of the defense challenges facing the new administration. This report describes just those issues that the next Secretary of Defense should place at the top of the agenda—issues that will require the attention of the Commander-in-Chief, and, if left unresolved, could lead to future military failure.

This report offers recommendations drawn from reports prepared by the Defense Science Board, an advisory body to the Secretary of Defense, which address topics at the confluence of technology, policy, and management.

Contributors

Dr. Craig Fields

Dr. Theodore Gold

Dr. Robert Hermann

Dr. William Howard

Dr. Miriam John

Dr. Ronald Kerber

Mr. Verne L. Lynn

Dr. Joseph Markowitz

General James McCarthy, USAF (Ret.)

Mr. Robert Nesbit

Mr. Vincent Vitto

Table of Contents

Our unmatched military capability alone is not sufficient for achieving national goals

America's traditional military capability is unmatched in the world today. We have an abundance of conventional and nuclear weapons. We enjoy the most advanced command, control, communications, and intelligence systems. We field the best weapon systems, from the reaches of space to the depths of the oceans, and the best trained and finest military personnel. Yet, none of this, by itself, can guarantee successful accomplishment of the national security and foreign policy objectives for which this formidable capability was developed.

… THERE ARE PRESSING ISSUES THAT THREATEN TO DEGRADE OUR CAPABILITIES AND COMPROMISE THE SUCCESS OF EVEN TRADITIONAL MILITARY MISSIONS.

International economics and natural resources, ideology and national will, and diplomacy and reputation all play an even greater role today than in the past and can impede our ability to achieve national objectives. Moreover, there are pressing issues that threaten to degrade our capabilities and compromise the success of even traditional military missions.

The President calls upon the Department of Defense (DOD) to perform certain traditional missions, in orchestration with other federal, state, and local government organizations. DOD's missions aim to stabilize relationships with major nations and regions around the world, so as to maintain economic, political, and social engagement; reduce the need or likelihood of armed conflict; and keep the American homeland safe.

Listed below are DOD's five primary missions. Beneath each are the pressing issues most likely to compromise the success of that mission.

1. Protect and defend the homeland.

- ***Weapons of mass destruction challenge the safety of our homeland and our military forces.*** A major factor in addressing the threat from weapons of mass destruction (WMD) is a fundamental lack of information needed for interdiction and deterrence, calling for a major increase in focus on the full range of WMD by our intelligence community. Furthermore, one of the easiest ways for terrorists to create weapons such as bio-weapons is from materials and equipment purchased or stolen in the United States, which places a particular premium on domestic intelligence.

  We should make it more difficult to acquire WMD in the first place—replacing the radioactive isotope Cesium-137, widely used in medical facilities throughout the country, is one possible step. We can improve U.S. capabilities for attribution and declaratory policies for retaliation, in service of deterrence. Finally, if national and military capabilities for WMD response, mitigation, and recovery for the civilian population and military personnel are significantly improved—such as with more training and clearer lines of responsibility and authority—adversaries' calculus for even using WMD could change in our favor.

- ***Our nuclear capability—weapons, skills, facilities—is declining.*** The nuclear threat is no less diminished with the rise of biological, cyber, and other asymmetric threats. Every current nuclear power except the United States is modernizing its nuclear capability. In contrast, there are early signs of serious problems with the safety and surety of the U.S. nuclear deterrent capability. Senior-level attention and management discipline must be restored. There are concerns, as well, over the performance of our conventional military capability if under nuclear attack—which calls for re-invigorated training of conventional forces for survival and operation in a nuclear environment. Moreover, there is no national consensus as to how to proceed in modernizing the nuclear deterrent, which is all the more reason that we must maintain our human resource skill levels in weapon design and nuclear effects. In short, leadership is both the problem and the solution.

2. Maintain the capability to project force around the world, so as to deter enemies, defend allies, and protect American interests. If deterrence fails, defeat adversaries swiftly and thoroughly.

- ***Our military and civilian information infrastructure is highly vulnerable.*** And our military forces are highly dependent on this infrastructure, so this is the Achilles' heel of our otherwise overwhelming military might. There is a growing awareness about advanced cyber threats, but scant real progress to better secure our information infrastructure against those threats. Of particular concern is the vulnerability of our space assets to cyber attack, not only satellites but also ground stations. Much can be done in the near term to improve cyber security that goes beyond the current "perimeter defense" strategy. Improvements include thoughtful acquisition and operation of the information infrastructure to ensure better security in the first place. Further, since we will never achieve invulnerability, we need to train to operate with degraded information infrastructure. We need to be prepared for a long-term, rapid-fire contest between defense and attack. Cyber warfare is here to stay. It will encompass not only military systems but also civilian commercial systems, not only high technology cyber attacks but also bombing and jamming, not only remote attacks but also threats from recruited insiders.

- ***DOD's business practices are having a long-term debilitating effect on our military forces.*** Poor business practices—acquisition, logistics, and infrastructure—raise costs and slow modernization so significantly that they threaten to compromise America's technology lead and force capability. In these areas, the Department lacks the business discipline that is commonly found in the commercial sector and which can be and needs to be applied within the Department—comprehensive business planning, specification of requirements, spiral development, systems engineering capabilities, advanced network interoperability, and logistics modernization are some examples. Coupled with this discipline is the need for clearer responsibility and accountability for acquiring and maintaining military force capabilities—a greater role for the combatant commanders who are actually the consumers responsible for military success.

3. Bring stability to nations and regions, including reconstruction, nation-building, peacekeeping, and regional de-escalation.

- ***Robust plans and capabilities are lacking to support country-specific stability operations.*** Stabilization and reconstruction must become a core competency within DOD and other departments. Enhancing U.S. abilities to transition to and from hostilities requires better planning and personnel with a wider range of skills, in areas such as civil affairs, languages, and cultural understanding. Effective strategic communication of U.S. intentions and values is a vital element of stability operations, requiring improvements as well. No less important is the need to improve knowledge, understanding, and intelligence.

4. Thwart terrorism and bring terrorists to justice, anytime and anywhere. Our concern is terrorists and terrorist organizations that would attack the United States, our allies, and our global strategic interests.

- ***We lack the deep penetration required for actionable intelligence—both foreign and domestic—to thwart terrorism.*** Developing intelligence regarding terrorists is both difficult and different than in the past. Intelligence analysis and information sharing—"connect the dots and share the dots"—important as they are, is actually a lesser hindrance than fundamental lack of information—that is, having "the dots" in the first place. An important aspect of improving our knowledge will come from broadening the scope of both foreign and domestic intelligence activities. We need deep penetration of terrorists and their supporters—such as information on finance and materiel—involving close-in sensing, tracking key individuals, and persistent collection. And we can make much greater use of unclassified, open sources of information as well. Finally, we need an intelligence "collection architecture" appropriate for thwarting terrorism. An architecture that harmonizes foreign and domestic intelligence, and all the means we have available for learning the capabilities, intentions, identities, and locations of terrorists and their supporters.

5. Support state and local authorities in providing relief from domestic catastrophe.

- ***The nation lacks validated operational contingency plans to respond to domestic catastrophes—whether natural or malicious.*** There is a rising threat of homeland attack, the scale of which may well exceed expectations and preparations. Attacks of such scale could occur as a single event or an orchestrated series of attacks across the country. Current plans are not adequate and we, as a nation, are not prepared. Furthermore, to the extent that DOD resources are called upon to aid local authorities in disaster relief, those military resources will not be available to simultaneously project force and defend American interests around the world. The resources needed could be substantial, as the number of DOD personnel involved with Hurricane Katrina was about the same as the entire military might of the UK and about half of the size of the force that we have in Iraq.

  "Hardening the homeland" requires preparation at all levels—the individual and family level as well as local, state, and federal government, including DOD—and it requires better partnership with the private sector. A key component of preparation is detailed planning and training in advance. National response plans and exercises involving all levels of government must be taken as seriously and conducted as professionally as our joint forces prepare for military combat. DOD in turn must take steps to raise its level of readiness to provide domestic catastrophe support, as it will surely be called upon to do so.

In addressing these challenges, DOD cannot "go it alone"—its success depends on orchestrated government action. Both civil and military skills are needed to affect national security policy, but government-wide organization of these skills is lacking. What is needed is an integrated operational concept, set of strategies, execution capabilities, and means for resource allocation.

Like every large organization, DOD can improve in many ways. But the issues identified herein, if not attended to with careful preparation, could lead to disastrous failure. These issues, along with recommendations for addressing them, are detailed in the remainder of this report.[1]

1. The recommendations, briefly described in this report, are fully explained and supported as appropriate with classified information, in the referenced studies.

1 Protect and defend the homeland

The first and most important duty of the government, as spelled out in the Constitution, is "To provide for the common defense." The highest priority national objective—of which there is little disagreement as to purpose—is preserving the Republic and protecting its citizens. Thus, "Job #1" for the U.S. military is defense of the homeland.

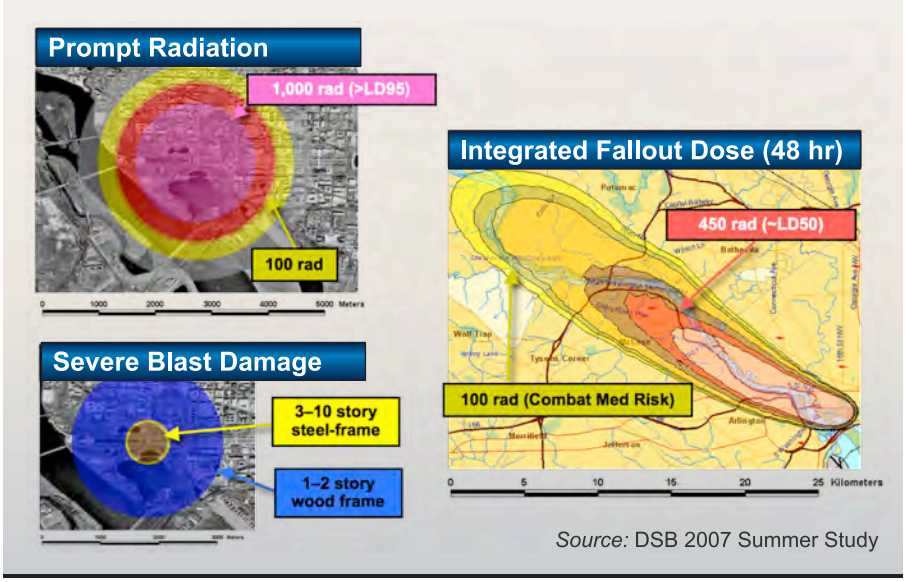
Throughout the latter half of the 20th century, the most significant threat to the U.S. homeland was the specter of a full arsenal exchange with the (former) Soviet Union—a threat dealt with by symmetrically assuring the destruction of their homeland. Mutually Assured Destruction, and deterrence more generally, seemed sufficient to protect the homeland from attack. This complacency was shattered along with the World Trade Center on September 11, 2001.

Since then, the nation has begun to reconsider both the threats to its homeland and the appropriate military countermeasures to those threats. The homeland can no longer be considered a sanctuary. Valid threats appear to come from non-state actors, who are loosely networked and difficult to deter—actors willing to use weapons of mass destruction, either smuggled into the country or produced within the United States itself. Yet, intelligence about adversary capability and intent is scant. Both domestic and foreign intelligence are critical and lacking.

WEAPONS OF MASS DESTRUCTION CAN ENDOW LILLIPUTIAN ADVERSARIES WITH THE THREATENING POWER OF PEERS.

Weapons of mass destruction challenge the safety of our homeland and our military forces

Weapons of mass destruction can endow Lilliputian adversaries with the threatening power of peers. Bio-warfare is a rising concern. The largely beneficial advance of biotechnology enables easier and easier preparation of virulent, infectious agents—even preparation within the United States where the technology is widely available. Nuclear weapons are in a class by themselves in terms of their potential for devastation and destruction. The production of nuclear weapons, particularly weapons grade fuel, remains the domain of nations, so far. But the line between peaceful use of nuclear power for energy production and nuclear weapons development is razor thin and difficult



Nuclear weapons are in a class by themselves. Even a small inefficient device using stolen enriched uranium would be disastrous.

to monitor. Moreover, there is an ever present danger that nuclear weapons will be purchased or stolen by terrorists who are difficult to deter. While the nation once worried about nuclear weapons delivered to its shores by bomber or ballistic missile, we now have to worry about delivery by private aircraft, ships, or trucks. Radioactive material that could be used to prepare "dirty bombs" is present throughout the United States. Cyber weapons could cause lasting damage, and significant loss of life, if used against such critical facilities as electric power stations, hospitals, and food processing or pharmaceutical production plants.

A national strategy to reduce vulnerability to WMD must do everything possible to prevent the worst people from acquiring and using the worst weapons. It requires that we perfect the means of attribution—to identify the perpetrators and their supporters—and devise clear and credible options to retaliate, so as to deter. It also requires that we urgently develop ways to mitigate the consequences and recover from the impact of such attacks. Effective mitigation and recovery could also serve as deterrence, influencing the calculus of a would-be attacker. All of these elements require exquisite intelligence.

… INFORMATION CANNOT BE SHARED OR CONNECTED IF IT DOES NOT EXIST IN THE FIRST PLACE.

WMD intelligence is improved, but still lacking

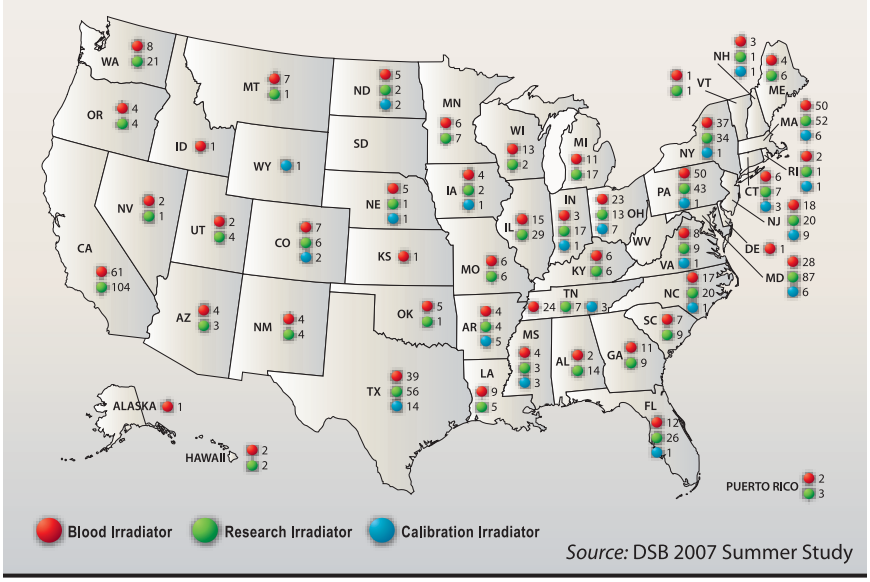
While intelligence vis-à-vis WMD has improved since September 11, deficiencies remain. There has been considerable attention to the balance between protecting information and sharing it—including sharing between foreign intelligence and domestic intelligence agencies—and how that balance should change. There has also been considerable focus on the analytical tools and approaches to connecting pieces of intelligence (the "dots"). Yet information cannot be shared or connected if it does not exist in the first place. With regards to WMD, there remains a worrisome lack of fundamental information.

