Report of the
Defense Science Board
2007 Summer Study

Challenges to Military Operations in Support of U.S. Interests

Volume II
Main Report

December 2008

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

Report Documentation Page

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Challenges to Military Operations in Support of U.S. Interests (Volume II Main Report)	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 Defence,for Acquisition, Technology, and Logistics,Washington,DC,20301-3140**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**505**	

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.

The DSB Task Force on Challenges to Military Operations in Support of U.S. Interests completed its information gathering in August 2007.

This report is unclassified and has been cleared for public release.

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

9 Dec 2008

MEMORANDUM FOR: UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS

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

I am pleased to forward the final report of the Defense Science Board 2007 Summer Study on Challenges to Military Operations in Support of U.S. Interests. The report offers important considerations for the Department of Defense in response to future threats to our nation's security.

This study, robust in scope, concerns itself with challenges the U.S. military might face in the future, emphasizing areas where the nation is less well prepared. Future adversaries are more likely to attack the nation with asymmetric tools of war, employed using non-traditional concepts of operation. Thus, challenges from nuclear weapons, from cyber warfare, in and from space, to force deployment and resupply, and on U.S. soil, may well dominate in the decades ahead. Addressing U.S. vulnerabilities in these and other areas is the focus of the study's effort, leading to actions for the Department that can improve the nation's posture against future threats.

I endorse all of the study's recommendations and encourage you to forward the report to the Secretary of Defense.

William Schneider, Jr.
DSB Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR: Chairman, Defense Science Board

SUBJECT: Final Report of the Defense Science Board 2007 Summer Study on Challenges to Military Operations in Support of U.S. Interests

U.S. conventional military capability remains unmatched by any state. As a result, nations and powerful non-state actors, weaker in conventional weaponry, will face the United States with unconventional weapons. Further, these asymmetric tools of war may well be employed using non-traditional concepts of operation. And the battlefield may no longer be limited to regions afar, but may include the U.S. homeland. The United States could well confront the possibility of going to war abroad in the face of significant devastation in the homeland—dividing forces between homeland catastrophe relief operations and combat abroad—even facing the possibility that deploy and supply of U.S. military forces could be delayed and disrupted.

How to contemplate this future, over the next two decades, was the focus of the Defense Science Board 2007 Summer Study. The question asked by the study is this: **Is the United States maintaining its capability to deter and defeat a nation or non-state actor who might employ unconventional as well as conventional means, in non-traditional as well as traditional ways, to thwart U.S. interests?**

To focus on challenges for which the United States might be less well prepared, the study investigated seven topic areas, making recommendations for actions in each of them:

- **Future of war**. The character of war is changing—it is irregular, catastrophic, disruptive and no longer confined to the traditional battlefield. This changing character of warfare calls for considerations about how the nation's military capabilities should evolve—the type of forces, reliance on information infrastructures, protection to forces and critical infrastructure, new capabilities. At the same time, other instruments of national power must be brought to bear, which will involve strengthening relationships between the Department of Defense and other federal partners.

- **Unconventional weapons and technology proliferation**. The technology equation, between the United States and potential adversaries, is key to the nature of future warfare and the ability of our nation to prevail. The range of possible destructive weapons is vast, but three stand out as the most critical: nuclear weapons, biological agents, and cyber warfare. There are

steps that can be taken—in prevention, attribution, mitigation, and recovery—that can improve the U.S. posture against such attacks.

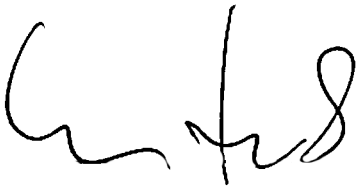
- **Nuclear proliferation—a special case**. The nuclear threat stands in a class by itself in terms of its potential for damage, disruption, and devastation. Thus, managing the challenge of nuclear proliferation deserves special attention. History has shown that it is possible to influence the decision to acquire nuclear weapons. Thus emphasis should be placed on developing tailored approaches to proliferation prevention to shape the nuclear environment. At the same time, the United States needs to prepare to cope with the military operational challenges of a more proliferated world—closing the sizeable gap between current capabilities and future needs.
- **Unconventional operational concepts and the homeland**. The capable adversary of the future will execute "one game"—attacking U.S. interests wherever the nation is most vulnerable, and that could mean the homeland. Overseas deployment, simultaneous with responding to a significant scale of attacks in the homeland, will stress DOD capabilities. Roles and responsibilities are not clearly defined, and adequate resources have not been invested in the homeland defense missions. Furthermore, the problem extends beyond DOD to the interagency and response communities, where the handoffs and roles are not well understood—in part because they are not effectively exercised.
- **What we know and don't