Our recommendations center on acquiring information. Information collection will need to be positioned more closely to the source or otherwise have the coverage and acuity needed to sense the observable signs. Collection will be more covert, usually, but occasionally overt if we want to send a warning that we are monitoring, have more persistence, and the capability to be more intrusive than before. The nation will need to place more emphasis on the special nature of WMD, requiring as it does individuals with particular expertise as well as specialized equipment and materials.

... AN EASY WAY FOR TERRORISTS TO CREATE CERTAIN FORMS OF WMD... WOULD BE FROM MATERIALS AND EQUIPMENT PURCHASED OR STOLEN WITHIN THE UNITED STATES.

The first step is to deny WMD acquisition and transport

The worst forms of WMD, nuclear weapons and some kinds of biological weapons, would likely be acquired by terrorists from nation-state proliferators. We should not overlook the fact that an easy way for terrorists to create certain forms of WMD, including some biological weapons, would be from materials and equipment purchased or stolen within the United States. For example, one of the nation's most serious vulnerabilities to a radiological dispersal device—or "dirty bomb"—is the widespread presence of the radioactive isotope Cesium-137 used primarily for medical applications throughout the country.



Radioactive materials that might be stolen to produce a "dirty bomb" can be found throughout the United States.

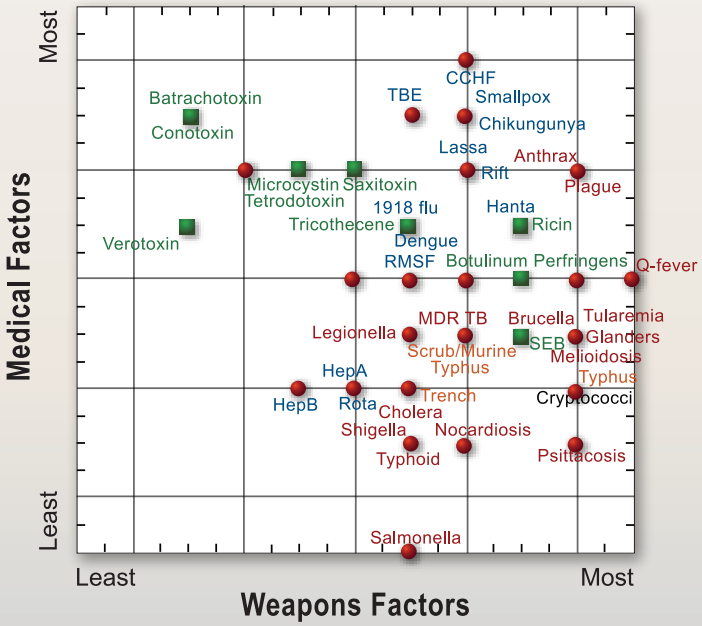
Detecting and interdicting a nuclear weapon in transit—or for that matter, almost any weapon of mass destruction—is unlikely without some type of intelligence tip-off. And we can't depend solely on technology. There are just too many ways to defeat or deceive radiation detectors, and there are too many false alarms.

Taken together, we recommend an even greater effort to strengthen and broaden international cooperative efforts in non-proliferation of nuclear and biological materials, as well as "loose expertise." We also recom-

mend making it more difficult to develop WMD within the United States by, for example, urgently removing easy access to certain WMD materials like Cesium-137.

With attribution and prospective retaliation we may be able to deter use of WMD

It is our stated intention to punish anyone who uses WMD against the United States or its interests abroad, or in any way aids and abets this use, witting or unwitting. Such declaratory policy will ring hollow, however, unless it is also clear that we have credible attribution capability and realistic retaliatory means. Attribution depends on combined intelligence and forensics, and both need improvement. Credible retaliation requires detailed understanding of adversaries and their values, as well as detailed planning to bring to bear all elements of national power.



Note: Potential for increased bio threat in next 5 years— modified or engineered bio materials. Medical factors include infectious dose data, virulence/lethality, diagnosis, treatment. Weapons factors include stock availability, weaponization, dissemination, persistence.

Source: Compiled by MIT Lincoln Laboratory; DSB 2007 Summer Study

Our defensive efforts against the most threatening bio-agents—those that are both easily employed as weapons and cause the most medical problems—are far from comprehensive.

We strongly recommend continued articulation of clear policies of retaliation as a means of deterrence. Equally important, however, is the need to make those policies credible by improved technical means of forensic analysis—nuclear, biological, and chemical; ancillary financial, transportation, and other intelligence information—and to develop realistic plans and options for punishing potential attackers and their supporters and suppliers.

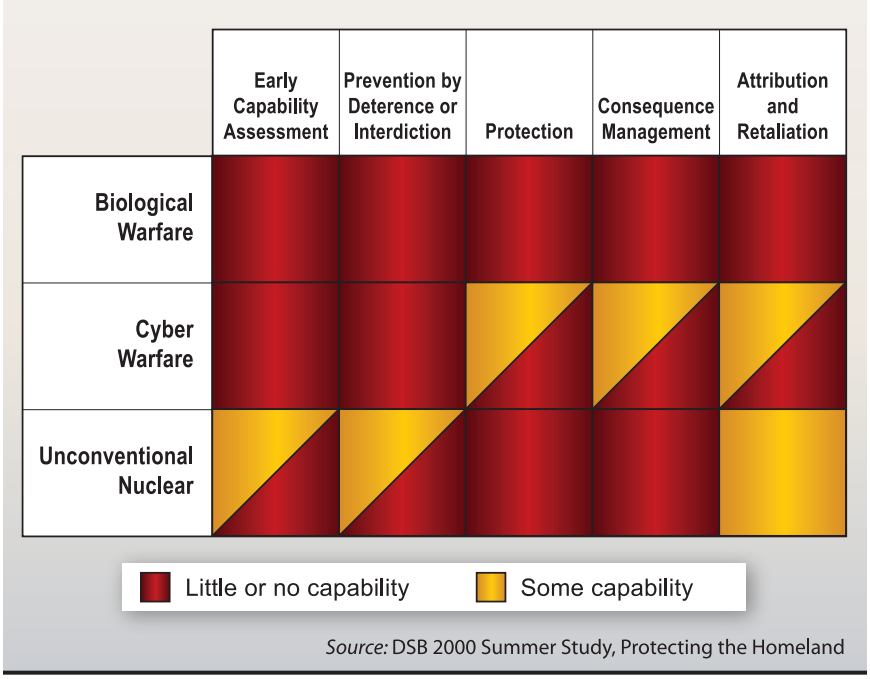
Mitigation and recovery on a national level is not well developed

The nation is still poorly prepared to mitigate a WMD attack. We lack capabilities to recover from even a low-yield nuclear event in a metropolitan area or a large-scale epidemic like plague. And the consequences of an attack, or even worse an orchestrated series of attacks, would be aggravated by accompanying cyber attacks to undercut recovery. Among many gaps, we simply do not

have in place an end-to-end medical surge capacity, taking into account each and every medical resource required from nurses to beds to respirators to quarantine capability.

Our national response planning falls short of realistic execution. Plans are not exercised with sufficient frequency, or the right set of players, or at the right scale. Nor are there mechanisms for continuous improvement based on lessons that emerge from the exercises. Required resources are neither available nor in place. Furthermore, there is too much "double counting"—presuming, for example, that the same National Guard troops can at once be counted upon to protect at home and fight abroad.

Our recommendation argues for realistic and repeated planning and re-planning, repeated exercising and improvement, and a radical increase in our medical surge capabilities. Technology development of high-payoff countermeasures—advanced medical countermeasures, advanced decontamination technology and techniques, and effective detection for early warning—are all required.



We are not ready to deal with a WMD attack on the homeland.

It is worth highlighting that mitigation and recovery will heavily depend on public response in an event. Clear and honest articulation of national plans, with realistic assessment and guidance, is critical to gaining and maintaining public support.

DOD's own mitigation and recovery needs improvement

In fact, DOD does have some unique capabilities in mitigation and recovery following a WMD attack. It has the management discipline to plan, resource, and exercise. It has a high-performance communication and information infrastructure and a practiced medical surge capability for trauma injuries.

However, DOD is not well prepared to protect its own forces from many kinds of WMD attack. It lacks the large-scale medical surge capability that would be required for many kinds of virulent biological agents, for example. DOD also lacks the ability to extend the protection afforded to its own bases to the civilian infrastructure on which it depends. Nor can it protect the local population, including those that provide a critical part of its workforce, or dependents of military personnel.

While DOD certainly has a good start on capabilities to mitigate and recover from WMD attacks, we see an urgent need to enhance those capabilities—even to the extent that they could also be available to support local authorities in time of national catastrophe, or at the very least serve as a model for states and local communities.

Our ability to respond as a nation to a WMD attack is hampered by uncertainty of responsibility and authority

Despite work to date on a national strategy and response plan, we see residual uncertainty among various levels of government regarding responsibility, authority, and accountability. It is clear that civil organizations are responsible for protecting the civilian population and infrastructure; for detecting and interdicting WMD at our shores and within the United States; and for consequence management should a WMD attack against the civilian population take place—with DOD supporting local authorities. It is also clear that DOD is responsible for protecting military facilities and personnel both in the United States and abroad, ensuring the nation's ability to project force and protect U.S. overseas interests.

However, there is a "gray area" regarding responsibility for protecting the civil infrastructure that is critical in support of DOD missions—transportation systems, commercial communications that underlie military communications, power generation and transmission systems, and the defense industrial base. Likewise, the responsibility for protecting key civilians is unclear, including the supporting civilian work force and military dependents. These ambiguities, real or perceived, must be clarified, with appropriate action to immediately follow. The fact that a

catastrophic WMD event seems unlikely to many decision-makers further compounds the problem and creates a tendency to delay action—which could be too late.

Our nuclear capability—weapons, skills, facilities—is declining

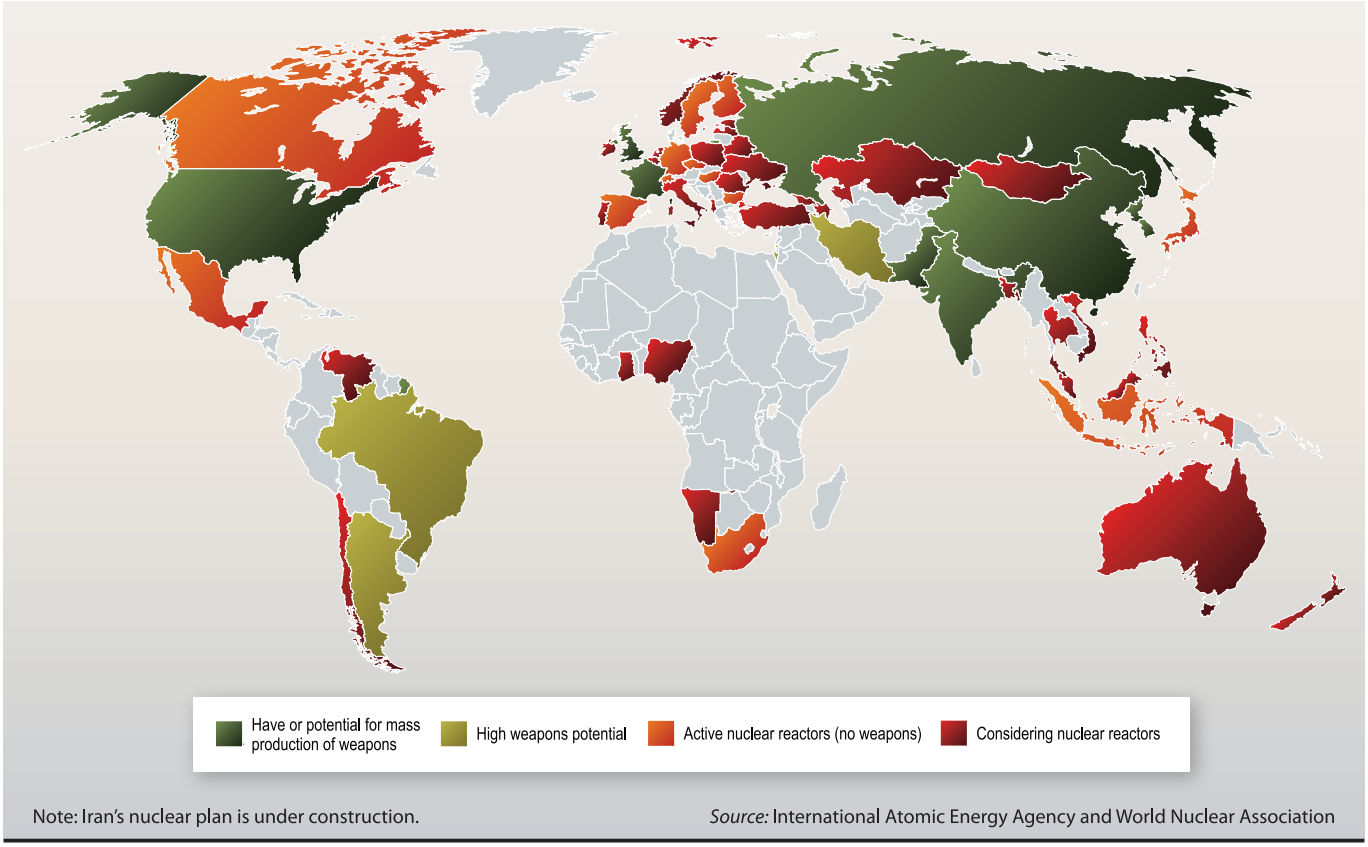
At the same time that concerns about terrorism, biological and cyber weapons, and "stray nukes" are on the rise, we can pay no less attention to the threat which preoccupied us for 45 years after World War II, namely the possibility of a nuclear attack by a foreign power.

The world is a more dangerous place

EVERY CURRENT NUCLEAR POWER EXCEPT THE UNITED STATES IS MODERNIZING ITS NUCLEAR CAPABILITY.

The world is becoming less safe in this regard. Every current nuclear power except the United States is modernizing its nuclear capability. Countries of concern, like North Korea, Iran, and Syria, are at various stages of becoming nuclear powers, in part to counterbalance U.S. conventional superiority. Some of our allies and partners are beginning to question America's commitment and relevance in extending nuclear deterrence, and may seek their own nuclear weapons. The Japanese dialog with the United States following the North Korean underground nuclear test, while not explicitly going that far, raised this issue.

We must also keep in mind that our allies and partners may not always be aligned with us in the future. Any degree of nuclear proliferation increases the likelihood of unintended or purposeful proliferation to terrorists and rogue states—many of whom have been clear about their interest in acquiring nuclear weapons. As more and more countries pursue electric power generation using nuclear energy, international monitoring regimes and capabilities will be stressed. The steps necessary to go from producing nuclear energy to developing nuclear weapons are well understood and difficult to detect. In the past half century, twenty countries started down the path to develop nuclear weapons, but for various political reasons either paused or even reversed course. Any of them might choose to resume their efforts and, today, could likely achieve nuclear-power status in record time.



Note: Iran's nuclear plan is under construction.

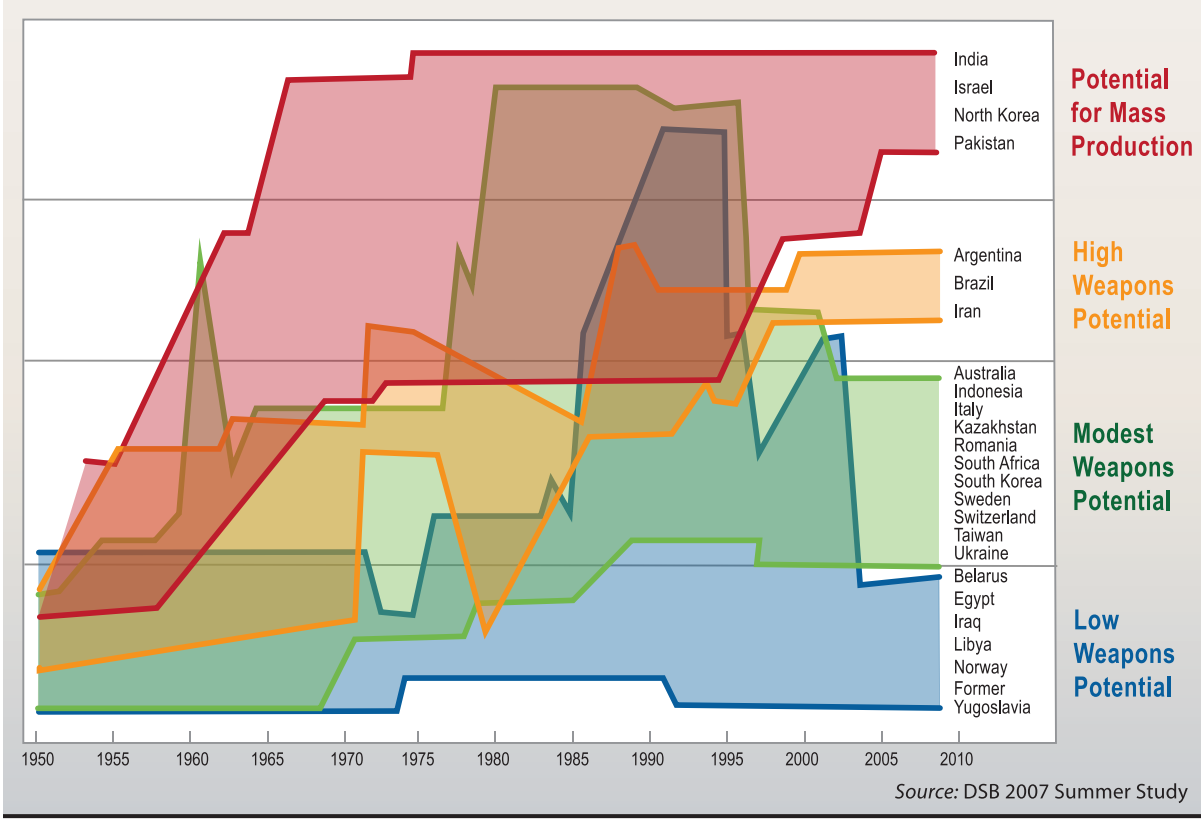
Source: International Atomic Energy Agency and World Nuclear Association

More and more countries will produce electricity using nuclear reactors. The line between producing electricity and producing weapons is thin and difficult to monitor.

There are early signs of serious problems with the U.S. nuclear deterrent capability

The prominence and priority of nuclear responsibilities within the military has been on the decline since shortly after the end of the Cold War. Recent incidents of careless handling and transport of nuclear weapons and inadvertent shipment of sensitive nuclear missile detonators to Taiwan are evidence of lack of disciplined adherence to procedures honed to ensure the safety and security of our weapons. These incidents have led to major personnel actions and reorganization in the Air Force and U.S. Strategic Command, but the issues go deeper and will take time, attention, and investment to reverse.

The United States has been engaged in retirement and dismantlement of a significant portion of its nuclear stockpile, and life extension of the remainder, since the early 1990s. No new weapons have been designed and manufactured. While the delivery vehicles for nuclear weapons are reaching the end of their lifetimes, no programmed alternatives



Proliferation can be managed. Twenty of 24 countries that began the process stopped short of developing nuclear weapons, but some of those 20 countries could restart their efforts.

are on the horizon. The oldest systems will go out of service in 20 years, and it takes 20 years to field a replacement from a "dead start," which is our current position. Further delay will serve only to produce a gap in our deterrence capability that will not go unnoticed by the rest of the world.

Most worrisome, however, is the decline and aging of our technical expertise. Within the National Nuclear Security Administration's nuclear weapons programs, the average age of staff has increased by about five years over the past decade—resulting in worrisome levels of retirement and attrition. Yet there is no strategic staffing plan to ensure critical skills are retained.

There are also problems with the performance of U.S. conventional military capabilities under nuclear attack

Despite the growing evidence of nuclear weapons proliferation and modernization, we continue to neglect training and exercising for operations in nuclear environments. For

example, there are no longer classes in nuclear doctrine or nuclear effects at the war colleges. Because we have waived the nuclear survivability requirement for many years, we do not understand how well most of our conventional forces, networked using commercial-off-the-shelf components, will perform in a nuclear environment. Our expert technical workforce in radiation effects has shrunk by 80 percent. Nuclear survivability of either military or civilian infrastructure is a very low priority.

There has been nearly a decade of impasse between the Congress and the Administration

The last Nuclear Posture Review did not result in an actionable foundation upon which to develop a strategy to address the decline in the nation's nuclear capabilities. Although the Departments of Defense, State and Energy have supported a roadmap for modernization centered on the Reliable Replacement Warhead (RRW), the Congress has not concurred. Given long standing congressional prohibition on exploration of new concepts that might produce new capabilities, future agreement on RRW might be limited to evolution of Cold War capabilities rather than development of a modern inventory better suited to today's deterrence needs. Even Department of Homeland Security (DHS) efforts on nuclear defense have been under intense scrutiny and criticism. The current congressional commission, the Congressional Commission on U.S. Strategic Posture, may catalyze constructive dialog and consensus, although that has not emerged from prior like efforts.

Leadership is the solution, but it has been the problem

The failure of leadership, over the last decade and a half, to build a consensus around a nuclear deterrent strategy suited to the multi-lateral complexities we now face is beginning to take its toll.

We can still probably deter a massive nuclear attack, but we will not retain this capability indefinitely as our weapons and platforms age beyond their lifetimes. The expected lifetime of current capabilities—barring surprises in aging materials and electronics—and the time needed to develop replacements is about the same. We need to begin

now if we are to avoid an all-too-visible gap in the nation's deterrent capability. Replenishing the expert workforce is on about the same timescale.

However, it is not only a matter of maintaining a credible deterrent against large-scale attack, but also deterring actions different from those in the past. Today's adversary is willing and able to use nuclear weapons on his own territory, or on our allies to whom we have extended the nuclear umbrella, in order to stop us. Our conventional forces are at risk in that situation, and our current nuclear capabilities, while overwhelming in number and yield, may not be relevant as a counter. This also applies to preventing or interdicting nuclear use in the homeland.

With all that said, the largest and first hurdle to overcome is neither money, nor technology, nor treaty obligations—it is a lack of leadership. We strongly recommend that the new President and his administration re-establish a focus on nuclear issues as a top priority in national security. The tools we used to great effect in the Cold War are still relevant, but must be applied in the new, more complex environment of the 21st century. We must develop policies and strategies to address the comprehensive, multi-dimensional aspects related to nuclear weapons, including force structure and size, non-proliferation, mutual agreements and transparency, and extended deterrence for our allies and partners. From the beginning, the Congress must be engaged so as to develop a national consensus. And, from the beginning, the world's nuclear powers must be engaged to reaffirm international norms and help stem growing proliferation concerns.

The Secretary of Defense should direct that the next Nuclear Posture Review and its implementation be given priority within the Department by senior military and civilian leadership. We need a comprehensive assessment of nuclear issues and definition of specific actions related to:

- ***Offense.*** Developing plans, strategies, and resources for modernizing critical force elements.

- ***Defense.*** Rebalancing budgets and training to give greater attention to operational survivability in the face of nuclear attacks.
- ***People.*** Reestablishing valued career tracks for those with nuclear expertise.

We acknowledge and appreciate that this is a difficult topic, both because it is an area where emotions run high, and where irreversible damage won't be evident for a long time—but warning signs are already upon us from too many directions to ignore.

2 Maintain capability to project force around the world, to deter or defeat

...THE DEPENDENCE ON INFORMATION INFRASTRUCTURE ...COUPLED WITH THE TECHNICAL VULNERABILITY OF THAT INFRASTRUCTURE IS THE "ACHILLES HEEL" OF OUR CONVENTIONAL FORCES.

Our military and civilian information infrastructure is highly vulnerable

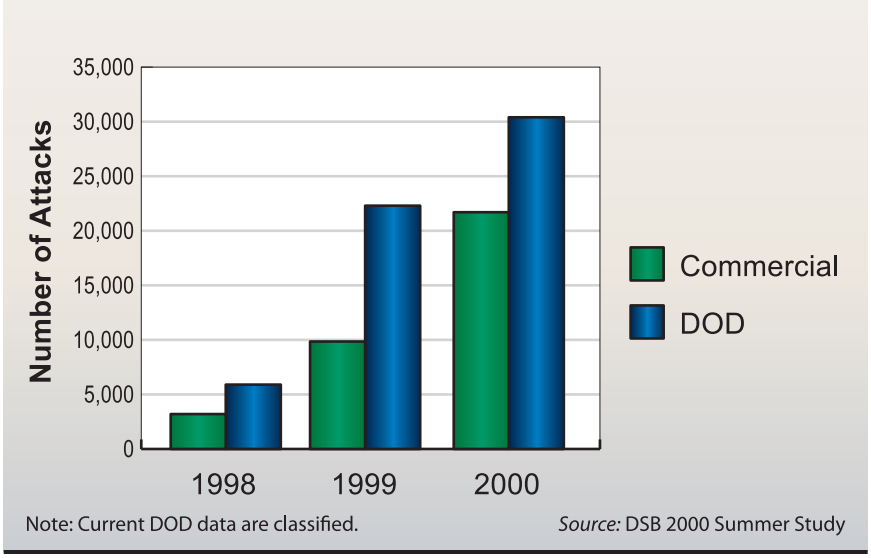
Our military forces depend on both military and civilian information infrastructure. Both are highly vulnerable. Irrespective of the nation's overwhelming military capabilities, the dependence on information infrastructure—sometimes called "net-centricity"—coupled with the technical vulnerability of that infrastructure is the "Achilles heel" of our conventional forces.

All of the nation's modern forces are increasingly dependent on accurate and timely information. The infrastructure that provides this information is subject to disruption and denial of service, to malicious modification of information, and to exploitation to learn our secrets. This infrastructure includes unique military radios, networks, satellites, and command and control facilities. It includes commercial communications and networks leased by DOD involving commercial satellites, terrestrial fiber, and transoceanic cables. It also includes critical data held by the defense industrial base and specific information technology embedded in individual weapon systems.

The options open to adversaries are many and varied. They can attack network systems and computers from afar, introduce malicious code or components during production—especially since much of the nation's software and hardware is produced abroad—and they can recruit insiders who can use their positions of trust for improper ends. Adversaries can jam our satellites, attack them with electromagnetic pulse (EMP), or target them with missiles in space or at their ground stations. They can sever undersea cables and land lines, or attack their terminals and switches.

There is growing awareness, and investment, but so far scant real progress on cyber security

There is increasing concern throughout the DOD about advanced cyber threats. Many studies are underway; budgets are being developed, evaluated, and amended; and organizations are being restructured. But there has been very little actual progress to date in terms of implementing cyber security improvements against advanced threats.



The number of cyber attacks is sharply rising, and these are only the ones we detect.

In simple terms our current cyber security strategy has been "perimeter defense"—placing a "fence" around our computers, weapon systems, or networks to keep out would-be penetrators.

It has been shown repeatedly that perimeter defenses can be defeated, sometimes by rather unsophisticated attacks and almost always by more advanced approaches. The United States has highly sophisticated experts, and when they have been asked to penetrate our own systems their record of success is 100 percent. While perimeter defenses can and should be improved, it is highly likely that our systems will continue to be vulnerable to well-financed and/or technically capable adversaries. As such, our strategy must be broadened.

Cyber security can never be perfect, but it can be much better

While improved policies, better training, and more long-term research are needed in cyber defense, the most important thing the Department could do now is accelerate implementation of near-term, well-understood measures to improve cyber defense. There is a cost for greater cyber security, but an even greater cost for not having it.

Immediate measures should include:

- More aggressive auditing of user activity on military networks to detect potential insider threats. This will

require use of automated tools and algorithms to sort out potentially suspicious activity.

- Acquiring critical hardware and software in a way that veils its intended destination and application in critical military systems.
- Much more frequent upgrades to hardware and software elements of critical systems and more variety in the commercial hardware and software purchased and employed.
- More comprehensive surveillance for potential data exfiltration—over the network, over-the-air transmission, and by physical means.
- A detailed and exercised back-up plan for how joint forces will adapt when the system is unavailable or its data corrupted. A demonstrated readiness to operate effectively in an information-degraded environment.
- A means to reconstitute the network using an independent communication path not associated with the compromised network.
- Encrypting all data stored in mobile devices.
- Minimizing the time between a decision to purchase commercial hardware and software and the time of delivery, to give an adversary less time to corrupt the new equipment.
- Removing unneeded functionality in our information systems—both in applications and operating systems. Every increment in functionality, every additional "feature," offers an adversary a new avenue for attack.
- Use of some government-produced elements in every critical system, so as to complicate an adversary's attack planning. Government-produced software and hardware is typically more expensive, but it can be produced in a secure environment.

The new administration should also pursue efforts that establish best practices for maintaining cyber security in the long run. The federal government is set to embark on the Comprehensive National Cybersecurity Initiative largely to enhance the security of the military and federal government information infrastructure. We believe the new administration should place the highest priority on

both supporting and extending this very significant effort. By "supporting" we mean not only ensuring full funding but also providing highly focused and frequent management attention to ensure that the agreed goals are actually met with the highest sense of urgency. By "extending" we mean moving even beyond the current impressive scope of the initiative to also include physical attacks as well as cyber attacks against information infrastructure; our space assets; better ways to purchase and operate the information infrastructure, in the first place; and encompassing the information infrastructure of the private sector industry segments—agriculture, manufacturing, finance, and transportation—upon which the entire country depends.

Furthermore, since our country's information infrastructure will never be invulnerable, we believe that all federal departments and agencies should regularly practice operating with degraded information infrastructure, much as the military regularly practices in preparation for combat. Practice makes perfect.

Our cyber vulnerability in space presents particular challenges

The surveillance, communication, and navigation services provided by space-based assets are a highly specialized, critical part of the military information infrastructure. Defending these assets presents some rather unique and costly long-term challenges. While many defensive measures will need to be taken over time, we recommend that improvements to space situational awareness be the immediate first step. Understanding what the threats to our space assets are, where they are, and what they may or may not do underlies all other defensive actions.

Be prepared for a long-term, rapidly evolving contest between defense and attack in cyber warfare

The steps above are only a start. Many more such improvements will be required. This area will need repeated cycles of testing, vulnerability identification, and application of additional defensive measures, drawing on new tools and techniques produced through research and development. The research and development burden will have to be carried in large part by the national security community since it is currently the primary target of advanced cyber threats.

DOD's business practices are having a long-term debilitating effect on our military forces

While vulnerabilities to cyber attacks are a clear and present danger to our military forces, cumbersome business practices within the Department of Defense present a long-term threat of gradual degradation—in effect, a self-inflicted wound. U.S. conventional forces are currently second to none, but the defense acquisition system is so slow that it continuously compromises our technology lead, and in effect extrapolates the past to the future. Inefficiencies in business practices—acquisition, logistics, and infrastructure—so significantly raise costs as to severely limit modernization and force structure, not only in terms of numbers but also affecting the balance among types of weapon systems in our arsenal. DOD is unable to acquire effective forces with efficiency and timeliness.

… CUMBERSOME BUSINESS PRACTICES WITHIN THE DEPARTMENT OF DEFENSE PRESENT A LONG-TERM THREAT OF GRADUAL DEGRADATION

Current DOD processes lack basic business discipline. Major programs regularly overrun their projected costs and schedules. Evidence of waste is everywhere. Logistics costs are excessive and still do not provide the agile, responsive support our forces need. The commercial sector routinely demonstrates profoundly better business practices.

The resource allocation and acquisition decision processes are highly bureaucratic and slow. The military is provided with materiel by a bureaucracy largely uninformed by or inattentive to the combatant commanders who are actually accountable for accomplishing missions—a bureaucracy that diffuses responsibility and avoids accountability.

The Department's excessively slow processes limit its ability to exploit current technology, much of it driven by the commercial sector—computers, software, the Internet, and microelectronics. The irony is that more agile adversaries may gain military and security advantages through purchase and fullest use of technology developed in the United States.

Having made the strategic decision to depend on information and network technologies as a core element of our

military force capability, the Department has not made the management changes necessary to fully implement this strategy. Current management practices remain primarily a product of the past—more attuned to acquiring vehicles than a future of using networks.

The globalization of technology and industry has changed the industrial base from which DOD must draw its capabilities. Leading edge technology needed by the military now comes not only from domestic firms but also from foreign and international ones. Yet, the Department does not have a clear concept for dealing with the new set of trade-offs created by this trend. Those trade-offs include superior performance, reliability, and price versus possible dependence and vulnerability of supply, or possible corruption of purchased microelectronics and software for purposes of cyber attacks. The tradeoffs also include the need to disclose the military's requirements, specifications, and priorities to foreign entities, and much more.

DOD's business practices need not be worse than the commercial sector's norm

There are commonplace tenets of good management practice that abound in the commercial sector. Without blazing any new trails in business processes, DOD's approach to acquisition, logistics, and infrastructure could be much improved. Importantly, we are recommending learning the lessons of commercial practices and not recommending universal, reflexive purchase of commercial products: sometimes commercial products will be what the military needs, and sometimes not.

We recommend that DOD have an authoritative business plan that will enforce discipline in the process of allocating resources to mission purposes: what is to be done, with what resources, and by what schedule. Business plans must state prioritized objectives—as it is difficult to accomplish an objective that has not been identified—persuasive strategies for accomplishing the objectives, and plans. They must also state tasks, schedules, expected costs, expected milestones along the way, and deliverables that employ the strategies to accomplish the objectives.

Responsibility and accountability for the various roles in building military force capability must not only be clearly spelled out, but also enforced. The responsibility for acquiring and maintaining military capabilities is vested in the armed services, in the defense agencies, and in the combatant commands around the world. Both providers and users must participate, with balance in their influence. This will require strengthening the role, participation, and influence of the combatant commands. They have the operational responsibility to employ all the armed forces as a joint team and should lead in the process of identifying their mission capability needs.

Our current business practice is to strictly adhere to rigid and overly precise so-called "requirements" even if they are later found to unrealistically elevate cost, slow schedule, or increase technical risk. The superior alternative is for accountable individuals to be informed by requirements, rather than allow requirements to dictate the process. A bureaucratic requirements process is no substitute for experienced judgment in dealing with developing technical challenges and changing operational needs.

"Spiral development' is an approach oftentimes employed in the private sector (and very occasionally within DOD) to develop new capabilities. It consists of repeatedly building, testing, improving, and ever increasing in scale—leading to large scale capabilities without monumental failures of cost, performance, or schedule along the way. In contrast, the typical DOD approach has been disparagingly nicknamed "requirements, delay, surprise." We suggest that spiral development become the norm for DOD, and that major new capabilities be developed in five years, not 20. DOD also needs an even more rapid management process for introducing limited capabilities to fielded military forces within two years, to better match the agility of our adversaries. In addition, a mechanism for the rapid insertion of new capabilities into forces engaged in operations should be developed.

Systems engineering capabilities within the services, agencies, and combatant commands need to be significantly

strengthened so DOD can be a "smart buyer" of products and services from industry as well as a "smart user" of these products and services. While there is tremendous benefit in temporarily hiring specialized engineering expertise from the private sector as needed, that is a poor substitute for having a foundation of expertise within the Department itself.

The most senior executives within DOD responsible for information, information systems and infrastructure, and networks must establish a better governance structure to manage development, configuration, interoperability, and operation of DOD's network structures. This will require strengthening the aforementioned systems engineering capabilities, and also defining clearer authorities, responsibilities, and accountability for decision making.

In the case of cyber attacks, discussed previously, it is worth noting that the nation's response to these attacks relies not only on advances in technology, but also on business practices that can be used to manage the acquisition and use of that technology in ways that mitigate attack. Particularly important is the development of concepts, plans, and governance processes for addressing the trade-offs between operational advantages and vulnerabilities of network centric strategies.

Given the essential role of logistics in military operations, the Defense Science Board has recommended the creation of a joint logistics command responsible for DOD's global end-to-end supply chain as a means of clarifying responsibilities and authorities for logistics support to mission effectiveness. "Unity of command" is as important to logistics as it is to combat.

Finally, DOD needs to create effective strategies for exploiting the globalized commercial industrial sector so as to effectively enable DOD's organizations.

In sum, all of these practices are "business as usual" for a well run, large, multinational corporation. DOD needs no less.

3 Bring stability to nations and regions

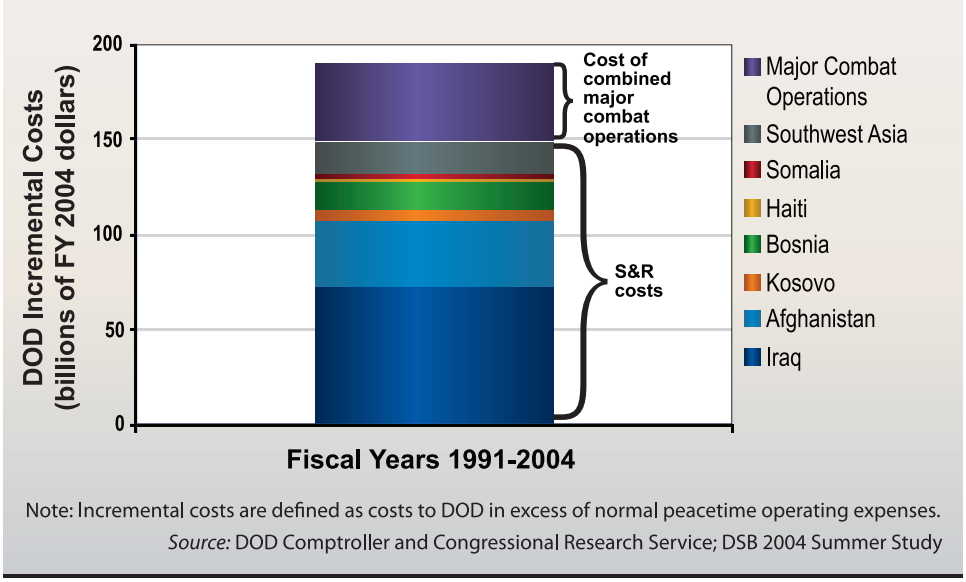
We lack robust plans and capabilities to support country-specific stability operations

America's armed forces are extremely capable of projecting force and achieving conventional military victory. Yet success in achieving U.S. political goals involves not only military success but also success in the stabilization and reconstruction operations that usually follow hostilities. Furthermore, better orchestration of all instruments of U.S. power in peacetime might obviate the need for many military excursions to achieve political objectives; or, failing that, at least better prepare us to achieve political objectives during stabilization and reconstruction operations.

...ORCHESTRATION OF ALL INSTRUMENTS OF U.S. POWER IN PEACETIME MIGHT OBVIATE THE NEED FOR MANY MILITARY EXCURSIONS TO ACHIEVE POLITICAL OBJECTIVES; OR … BETTER PREPARE US TO ACHIEVE POLITICAL OBJECTIVES DURING STABILIZATION AND RECONSTRUCTION OPERATIONS.

We engage in stability operations more frequently than combat operations and have engaged in foreign stability operations throughout our history—in 1847, for example, Major General Winfield Scott's forces occupied and administered Mexico City. While most combat operations are followed by stability operations, not all stability operations are preceded by combat operations, such as in response to the collapse of a failed state.

Stability operations are costly. Since the end of the Cold War, 80 percent of our supplemental funds for operations have been for stability operations. We have not yet learned to use technology to reduce the cost of stability operations as we have for combat operations, but technology has significantly amplified the capabilities of insurgents to disrupt U.S. operations. Since the end of the Cold War, the United States has begun new stabilization and reconstruction operations every 18 to 24 months. Since each operation typically lasts five to eight years, cumulative requirements for human resources can add up to three to five times what are needed for a single operation. History indicates that stabilization of relatively orderly societies, without ambitious goals, may require five troops per 1,000 indigenous people; while stabilization of disorderly societies, with ambitious goals involving lasting cultural change, may require 20 troops per 1,000 indigenous people.



Note: Incremental costs are defined as costs to DOD in excess of normal peacetime operating expenses.
Source: DOD Comptroller and Congressional Research Service; DSB 2004 Summer Study

Incremental costs for stability operations overshadow those for combat operations—by a factor of four between 1991 and 2004. That ratio is much higher now.

It is clear from our recent experiences in Afghanistan and Iraq that the United States must expect to encounter significant challenges in its future stabilization and reconstruction efforts—efforts that seek to ensure stability, democracy, human rights, and a productive economy in a nation of concern. Achieving these ends requires effective planning and preparations years before the outbreak of hostilities, as well as employment, in the period following hostilities, of capabilities that are not traditional to U.S. armed forces. Achieving these ends will also require sustained U.S. will, insofar as substantial resources will be required over long periods of time.

The United States can be more effective in meeting the challenges of the transition to and from hostilities, challenges which require better planning, new capabilities, and more personnel with a wider range of skills. Our vision for enhancing U.S. effectiveness in the transition to and from hostilities has two dimensions.

The first dimension is management discipline. We have great respect for the military services' approach to management, covering the full gamut of:

- personnel selection, training, education, and promotion
- planning, budgeting, and resource allocation
- exercises, games, modeling, and rehearsal
- performance and readiness measurement
- doctrine development

We believe this management discipline, now focused on combat operations, must be extended to peacetime activities, to stabilization and reconstruction operations, and to intelligence—not only within DOD, but across the government. With regard to intelligence, making use of this

management discipline, which has been effective in the employment of U.S. military capabilities for combat operations, could result in greater confidence in the intelligence, information, knowledge, and understanding that is needed for stabilization and reconstruction efforts to succeed.

The second dimension is building and maintaining certain fundamental capabilities, now lacking, that are critical to success in stabilization and reconstruction. While management discipline is essential, it will not, be effective in and of itself. It must be coupled with capabilities that are critical to preparing for and executing stabilization and reconstruction operations. These include:

- capabilities to aid in rebuilding civil society
- strategic communication
- knowledge, understanding, and intelligence of countries of interest
- identification, location, and tracking for asymmetric warfare

These capabilities, without the management schema, would lack orchestration and be employed ineffectively; the management schema without the capabilities would be impotent.

We can achieve better direction, planning, and oversight

We believe a new coordination and integration mechanism is needed to bring management discipline to the continuum of peacetime, combat, and stabilization and reconstruction operations. For countries where there is a high probability of U.S. intervention, the President should direct the initiation of a robust planning process through the National Security Advisor, with the National Security Council. The elements of that process must include:

- ***Contingency planning and integration task forces.*** Full-time activities that could continue for months or years; staffed by individuals from all involved agencies, who have deep expertise in the countries of interest and in needed functional areas.
- ***Joint interagency task forces.*** Composed of senior government executives and military officers who operate

within a particular country or area of interest, these task forces should be created to ensure coordination and integration of the activities of all U.S. players "in-country."

- ***A national center for contingency support.*** A federally funded research and development center with country and functional expertise to support the contingency planning and integration task forces and the joint interagency task forces. The center would augment skills and expertise of the government task forces, provide a broad range of in-depth capability, support the planning process, and provide the necessary continuity.
- ***A focal point at each regional combatant command for stabilization and reconstruction planning and execution.*** The most likely candidate for this role is the combined/joint forces land component commander.

The process should be codified in a presidential directive. While this government-wide process is being put in place, DOD should move swiftly to address its own role in that process and to strengthen its capabilities, which in the interim would provide tremendous benefit to the nation. In addition, DOD should actively support the development of core competencies in planning in other departments and agencies—principally the Department of State.

In fact DOD Directive 3000.05 dated 28 November 2005 is well composed to do just that: ensure transformation within DOD to more effectively conduct stability operations. The implementation of that directive was comprehensively reviewed in August 2006; to quote the Deputy Secretary of Defense on that review "much remains to be done." In fairness, the Department has been highly focused on achieving success in Afghanistan and Iraq. The irony, however, is that the substantial resources focused on these current stability operations is compromising our ability to successfully prepare for stability operations in the future.

Stronger stabilization and reconstruction capabilities are needed and achievable

DOD and the Department of State need to make stabilization and reconstruction missions a core competency. Success in these missions depends on a stronger partnership and closer working relationship between the two depart-

ments. Moreover, both departments need to augment their existing capabilities for stabilization and reconstruction.

Stabilization and reconstruction operations are not a so-called lesser-included task of a combat mission, but a separate and distinct mission with some unique requirements for organizing, manning, equipping, and training. Thus, stabilization and reconstruction requirements should become a major driver for the future force. We recommend a number of actions that will help bring appropriate attention to stabilization and reconstruction operations:

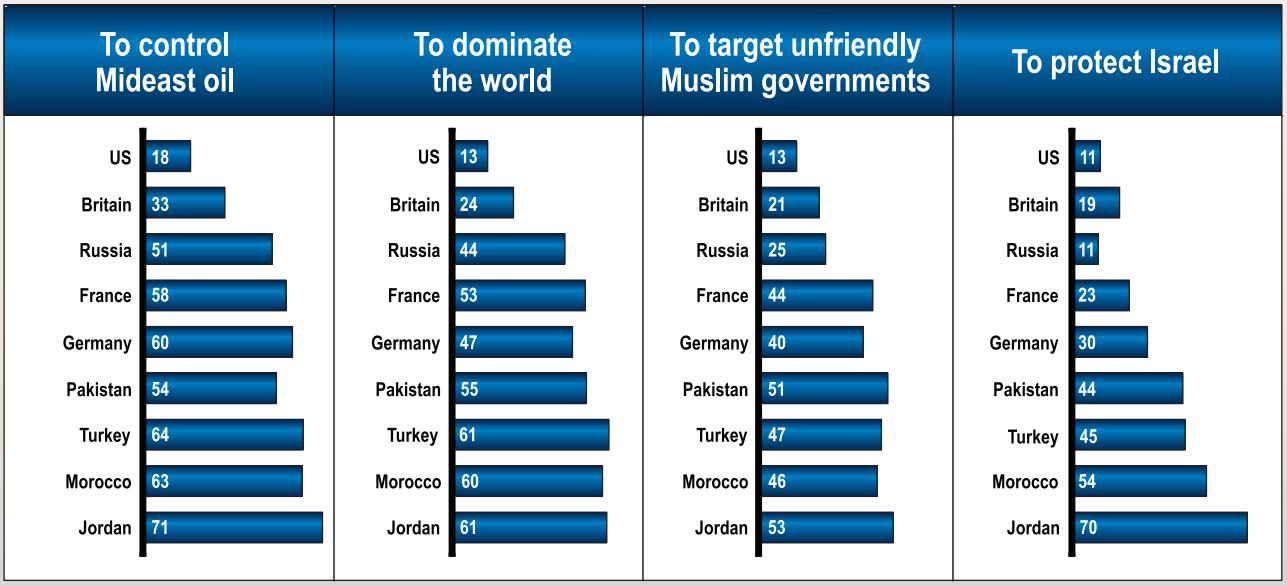
- Stabilization and reconstruction plans should be fully integrated with combatant commander operational plans for combat, not treated as an annex or "afterthought" to those plans.
- The Army should accelerate restructuring its National Guard and Reserve forces with an emphasis on modular capability for the stabilization mission. In particular, the military services need to recruit more senior professionals into the reserves with the requisite skills and experience for civil affairs—such as local government, civil infrastructure, and private sector finance. This would contribute to
  - restoring and maintaining public order
  - safeguarding, mobilizing, and using local resources
  - facilitating the equitable distribution of humanitarian supplies and services
  - ensuring essential civil services
- We also need to more effectively exploit our "fifth force provider" (in addition to the four military services), namely the private sector. The private sector provides enormous and effective services for stability operations; witness the tens of thousands of contractor personnel in Iraq. It also provides essential skills that DOD understandably lacks, such as the operation of urban infrastructure. Employing the indigenous private sector provides the double benefit of the services themselves and local economic well-being promoting stability. The combatant commanders' portfolio of contingency plans for stability operations should fully take participation of the private sector into account.

- Stabilization and reconstruction should become a core competency of general purpose forces through training, leader development, doctrine development, and other tools DOD applies to combat missions.
- The service secretaries and Joint Chiefs of Staff should integrate stabilization and reconstruction operations into the services' professional military education programs. The curriculums of service schools and joint military colleges and universities should include understanding of cultural, regional, ideological, and economic concerns. Participation by students from other agencies and departments should be increased.
- Stabilization and reconstruction operations should also be integrated into premier training events and exercises at every level.
- U.S. Joint Forces Command should further develop, publish, and refine joint doctrine for stability and reconstruction operations.

Strategic communication of U.S. intentions and values is critical for stability operations

Strategic communication—which encompasses public affairs, public diplomacy, international broadcasting, information operations, and special activities—is vital to America's national security and foreign policy. Over the past few decades, the strategic communication environment and requirements have changed considerably as a result of many influences. A rise in anti-American attitudes around the world, the use of terrorism as a framework for national security issues, and the volatility of Islamic internal and external struggles over values, identity, and change have all contributed to this transformation.

Furthermore, strategic communication has been affected by changes in the information environment—information saturation and global transparency created by satellite TV (and thus fast-breaking news) as well as a host of other inexpensive and widely available information technologies, such as cell phones, wireless handhelds, high-resolution commercial space imaging, e-mail, the Internet, and blogging. These factors give even greater importance



Note: Questions asked of those who believe the war on terrorism is not a sincere effort, or have mixed views. Percentages show the percent of the total population who believe each is an important reason the US is conducting the war on terrorism.

Source: Pew Global Attitudes Project; DSB 2007 Summer Study

America's motives and intentions are sometimes misunderstood by countries around the world.

to the credibility, reputation, and "brands" of information providers, including governmental ones.

Since September 11, 2001, the United States has taken steps to improve strategic communication. Examples include the Coalition Information Center created in the White House, high-ranking officials devoting personal time to advocating policies and shaping perceptions, international broadcasting, and embedded media are examples. But these steps are not sufficient. The U.S. government needs a strategic communication capability that is planned and directed in the nation's interest. Missing today are:

- strong leadership
- strategic direction
- adequate coordination
- effective research
- sufficient resources
- adequate exploitation of commercial capabilities
- a culture of measurement and evaluation

A unifying presidential vision and broad bipartisan congressional support are critical. The President should issue a directive to strengthen the U.S. government's ability to

- understand global public opinion
- advise on the strategic communication implications of policy making
- communicate with global audiences
- coordinate all components of strategic communication
- provide a foundation for new legislation on its planning, coordination, conduct, and funding

Changes in the Departments of State and Defense will be needed to support and implement a presidential vision on strategic communication.

DOD should work with the Department of State and with Congress to establish an independent, not-for-profit organization as the focal point to engage experts and thought leaders from the private sector and civil society in support of our government-coordinated and executed strategic communication activities. This organization would perform comprehensive research and analysis on cultural understanding, languages, and communications technologies. It would also engage the private sector in program development.

Stabilization and reconstruction operations require improved knowledge, understanding, and intelligence

The knowledge required to effectively conduct stabilization and reconstruction operations is different from the military knowledge required to prevail during hostilities, but no less important. Knowledge of a nation's security interests and external relations, armed forces, the local political scene, security, and internal social, cultural, and economic conditions are as important to stability operations as is the knowledge of the enemy order of battle during hostilities. DOD and the military services must treat acquiring knowledge of culture and developing language skills as seriously as learning combat skills: all are needed to successfully achieve U.S. political and military objectives.

But collecting, compiling, and sustaining cultural knowledge, as well as developing linguistic competency in a wide array of languages, requires a long-term effort and attention span, not the short-term focus that is typical of those who use and collect information and intelligence today. The collection, analysis, and integration must be conducted

far in advance of DOD's need. Much of the information is unclassified and available from open, albeit sometimes obscure, sources. A new approach is needed to establish systematic ways to access and coordinate the vast amount of knowledge available both within and outside DOD.

The combatant commanders urgently need to develop intelligence plans as a required element of their adaptive planning process. These plans must be realistic for satisfying information needs for peacetime, combat, and stabilization and reconstruction (including support to other departments and agencies). The development of these "intelligence campaign plans" will provide a disciplined process for planners and operators to specify what knowledge they need to achieve their objectives, and for intelligence organizations to assess whether they possess or can provide that knowledge.

DEVELOPING THE CAPABILITIES DESCRIBED HEREIN REQUIRES PREPARATION YEARS IN ADVANCE. THE UNITED STATES CANNOT SUCCEED AT THE LAST MINUTE...

Language and cultural understanding skills are key enablers of country and area knowledge. Today, DOD lacks sufficient personnel with the language skills and cultural understanding required for countries likely to be of future interest.

Finally, open sources can provide much of the information needed to support peacetime needs and stabilization and reconstruction. Open source information can be used to develop a broad range of products for stabilization and reconstruction operations—such as genealogical trees, electricity generation and electric power grid maps, cultural materials in support of strategic communication plans, and background information for noncombatant evacuation operations.

Developing the capabilities described herein requires preparation years in advance. The United States cannot succeed at the last minute and trying to do so significantly raises costs in any event. Coordination, the traditional interagency currency in the government, is necessary but insufficient for effective orchestration and success. Strong capabilities are also required.

4 Thwart terrorism and bring terrorists to justice—anytime and anywhere

...SHARING HELPS, COLLABORATION HELPS, ORGANIZATIONAL REARRANGEMENTS SOMETIME HELP. BUT IF WE ARE INFORMATION POOR TO START WITH, THAT FACTOR HAS TO BE ADDRESSED OR NONE OF THESE OTHER THINGS MATTER.

We lack the deep penetration required for actionable intelligence—both foreign and domestic

The limiting factor in thwarting terrorists is learning their identity and location. Terrorists have gotten better at their tradecraft—they are harder to detect and more lethal. In turn, we are spending a considerable amount on intelligence overall, and many intelligence community efforts have been redirected toward terrorism. Despite concerted efforts, we still lack the deep penetration required for actionable intelligence—both foreign and domestic.

Developing intelligence regarding terrorists is both difficult and different

The number one issue in counterterrorism is that we are information limited. Many nostrums for improving intelligence in support of counterterrorism focus on "connecting the dots" on the presumption that we have all the dots. We do not, nor are we sufficiently astute and aggressive in collecting them.

Sharing helps, collaboration helps, organizational rearrangements sometime help. But if we are information poor to start with, that factor has to be addressed or none of these other things matter.

The all-too-popular view that we have all the information we need but just need to process and share it better is patently and dangerously wrong in the case of counterterrorism.

There are significant differences between intelligence as practiced successfully in the Cold War and intelligence relevant to today's terrorism threat:

- Adversaries are not well known. Focusing efforts and intelligence collection and analysis capabilities is more difficult.
- The familiar geographic boundaries are gone. Monitoring and searching must now be done globally.
- Weapons and destructive capabilities of adversaries are not likely to be known with sufficient precision, which makes it necessary to plan for "worst case" scenarios.
- The familiar "indications and warnings" are not very useful; still, effective new ones have not been developed.
- Terrorists and their accoutrements and activities are moving targets with small footprints. Small, diversified, and distributed, they blend in with benign civilian activities.
- Acquiring usable information against moving targets requires "persistent" collection, to which the intelligence community has come late and haltingly, with an imperfect understanding of why persistence is needed.

To oversimplify slightly, there are three threads we can pull to unravel the terrorist web. We can follow terrorists and their supporters; we can follow the equipment, materials, and money that terrorists need; and/or we can start with their likely targets and work backward from there.

- Equipment, materials—CBRNE (chemical, biological, radiological, nuclear, high explosive) and precursors thereof—and money can be tracked with some effort. Rarer, scarcer items of limited origin may be easier to follow. So, too, may electronic transfer of funds and other vital information. However, tracking people, material, or transactions will never be foolproof and cannot be the only mechanism employed.
- Terrorists and their supporters are motivated, recruited, and trained, and therefore offer intelligence observables. Individuals with special skills have certain notoriety. Terrorists and their supporters talk to one another and network/link analyses are especially productive.
- Targets can be iconic, critical infrastructure nodes, or simply concentrations of people to run up the casualty tally. Vulnerability analyses can suggest attack vectors and observation can reveal "casing" and other preparation activities.

The Intelligence Community, together with its consumers, should define, design, and implement a true "collection architecture." This architecture should reflect the transition in emphasis from largely fixed installations to people and activities "hiding in plain sight," requiring "persistence" and orchestrating use of all of the powerful tools available to the community. More than ever collection needs to be close-in, intrusive, and covert, and must achieve deep penetration.

Domestic intelligence must be on par with foreign intelligence

A shift away from state-sponsored terrorism as well as the potential for terrorist activities within the U.S. proper challenges intelligence—both domestic and foreign in concert—in support of securing the homeland.

- Threats are more loosely networked, less bureaucratic, less visible and, thus, less knowable.
- They may be homegrown, perhaps connected with foreign terrorists or perhaps just inspired by foreign terrorists, which presents domestic intelligence collection concerns.
- Fund-raising may be local and diversified, either within the United States or abroad.
- Materiel for terrorists' weapons may be acquired within the United States, thus avoiding border scrutiny.
- Their acts may be harder to deter because there may be little we can "hold at risk" if there is no attributable state sponsor.

In an earlier era, when state-sponsored terrorism represented the only serious threat, most U.S. intelligence efforts were focused on, and prosecuted in, other countries. Inimical foreign states recruited, motivated, and trained the terrorists; provided materiel support; and designated targets. In a curious sense, this helped our intelligence efforts.

The apparatus of state-sponsored terrorism, while a guarded secret, is generally professional and coherent. It could be understood, in part, because it was comparatively large, likely bureaucratic, and relatively stable over time.

As such, it may prove a malleable intelligence target. That is, state-sponsored terrorism, in one form or another, has a knowable structure along many dimensions.

Homegrown, indigenous, and/or locally nourished terrorism presents additional challenges. While the ideology may be global, the recruitment, planning, and execution may be local.

- We demonstrate a preference for treating terrorism at home as a law enforcement issue, requiring a criminal predicate before collecting information, versus anticipatory intelligence gathering.
- Excepting nuclear weapons, most weapons of mass destruction/disruption are locally available or producible and need not be imported across a scrutinized national border. Hazardous materials are located throughout the United States.
- Expertise and information on WMD is available in our institutions of higher learning and in our advanced industrial base. There is no practical and desirable way to change that.
- There is no shortage of attractive targets—economic, iconic, and defense—and frequent mass convocations.
- The availability of disaffected potential recruits may be growing, particularly as our prison population grows. "Self-radicalization" is particularly worrisome.

Broadening the scope of intelligence activities to include domestic intelligence involves the Department of Homeland Security, which is a new cabinet office, a new member of the Intelligence Community, and a new partner for the Department of Defense. This presents a challenge and an opportunity.

The creation of the Director of National Intelligence responded, in part, to the September 11 attacks against our homeland and placed domestic as well as foreign intelligence within the purview of a single individual. Notwithstanding, the successive directors of national intelligence have been slow to embrace domestic intelligence and that must be remedied.

...THE DIRECTOR OF NATIONAL INTELLIGENCE MUST HARMONIZE FOREIGN AND DOMESTIC INTELLIGENCE, AND EMBRACE THE LATTER, SO THAT SOMETIME IN THE FUTURE THE U.S. DOES NOT BECOME AN OVERLY SAFE HAVEN FOR TERRORISTS.

The Secretary of Defense and the Director of National Intelligence should bridge the schisms between military intelligence and civilian, between national strategic and theater-tactical-operational intelligence. The Defense Human Intelligence service must complete its upgrade and professionalization. In turn, the Director of National Intelligence must harmonize foreign and domestic intelligence, and embrace the latter, so that sometime in the future the U.S. does not become an overly safe haven for terrorists. We believe that all this is possible, and essential, while at the same time preserving the freedoms and rights of U.S. citizens at home and abroad.

The management discipline that serves us well in preparing for combat can help in preparing actionable intelligence.

The Defense Science Board has observed that rooting intelligence activities more firmly in military operations requires a certain management discipline, referred to as "intelligence campaign planning"—conveying important improvements.

- Combatant commanders should develop intelligence plans as a required element of their adaptive planning process—plans that include realistic collection and exploitation for timely delivery of actionable information; and assessments of our intelligence readiness as we now assess our combat readiness.
- These intelligence campaign plans should cover the ineluctably intertwined nature of counterterrorism, combat, and stabilization and reconstruction, including counter-insurgency operations.
- These intelligence campaign plans should be exercised and evaluated, noting that if the intelligence plans are not executable, then the operational plans are not either.

Open sources are a valuable tool for terrorist information

The Defense Science Board, every commission, and every observer and critic of the Intelligence Community have pointed out the value of open source materials and the

relatively efficient, low-risk acquisition attendant on these materials. Notwithstanding, the Intelligence Community retains a propensity to undervalue and shortchange this intelligence collection discipline.

Understanding ideologically motivated terrorists—by far the majority, to include Radical Islam—means understanding their ideology. They are keen to publish, to motivate their ranks, proselytize to swell their ranks, and to put their enemies on notice.

Much of what we know about terrorist groups comes from open sources. Much of what we do not now know and need to know is to be found in open sources. Notwithstanding, acquisition and analysis today is insufficient. There remains considerable opportunity for investment—at bargain prices, compared to other intelligence disciplines, and proven effective.

In a related area, we have learned the value of "mapping the human terrain." Open sources can be quite useful here, too. But we have yet to fully exploit theses opportunities. This will not be a substitute for on-the-ground experience, but it can inform those operators. The Intelligence Community and the military departments must continue to improve their language and cultural knowledge and accelerate efforts to "map the human terrain," not just in today's hotspots but more globally, recognizing that terrorism flourishes—on purpose—where and when we are not looking.

The rosy bottom line for exploiting open sources is that terrorists are making more and more use of open sources, especially as electronic media reach ever-larger audiences and the barriers to entry in publishing continue to fall dramatically—blogs need neither printing plant nor transmission tower. The increasing value of open source intelligence stands in contrast to other collection disciplines, where adapting terrorists continue to improve their tradecraft.

5 Support state and local authorities in providing domestic catastrophe relief

… THE RESPONSE TO HURRICANE KATRINA INVOLVED AS MANY DOD PERSONNEL AS THE ENTIRE ARMED FORCES OF THE UNITED KINGDOM.

The nation lacks validated operational contingency plans to respond to domestic catastrophes—whether natural or malicious

DOD is the main resource for the U.S. national response to domestic disasters, natural or malicious, because it is the governmental organization with by far the largest standing contingency capability. The past fifteen years have seen several national emergencies in which DOD has played a major role in response. For example, the response to Hurricane Katrina involved as many DOD personnel as the entire armed forces of the United Kingdom. But it is also the case that the combined local, state, and federal response was hampered by lack of planning preparation, confused chains of command, incompatible communications, and lack of coordination.

Additionally, the United States faces a new threat to the homeland which could extend beyond historic proportions—a campaign of repeated distributed, asymmetrical attacks from terrorists or foreign powers. Insofar as the response to such an incident becomes a federal responsibility, DOD will surely be called upon.

The nation is unprepared to cope with such an event.

There is a rising threat of homeland attack

The United States can no longer think of war as an "away game." Capable adversaries will execute "one game," wars attacking U.S. interests wherever the nation is most vulnerable, including the homeland. Potential aggressor states and non-state actors alike have noted that the most lucrative approach to war with the United States could well be outside the U.S. moral framework. Our homeland is vulnerable.

Adversaries may reason that asymmetric attacks could:

- Deter U.S. entry into foreign affairs of little or no publicly perceived national security impact or threat, and also divide U.S. forces and leadership attention between foreign and homeland concerns.
- Halt or impede U.S. operations at home or abroad by threatening those elements of the military deployment, logistics, and supply chain located within the United States.
- Impede the nation's ability to project force by executing a wide range of information operations—such as cyber attacks with effect in the United States and possibly originating in the United States—which are difficult to trace, and could delay or diffuse the national process of committing to war.

Missiles Manufactured in Tucson, Arizona

- AIM-9X
- AMRAAM
- EKV (Exo-atmospheric Kill Vehicle for the BMD system)
- ESSM (Evolved Sea Sparrow)
- Javelin
- Maverick
- Phalanx
- Phoenix
- RAM
- Sparrow
- Standard Missile
- Stinger
- TOW (anti-tank missile)
- Tomahawk

Source: DSB 2003 Summer Study

Disrupting even a single defense contractor's operations could significantly hinder combat operations abroad.

Attacks on the U.S. homeland (except by strategic weapons such as ballistic missiles and bombers) have been unthinkable for a long time. Today's national political and military leadership have difficulty embracing the concept and operations of a two-front war, with a homeland battlefield.

America's air and sea power make a conventional mass invasion improbable, but scattered attacks on installations, infrastructure, and people, and their consequent domestic disruptions, are more likely and could be attractive to an adversary. Asymmetric attacks, targeted to achieve particular effects, so successfully used by U.S. forces to inflict maximum impact on America's foes with minimum force, are also useful to aggressors. Such attacks can distract the U.S. populace; disrupt infrastructures, commerce, and government; and also hamper

support to U.S. forces operating abroad—using limited, focused efforts.

The U.S. homeland could be subject to multiple attacks (such as from improvised explosive devices (IEDs), suicide bombers, or sniper attacks), WMD (real or threatened), civil disruption, and infrastructure and network attacks. The military consequences of such acts could be severe. The civilian impact can only be imagined, but would be of major importance.

Effective national readiness to respond to attack will have an impact on a would-be attacker's decision to act—in effect serving as a deterrent. To a large extent, effective national readiness also addresses our ability to respond to domestic catastrophes such as natural disasters, since in most instances natural calamities will be of lesser magnitude. Many attacks on our homeland by terrorists or foreign powers can be significantly more deadly and dangerous than Hurricane Katrina.

Homeland disasters and attacks will exceed expectations and preparations

The Defense Science Board has characterized domestic catastrophes and homeland assaults on a scale and scope beyond those of isolated terrorist incidents (the kinds of incidents that led to the creation of the Department of Homeland Security). These studies envision cascading incidents in the homeland, at multiple points, approximately simultaneously.

In the case of homeland attack, incidents conducted by an attacker with a high degree of planning and resources likely will be on a scale beyond that anticipated in current homeland security and homeland defense plans. The openness of American society, its size, the geographical extent of its infrastructure and its diversity makes it practically impossible to avoid all disasters, natural or manmade. In its homeland roles, DOD will have to divide its attention and resources between protecting the homeland from natural catastrophes and homeland attacks, and prosecuting forward offensive operations against the adversary.

Specific catastrophes in the U.S. homeland cannot be precisely predicted: surprise should be an expected element. Dealing with the consequences of disaster(s) will have as much or more to do with addressing common issues as with the specific nature or cause of the attack. Anticipated incidents could threaten the breakdown of orderly society, brought about by:

- Failure of critical infrastructure, resulting in a lack of essential goods and services, such as electric power, food, water and sewer, medical services, transportation, oil and gas production, delivery and storage, banking and finance, information and communications, government services, police and fire departments.
- Professional resources, sized to handle only one or two crises at a time, are insufficient to respond to multiple catastrophes—resources such as the Federal Bureau of Investigation (FBI), National Guard, DOD, DHS, police, fire, medical personnel, the American Red Cross and others.
- Public anger manifested through misguided, vigilante-style attacks.
- Impaired ability of national, state, and local governments to govern due to a lack of, or confusing communications, and insufficient, disorganized emergency response.

Without adequate preparedness at all levels of government, across the private sector, and among the populace, post-incident results could be truly catastrophic and could include:

- ***Flight and refugees.*** Remaining in place could be untenable for many people for actual or perceived reasons.
- ***Breakdown of mutual aid agreements.*** National Guard, first responder, and medical communities rely on mutual aid to cope with large-scale emergencies. Under attack, however, leaders in unaffected areas may elect to conserve local resources and opt not to support mutual aid agreements.
- ***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 in confinement.
- ***Hoarding.*** The rush to amass excess goods after the attack.
- ***"Shoot your neighbor."*** As people perceive civil order deteriorating, they will escalate the force they use to protect home and family from interlopers.
- ***Rampant rumors.*** Media will propagate messages from many sources without confirmation.
- ***Population center "meltdowns."*** Many U.S. population centers are located where life without infrastructure services is difficult to sustain—the desert southwest in summer and northern cities in winter, for example.

American society has evolved to depend on "just-in-time," centrally managed networks of water, power, food, fuel, health care, communications, and transportation leaving the United States extremely vulnerable to carefully targeted and planned attacks. Over time, the 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. Many people today do not know their neighbors, let alone have the capability or capacity to form effective support networks for long periods of time. This is particularly true in large population centers, which may be the most vulnerable and thus the most attractive targets. Skepticism of authority makes governing in a disaster difficult, while the public expects governmental assistance to mitigate the aftermath.

Preparing to protect the homeland is everyone's job

The United States is a "soft" target, whether for natural disasters or for malicious attacks. Americans have become increasingly conditioned to assume disaster relief will come from communities and that state and federal resources will always be available. In the case of widespread natural disaster (e.g., a serious West Coast earthquake) or serious homeland attack, however, governmental resources will be overwhelmed. It could take days or longer for national resources to respond to a large-scale distributed attack or other major event.

As a result, hardening the U.S. homeland must be carried out on several levels, starting with individual families. All layers, however, must see themselves as part of a single, national team. A culture of preparedness on each level will significantly reduce the consequences of attacks on the homeland.

Individual preparedness will be invaluable, though difficult to inspire

Instilling a culture of individual and family preparedness within society at large can provide both physical and psychological benefits to individuals and families. Greater hazard awareness, training, home storage of relief supplies, and family communication and evacuation plans reduce the likelihood that families must rely on the emergency relief structure immediately following an emergency. Further, families prepared to hunker down for some time will be less likely to flee unnecessarily. Family preparedness is the fastest, least costly, most dispersed form of coping with a disaster.

The best place to begin infusing a culture of preparedness is with military dependent families living on or near military bases, as well as the families of first responders. As these families move within society at large they will help promote readiness thinking in the larger community. Additionally, soldiers, sailors, and airmen on duty away from their families and first responders will be more reassured by knowledge of their families' resilience. As a group of noncommissioned officers told the Defense Science Board, "We can't protect our country if we can't protect ourselves." The same applies to civilian first responders.

Local and state responders are on the front line

Local and state first responders are the leading edge contending with emergencies. While most are professionals, many are volunteers (especially fire personnel). DHS has in place programs to encourage local auxiliary police, fire, and medical cadres to augment professional response, however much more remains to be done.

The National Guard is everyone's main resource—and that's the problem

The National Guard is the backbone of state emergency response. The Guard has plans and resources in place, as an arm of state government, to respond to state emergencies and, through mutual aid agreements, regional emergencies. Many members of the National Guard, however, are also local first responders or in critical positions in the private sector. Further, National Guard troops are critical elements of deployed combat forces abroad and may not be available in case of emergencies at home. Conditions and extent of federalization of National Guard forces for domestic disasters are not well established. Double- or triple-counting people available for local, state, and federal service is an under-appreciated weak point in U.S. disaster response plans.

The private sector must become first responders, along with government

Private companies own or operate most national infrastructure. They have the best expertise for restoring services in times of crisis. Yet private industries (e.g., railroads, electric power utilities, communications providers, trucking firms) have not been accepted by the federal government as true disaster-response partners. Private infrastructure firms and industry associations have been denied appropriate, useful intelligence that could be used to defend against infrastructure attacks. Further, the cost of being prepared to respond is usually not justifiable in running a business with a bottom line.

The private companies and industry associations responsible for infrastructures critical to the functioning of government and American society must be embraced as full partners with all levels of government in anticipating and responding to domestic catastrophes. Keeping private infrastructure operators at arm's length from governmental planning, intelligence, and response is not in the national interest.

In turn, the incentives, limited liability, immunity, and waivers must be in place to make it sensible for private companies to prepare to be first responders.

The federal government, particularly DOD, has by far the greatest resources

In their early stages, attacks on the homeland may be mistaken for isolated terrorist incidents, natural disasters, or local emergencies to be addressed with the Department of Homeland Security or local authorities in the lead. As the true nature of a concatenated attack or natural catastrophe reveals itself, with DOD playing an increasing role, the President is authorized by law to transfer leadership responsibility for response and consequence management to DOD. Emphasis switches to actions that could be described as "war within the homeland." The U.S. Northern Command Homeland Defense Plan outlines a robust range of actions within the continental United States ranging from threat deterrence and support for civilian law enforcement to contingencies for escalation to the severe end of the scale—"decisive operations."

DOD has applied inadequate attention and resources to its homeland missions and plans. The transfer of leadership and responsibility from civilian agencies to DOD, as our understanding of an incident escalates and as ordered by the President, is a significant discontinuity in our national planning. Roles and missions are not well understood throughout the chain of command. Portions of the Homeland Defense Plan have not been integrated and coordinated with appropriate agencies and government actors. DOD does not know with certainty what is expected of it and the homeland security community does not know what to expect from DOD. The transfer of leadership and responsibility from one group of agencies to another is not well understood.

National response plans and exercises should be taken as seriously as the military services take plans and exercises for combat

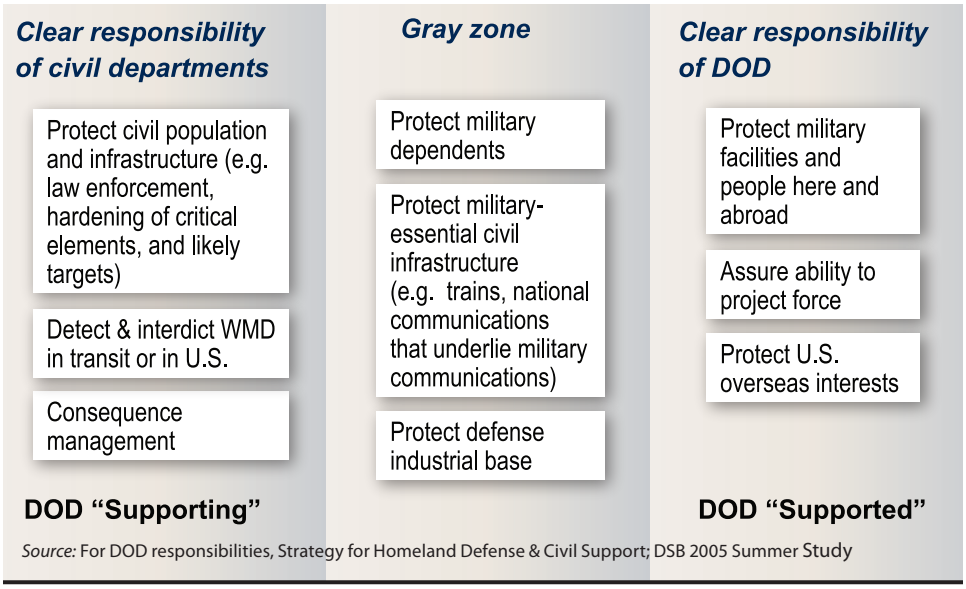
While doctrine and operational plans for homeland emergencies exist, with processes in place for review and revision, realistic exercise and evaluation of these plans is lacking. There are many exercises, but they are not effective—often more broad than deep, top-down with little bottom-up contribution, and stopped before difficult issues of transfer of command or interagency conflict arise.

They are highly canned and scripted; unknowns (such as public panic) and surprises do not come into play, though they should. Further, some exercises (such as Northern Command's Ardent Sentry) appear to have been designed to avoid difficult interagency interactions.

More worrisome than the disjointed nature of plans and exercises is the lack of any effective process for learning based on exercise experience. Observations are made during exercises, but there are no mechanisms to promulgate lessons throughout the many organizations involved. Lessons are taught, but lessons are not learned.

Welding the disparate elements of the single, national disaster preparation and response team—that may draw on state, local, and federal authorities as well as the private sector—into a closely coordinated whole relies on agreed-upon contingency plans, validated by meaningful, top-to-bottom exercises with rigorous follow up on lessons learned.

Realistic, objective-based planning and exercises are essential to an effective response to disasters, whether natural or malicious. These plans and exercises should embrace specific action plans at all levels of the national team, including state and local authorities and the private sector, for ameliorating effects of anticipated catastrophes. Resources called upon must be in place, verified and committed, not just imagined. Roles of each layer of the team must be agreed to and practiced; the decisions likely to confront leaders at all levels should be considered and practiced as well. Surprises should pervade exercises and not be excuses for halting or redefining the program. Thoroughly finding and fixing the



Responsibility and authority for mitigation and recovery are not always clear. Confusion can impede response with disastrous results.

flaws and gaps within plans through exercising is the only way, short of an actual catastrophe, to validate plans and to strengthen the informal networks among people at all levels needed for effective response.

Preparing for homeland catastrophe on a national scale is a clear responsibility of federal government, not instead of, but in addition to, preparation on a state and local level. DHS and DOD each have extensive activities in this area, but they are, for the most part, uncoordinated and lack validation. Leadership in assembling and exercising the national disaster response team, which must orchestrate preparedness among states and municipalities, can only be provided from the national level.

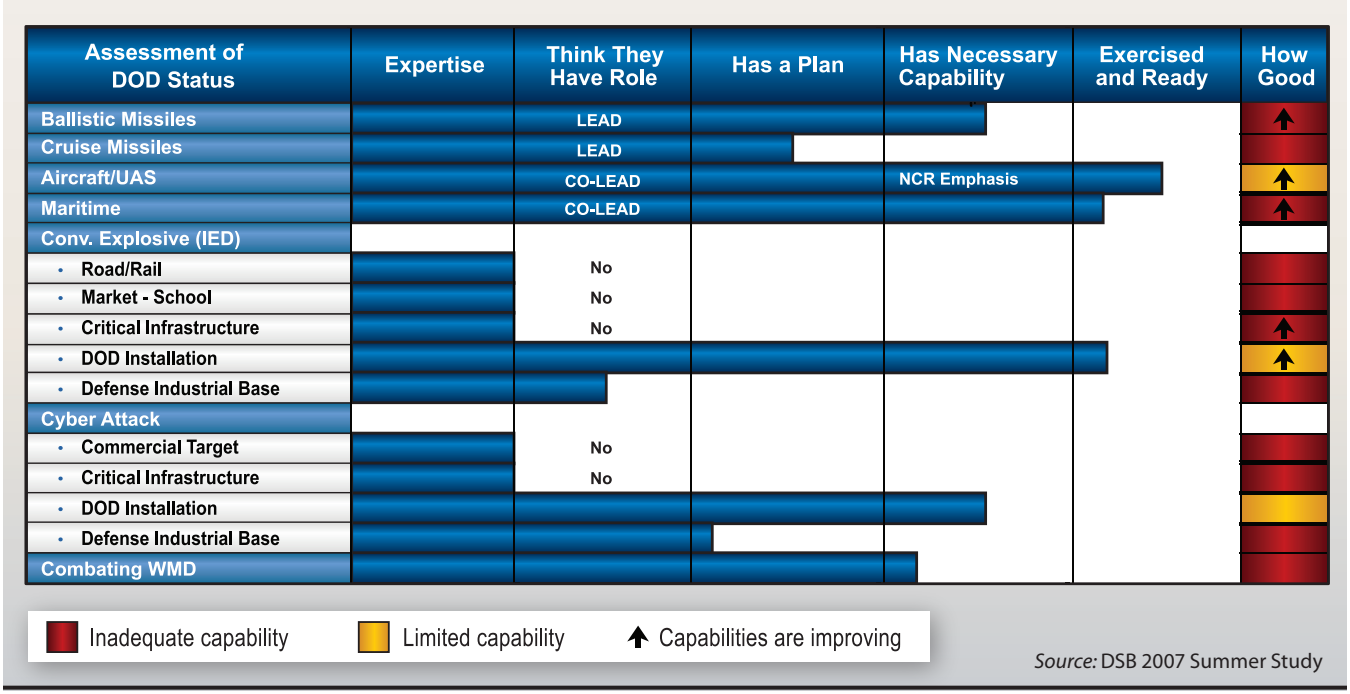
DOD must raise its level of readiness to provide domestic catastrophe support

DOD, which has most of the skill, equipment, materiel, and leadership required to address national emergencies, will be called upon to address most significant crises. Its role depends on the nature of the emergency:

- ***Homeland security.*** DOD can be called upon to support DHS and the Attorney General to prevent and reduce vulnerability to attack, and minimize damage and recovery from attack.
- ***Defense support to civil authorities.*** DOD can provide support for domestic emergencies and for designated law enforcement and other activities as directed by the President or Secretary of Defense.
- ***Homeland defense.*** DOD is responsible for protecting U.S. sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression.

Constitutionally, homeland defense is a federal responsibility. Furthermore, the public will expect DOD to defend the homeland and DOD will be ordered, by the national leadership, to participate in prevention, mitigation, and remediation of homeland disasters.

DOD acknowledges responsibility (with the Coast Guard) for homeland defense against air, sea, and missile attack. DOD leadership, both civilian and military, however has been slow to accept expanded responsibilities in other



There is substantial room for improvement in DOD's readiness for homeland defense.

homeland defense areas following the incidents of September 11, 2001.

In its traditional roles of air and maritime defense, DOD has or is developing capabilities, although they are not well exercised in homeland defense roles. Major shortfalls are clear in other homeland defense areas as well. DOD has not stepped up to its responsibilities in the broader homeland defense arena, either in commitment or resources.

The United States has been slow to recognize the possibility of assaults on the U.S. homeland. The nation has evolved into an interconnected society, closely bound to nations and worldwide energy, information, transportation, and financial networks. The vulnerability of these networks and of the society they support renders the nation highly vulnerable to disruption.

The United States is not well prepared to confront assault on its homeland. The response to Hurricane Katrina illustrated this point. Imagine a disaster on an even broader scale, or a series of deliberate attacks of a similar scale. Homeland disaster preparedness must be a national priority. DOD and DHS, acting in concert, must step up to their responsibilities to prepare for action in the homeland as well as abroad.

Lack of cooperation, rising costs, and organizational culture hinder the nation's success

ALL OF THE IMPORTANT ISSUES CUT ACROSS MANY DEPARTMENTS AND AGENCIES, REQUIRE MORE INTEGRATION IN PLANNING AND RESOURCING, AND MORE COHERENCE IN EXECUTION, THAN CURRENTLY ACHIEVED WITH THE PRESENT INTERAGENCY COMMITTEES.

DOD cannot "go it alone"—its success depends on orchestrated government action

Since September 11 it has become clear that a government-wide approach to national security is required, for planning, preparing, resourcing, training, and exercising. The players involved encompass DOD and the Intelligence Community, the civilian federal agencies, and state and local government. DOD cannot successfully execute its missions without an orchestrated partnership with other government organizations.

The nation needs an organizational approach for addressing truly important security issues that is different from the current de facto approach which depends largely on DOD. All of the important issues cut across many departments and agencies, require more integration in planning and resourcing, and more coherence in execution, than currently achieved with the present interagency committees. DOD has a critical role but is not in a position by charter or competence to lead all of the national security efforts to which the country must respond.

The pressing issues discussed in this report serve to demonstrate the inter-dependence of different government organizations in pursuit of national security objectives.

- Joint forces rely on the domestic critical military infrastructure—military garrisons and lines of supply, transportation networks, contractor factories, and commercial communications—to maintain supplies as they perform their military mission abroad. In turn, ensuring domestic safety in the face of potential threats to domestic critical military infrastructure depends on local police, the FBI, and the Department of Homeland Security.

- When DOD is called upon to work with local authorities should an attack on the U.S. homeland occur, its resources become divided between domestic catastrophe relief and projecting force abroad. Minimizing that division and diversion depends on orchestrated preparation, long in advance, by DOD, other parts of the federal government like the Departments of Homeland Security and State, local government capabilities like police and fire departments, and local hospitals.
- Preventing and defending against attacks on our homeland cannot be and is not the responsibility of DOD alone. The Intelligence Community shares responsibility and capability, as does DHS, the Department of State, and the FBI. (It should be noted that the FBI has a substantial presence abroad, where it oftentimes enjoys very good relationships with local law enforcement; and its role in providing domestic intelligence is important in that planning and preparation for such attacks, whether by terrorists or states, may very well partly take place within the United States.)
- Successfully performing stabilization and reconstruction operations demands not only military skills to ensure public safety, but also civilian skills such as those related to local governance, infrastructure, schooling, the economy; knowledge of local language, history, customs and religions; and honest and effective strategic communication. Departments of government other than DOD such as State, Treasury, and Commerce can make critical contributions, as can the Intelligence Community and private sector organizations.
- Both the military and the civilian economy depend heavily on the nation's information infrastructure—a critical asset that is vulnerable to attack. Protecting the nation's information infrastructure, including DOD's shared and unique information infrastructure, is not the responsibility of DOD alone: the Intelligence Community, the FBI, and DHS all play critical roles.

OUR ENEMIES RESPECT NO BOUNDARIES. BOTH CIVILIAN AND MILITARY SKILLS ARE NEEDED TO AFFECT NATIONAL SECURITY POLICY. EVENTS WITHIN THE UNITED STATES CAN EITHER ENABLE OR SEVERELY HINDER OUR ABILITY TO FIGHT ABROAD.

What is needed is an integrated concept, a set of strategies, execution capabilities, and a means for allocating resources. Such government-wide orchestration is lacking today and will be difficult to accomplish. Our enemies respect no boundaries. Both civilian and military skills are needed

to affect national security policy. Events within the United States can either enable or severely hinder our ability to fight abroad.

The organizational structure and authority for coordinated activity among the various departments and agencies of the executive branch exists today. No new committee is needed. The President, the National Security Advisor, the National Security Council, the Homeland Security Advisor, and the Homeland Security Council are well positioned to coordinate government-wide activity.

However, what is straightforward in principle is challenging in practice. The Department of Homeland Security and the Office of the Director of National Intelligence are new organizations still establishing how they will function. There are misalignments between authorities and resources, e.g. the Department of State's authorities and responsibilities relative to stabilization and reconstruction, and relative to strategic communication, are not matched by its current capabilities and resources. Steadily improving performance will not come from reorganization, but from the relentless daily application of proven management discipline.

In addition to the executive branch, government-wide responses involve other actors as well, not all perfectly positioned to act as part of a national team, but who could do so with planning and preparation. Congress, for one, must be engaged. The states and municipalities, which enjoy substantial independence from the federal government, differ with regard to priorities, plans, preparations, and budgets. In each of these cases, it will fall to the President and the national security apparatus to exercise the most effective leadership and management.

The importance of government-wide collaboration cannot be overstated, as the dual roles of the National Guard so aptly illustrate. This resource plays a central role in both state planning and preparation for disasters and in DOD planning for military expeditionary forces—which can result in double-counting individuals who may be called upon for concurrent critical needs. Further, we find that our national exercise program—wherein local, state, and federal agencies, including but not limited to DOD, prac-

tice together—is in dire need of improvement. While exercises seem to be plentiful, many of the challenges we face and the capabilities we will need are untested. Further, it is unclear the degree to which improvement follows from deficits inevitably uncovered during exercises.

As a major step toward the management discipline needed to effect government-wide action in service of national security, we urge the President, by delegation to DOD and DHS, to ensure that plans are in place for a wide range of national security issues that may arise. Those plans must be validated by employing the same practices used by the military services in planning and preparing for combat.

"Validation" means that the plans are exercised by all participants to uncover flaws and gaps; that those errors are fixed; that all participants agree to play their role; that the resources needed to successfully execute the plan actually exist and are not "double counted"; that roles, missions, responsibilities, and accountability be clear. Plans should be exercised repeatedly so that skills and experience are maintained and so that the "cost," in the broadest sense, is known as well as can be.

Accomplishing this will not be easy. The culture for this precise, validated planning is deeply imbued within DOD, but not nearly as much in other parts of the executive branch or state and local organizations. The monetary cost of validated planning is high; and the cooperation of all bodies—including the Congress, states, and local municipalities—is required. However, we see no alternative to having plans in place if we want to protect our way of life.

OUR NATIONAL SECURITY STRATEGY TACITLY EXPECTS THAT OUR JOINT MILITARY FORCES ARE READY TO NOT ONLY SUCCESSFULLY EXECUTE ALL OF THOSE MAIN MISSIONS, BUT SOMETIMES DO SO SIMULTANEOUSLY.

The "cost" of success may be high, and is getting higher

Our national security strategy tacitly expects that our joint military forces are ready to not only successfully execute all of those main missions, but sometimes do so simultaneously. A lengthy, protracted stability operation might very well provoke war with a near-peer or vice versa. Either might provoke an attack on the homeland requiring domestic catastrophe relief. Terrorism can be a contributing challenge for any of the other missions.

The "cost" of successfully performing these missions is not limited to money. The ledger must also include loss of U.S. military and civilian lives, loss of lives among friendly nations, effects on our civil liberties and way of life on a daily basis, economic consequences relative to our international trade, and our reputation around the world.

Furthermore, the cost of military success is on the rise as more and more potential adversaries gain access to modern technology of military relevance—proliferation that can't be stopped and is even difficult to slow. While we too have better and better technology to raise the cost for potential adversaries, the shifting balance does not seem to be in our favor.

All that taken together, DOD's budget and resources, substantial though they might seem, are inadequate to successfully accomplish all of the missions it may be called upon to concurrently perform. While DOD could and should be more efficient in use of its resources, improvement would yield but a fraction of what will be needed. A part of that required increase might be assumed by expanding the resources—and the capabilities—of civilian federal, state, and local organs of government; but the total cost to the citizenry will be essentially the same.

In short, we have to smartly ration use of our scarce military resources. Our urging is that elected leaders obtain a sense of the "cost," in the broadest terms, of employing our military as an instrument of power in support of national objectives before making a decision to do so, and thus be able to make a reasoned judgment regarding whether the costs outweigh the likely benefits or the converse.

Why things are the way they are

In considering the pressing issues that compromise our ability to achieve DOD's main missions, a number of underlying factors pose challenges to success.

As mentioned above, **the Constitution's concept of separation of powers**, with the laws and practices that devolve thereof, does not forbid concerted government action. But neither does it require or even facilitate such orchestration.

The proliferation of technology is providing increasing challenges. Militarily relevant technology—such as biotechnology and the Internet—is increasingly available around the world and is increasingly easy to use. What once required the expertise of a university professor is now routine for a high school student. With access to these tools, countries we would never consider a military peer and even terrorist groups are within sight of the capabilities to do strategic harm to the United States and its allies. Terrorist groups, so enabled with technology, provide particular problems: it is difficult to know what they hold dear and what we can realistically put at risk as a deterrent. Our own use of technology, such as digital computing and communication, carries with it not only advantages but also dependencies and vulnerabilities. Much technology is central to both peaceful purposes and military purposes, and it is almost impossible to collect the intelligence needed to decide which is being pursued.

Further, **the private sector owns much that the nation seeks to secure**—such as communication, banking, manufacturing, and transportation systems. It also owns much that is needed to maintain national security, e.g. health care facilities. However, the private sector is reluctant to invest in preparation for events judged extraordinarily unlikely, preparation such as sustaining unused excess capacity in hospitals in case of national emergency or fully protecting agricultural assets that have never been threatened. There is a difference between the public and private sector's inclination to invest in very low likelihood events, even events that could be catastrophic.

In many instances the **incentives** that motivate individual work and career decisions—getting and retaining jobs, salaries, and promotions—are not perfectly aligned with public service needs. Lowering costs for the citizenry might also represent lowering profits of a company or employment in a region, for example. Every successful company devotes a great deal of attention to ensuring that what is right for the individual employee is also right for the company as a whole, but that alignment is not well achieved within the public sector.

While the United States is a very wealthy nation, our **resources are not without limit**. Among DOD's traditional missions, stability operations are particularly expensive insofar as a very large number of highly trained personnel must be sustained abroad for a number of years, and there are no technology enablers, fixes, hedges or multipliers to reduce that cost. DOD is the only department or agency of the executive branch funded to maintain a large contingency capability which can be used in time of need, and which can exercise and train between missions and deployments. Adding a comparable large contingency capability to other departments, such as the Department of State, would be proportionately costly. The federal government faces significant obligations for important domestic programs like Social Security and Medicare, and those costs will likely increase with the demographic trends of the population. Many of the pressing issues for DOD might be cured with additional funding, but national security concerns have to compete with everything else for financial resources.

Organizational culture presents its own challenges. There is no "law of nature" that requires organizations to become bureaucratic and slow to adapt to changing circumstances as they age and grow—but that is what seems to happen. There is also no "law of nature" that requires successful organizations to be overly confident—but this too seems to often happen. We have seen as much in the slow adaptation of the military services to the asymmetric challenges facing the nation today—even as DOD remains by far the largest, most successful, and most capable military organization. Thus, it is essential to protect those pockets of innovation, agility, and prudent risk-taking within DOD that fly in the face of history decade after decade—such as the Defense Advanced Research Projects Agency (DARPA) and our special forces. Parts of the Army and Marine Corps have demonstrated impressively agile adaptation as well in response to their experiences in Iraq.

None of these underlying drivers is going to change very much, very fast, or necessarily at all. But they can be managed with explicit attention to incentives within the national security community.

These are urgent matters

The pressing issues explained herein present a daunting agenda:

- how our ability to protect our homeland may be compromised by the difficult challenge of weapons of mass destruction and by the decline in our nuclear capabilities
- how our ability to project military force around the world, both to deter our enemies and defeat them if necessary, may be compromised by our vulnerability to cyber attacks and by the long term debilitating effect of our business practices
- how our ability to counter terrorism is limited by the intelligence we can gather, both abroad and within the United States
- how our ability to bring stability to nations and regions depends on planning and preparation we have yet to carry out
- how our ability to respond to domestic catastrophes, whether natural or malicious acts of terrorists or foreign states, also depends on planning and preparation we have yet to put in place

...WE CANNOT TAKE OUR TIME TO ADDRESS THESE PRESSING ISSUES...

WE NEED TO FEEL A SENSE OF URGENCY AND ACT ACCORDINGLY.

Fortunately, all of the aforementioned pressing issues can yield in part or in whole to solutions that the Defense Science Board and others have put forward—such as some of the key recommendations from this report, summarized in the following table. Some will require substantial resources to resolve, others "merely" creative and enlightened leadership.

However, we cannot take our time to address these pressing issues. We are at war in Afghanistan and Iraq, with over 180,000 military personnel and perhaps 30,000 U.S. civilian contractors at risk. We cannot know how militant Islamic jihadist terrorism will develop or what it will do. Nations of concern, both rogue states and the largest nations, are enlarging their armories. We need to feel a sense of urgency and act accordingly.

Some Key Recommendations for Addressing the Pressing Issues

Protect and defend the homeland	
Weapons of mass destruction challenge the safety of our military forces	• Improve close-in intelligence • Deny acquisition of weapons of mass destruction including immediate replacement of Cesium-137 in medical systems • Deter use of WMD with improved attribution and more clearly perceived retaliation • Urgently provide improved capabilities for mitigation and recovery including improved exercises and establishing clear lines of responsibilty • DOD should set an example of preparation and protect its own people and capabilities
Our nuclear capability—weapons, skills, facilities—is declining	• Restore senior-level attention and tight adherence to nuclear surety procedures • Develop a plan to maintain skill levels of personnel in both weapon design and in nuclear effects • Re-invigorate training of conventional forces for survival in a nuclear environment • Provide the nuclear leadership, at the national level, needed but missing for the last decade and a half
Maintain capability to project force around the world, to deter or defeat	
Our military and civilian information infrastructure is highly vulnerable	• Give a very high priority and corresponding resources to improving cyber security • Recognize, accept, and plan for even our classified networks being attacked and exploited by adversaries • Be prepared for a long-term rapid-fire contest between defense and attack in cyber warfare • Develop space situational awareness
DOD's business practices are having a long-term debilitating effect on our military forces	• Require authoritative business plans to enforce discipline in allocating resources to mission purposes • Change "requirements" from absolute dictum to development guidance • Make true spiral development the norm for DOD development • Reconstitute system engineering capabilities within DOD • Establish a better governance structure to manage the development, configuration, interoperability, and operation of DOD's network structures • Create a joint logistics command responsible for end-to-end military supply chain
Bring stability to states and regions	
We lack robust plans and capabilities to support country-specific stability operations	• Extend the management discipline of combat to stability operations • Make stabilization and reconstruction missions one of the core competencies for DOD and the Department of State • More effectively exploit capabilities of the private sector • Create new coordination and integration mechanism across the government • Provide the leadership, strategic direction, adequate coordination, effective research, sufficient resources, and a culture of measurement and evaluation for strategic communication that are necessary but missing today • Develop and implement a long-term plan for foundations in language and cultural understanding

Thwart terrorism and bring terrorists to justice—anytime and anywhere	
We lack the deep penetration required for actionable intelligence—both foreign and domestic	• Focus intelligence on deep penetration that is required for actionable intelligence with close in sensing, tracking people, intrusive, covert, persistent collection • Define, design, and implement a true "collection architecture" • Improve orchestration of foreign and domestic intelligence
Support state and local authorities in providing domestic catastrophe relief	
The nation lacks validated operational contingency plans to respond to domestic catastrophes—whether natural or malicious	• Nurture a culture of preparedness on all levels to significantly reduce the consequences of attacks on the homeland • Deal with the double counting problem with the all-important National Guard • Incentivize private industry participation in disaster preparedness • Clarify roles and responsibilities for responses including transfers of responsibility as level of destruction esacalates • Improve effectiveness of exercises and involve all potential participants
Lack of cooperation, rising costs, and organizational culture hinder the nation's success	
DOD cannot "go it alone"—its success depends on orchestrated government action	• Provide the leadership needed to ensure teamwork and cooperation between elements of the federal government and between the federal, state, regional, and local governments
The "cost" of success may be high, and is getting higher	• Project the cost, in the fullest sense, of employing the military as an instrument of foreign policy before actually committing forces
Why things are the way they are	• Protect pockets of innovation, agility, and prudent-risk taking such as DARPA and special operations forces

References

Business Practices

Final Report of the Defense Science Board Task Force on Globalization and Security, December 1999

Report of the Defense Science Board/Air Force Scientific Advisory Board Joint Task Force on Acquisition of National Security Space Programs, May 2003

Report of the Defense Science Board Task Force on Enabling Joint Force Capabilities, August 2003

Defense Science Board Task Force on High Performance Microchip Supply, February 2005

Report of the Defense Science Board Task Force on Management Oversight in Acquisition Organizations, March 2005

Defense Science Board Summer Study on Transformation: A Progress Assessment, Volume I, February 2006

Defense Science Board 2006 Summer Study on Information Management for Net-Centric Operations, Volume I: Main Report, April 2007

Defense Science Board 2006 Summer Study on 21st Century Strategic Technology Vectors, Volume IV: Accelerating the Transition of Technologies into U.S. Capabilities, April 2007

Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DOD Software, September 2007

Defense Science Board Task Force on Logistics Transformation, Phase II, January 2008

Domestic Catastrophe Relief

Protecting the Homeland, Report of the Defense Science Board 2000 Summer Study on Defensive Information Operations, Volume I: Executive Summary, February 2001

Defense Science Board 2003 Summer Study on DOD Roles and Missions in Homeland Security, November 2003

Interim Report of the Defense Science Board Task Force on SARS Quarantine, December 2004

Defense Science Board Summer Study on Transformation: A Progress Assessment, Volume I, February 2006

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

Defense Science Board Task Force on Deployment of the Members of the National Guard and Reserve in the Global War on Terrorism, September 2007

Defense Science Board 2007 Summer Study on Challenges to Military Operations in Support of National Interest (forthcoming 2008)

Government-wide Cooperation

Report of the Defense Science Board Task Force on the Creation and Dissemination of All Forms of Information in Support of Psychological Operations in a Time of Military Conflict, May 2000

Report of the Defense Science Board Task Force on Strategic Communication, September 2004

Defense Science Board 2005 Summer Study on Transformation: A Progress Assessment, Volume II: Supporting Reports, April 2006

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

Defense Science Board Task 2006 Summer Study on 21st Century Strategic Technology Vectors, Volume I: Main Report, February 2007

Report of the Defense Science Board Task Force on Strategic Communication, January 2008

Information Infrastructure

Defense Science Board Task Force on High Performance Microchip Supply, February 2005

Defense Science Board 2006 Summer Study on Information Management for Net-Centric Operations, Volume I: Main Report, April 2007

Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DOD Software, September 2007

Nuclear Capability

Defense Science Board Studies

Report of the Defense Science Board Task Force on Defense Nuclear Agency, April 1993

The Defense Science Board 1997 Summer Study Task Force on DOD Response to Transnational Threat, Volume I: Final Report, October 1997

Report of the Defense Science Board Task Force on Nuclear Deterrence, October 1998

Report of the Defense Science Board Task Force on Tritium Production Technology Options, January 1999

Protecting the Homeland, Report of the Defense Science Board 2000 Summer Study Task Force on Defensive Information Operations, Volume I: Executive Summary, February 2001

Defense Science Board 2003 Summer Study on DOD Roles and Missions in Homeland Security, November 2003

Report of the Defense Science Board Task Force on Future Strategic Strike Forces, February 2004

Defense Science Board Task Force on B-52H Re-Engineering, June 2004

Report of the Defense Science Board Task Force on Preventing and Defending Against a Clandestine Nuclear Attack, June 2004

Report of the Defense Science Board Task Force on Employment of the National Ignition Facility, October 2004

Report of the Defense Science Board Task Force on Nuclear Weapons Effects Test, Evaluation, and Simulation, April 2005

Report of the Defense Science Board Task Force on Future on Strategic Strike Skills, March 2006

Report of the Defense Science Board Task Force on Nuclear Capabilities, December 2006

Defense Science Board 2005 Summer Study on Reducing Vulnerabilities to Weapons of Mass Destruction, May 2007

Defense Science Board Permanent Task Force on Nuclear Weapons Surety Report on Unauthorized Movement of Nuclear Weapons, February 2008

Defense Science Board 2007 Summer Study on Challenges to Military Operations in Support of National Interest (forthcoming 2008)

Report of the Defense Science Board Task Force on Nuclear Deterrence Skills (forthcoming 2008)

Report of the Joint Defense Science Board/Threat Reduction Advisory Committee Task Force on the Nuclear Weapons Effects National Enterprise (forthcoming 2008)

Other Articles and Reports

Kontseptsiya natsionalnoy bezopasnosti Rossiikoy Federatsii Utverzhdea Ukazom Prezidenta RF ot 17 dekabrya 1997 g. No 1300, (http://www.scrf.gov.ru/documents/decree/2000/24-1/html)

Voyennaya Doktrina Rossiiskoy Federatsii, Utverzhdena Ukazom Prezidenta, RF ot 21 aprelya 2000 g. No. 706.

Nikolai Sokov, “Russia’s New National Security Concept: The Nuclear Angle” CNS Report, January 2000.

“Strategicheskaya Komandno-Shtabnaya Treniroivka VS Rossii”, Nezavisimaya gazeta, February 17, 2001.

Yuriy Golotuyk, “I v Vozdukhe Tozhe Problemy” Vremya novostey, February 19, 2001.

Vladimir Putin, “Zakluychitelnoe Slovo na Soveshchaniis Rukovodyashim Sostovom Vooruzhennykh Sil Rossii”, October 2, 2003 (available at htpp://www.president.kremlin.ru/text/appears/2003/10/53277.shtml).

Nikolai Sokov, “Russia’s Nuclear Doctrine”, Center for Nonproliferation Studies (CNS) Report, August 2004.

Prime Minister Tony Blair “Parliamentary Statement on Trident,” 2006

D. Lewis Dunn, “Influencing Foreign Perspectives on U.S. Nuclear Policy and Posture,” DTRA/ASCO, 2006.

Steve Gutterman, "Russia Test New Missiles, Warns U.S.", Associated Press, May 30, 2007

President Nicolas Sarkhozy, speech delivered on the Presentation of Le Terrible, Cherbourg, 2008.

Statement by Sergey Ivanov, available at http://www.mil.ru/articles/article3667.shtml

International Atomic Energy Agency. (http://www-pub.iaea.org/MTCD/publications/PDF/RDS1-26_web.pdf) Accessed June 25, 2008.

World Nuclear Association. (http://www.world-nuclear.org/info/inf102.html) Accessed June 2, 2008.

U.S. Department of State. On-The-Record Briefing with Secretary of State Condoleezza Rice, October 17, 2006. http://www.state.gov/secretary/rm/2006/74667.htm. Accessed July 3, 2008.

U.S. Department of State. Remarks with Japanese Foreign Minister Taro Aso After Their Meeting, October 18, 2006. http://www.state.gov/secretary/rm/2006/74669.htm. Accessed July 3, 2008.

Utgoff, Victor and David Adesnik, "On Strengthening and Expanding the US Nuclear Umbrella to Dissuade Nuclear Proliferation," P-4356, Institute for Defense Analyses, July 2008.

Stabilization and Reconstruction

Defense Science Board 2004 Summer Study on Transition to and From Hostilities, December 2004

Report of the Defense Science Board Task Force on Institutionalizing Stability Operations within DOD, September 2005

Defense Science Board Task 2006 Summer Study on 21st Century Strategic Technology Vectors, Volume I: Main Report, February 2007

Thwarting Terrorism (Intelligence)

Defense Science Board Studies

Defense Science Board 2003 Summer Study on DOD Roles and Missions in Homeland Security Volume II, Part A: Supporting Reports, May 2004

Report of the Defense Science Board 2003 Summer Study on Roles and Missions in Homeland Security, Volume II, Part B: Supporting Reports, Information Sharing and Analysis Panel Report, September 2004

Defense Science Board 2004 Summer Study on Transition to and From Hostilities, Volume II: Support Papers, December 2004

Other Articles and Reports

Michael Scheuer, Al-Qaeda Doctrine: Training the Individual Warrior, http://www.jamestown.org/terrorism/news/article.php?articleid=2369944

Weapons of Mass Destruction

The Defense Science Board 1997 Summer Study Task Force on DOD Response to Transnational Threat, Volume I: Final Report, October 1997

Leveraging Advances in Biotechnology and Medical Informatics to Improve Homeland Biodefense Capabilities, Volume IV, Protecting the Homeland, Report of the Defense Science Board 2000 Summer Study, October 2001 (limited distribution).

Protecting the Homeland, Report of the Defense Science Board 2000 Summer Study Task Force on Defensive Information Operations, Volume I: Executive Summary, February 2001

Defense Science Board 2003 Summer Study on DOD Roles and Missions in Homeland Security, November 2003

Report of the Defense Science Board Task Force on Preventing and Defending Against a Clandestine Nuclear Attack, June 2004

Report of the Defense Science Board Task Force on Nuclear Weapons Effects Test, Evaluation, and Simulation, April 2005

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

Defense Science Board 2005 Summer Study on Reducing Vulnerabilities to Weapons of Mass Destruction, May 2007

Defense Science Board 2007 Summer Study on Challenges to Military Operations in Support of National Interest (forthcoming 2008)

OFFICE OF THE UNDER SECRETARY OF DEFENSE
FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
WASHINGTON, D.C. 20301-3140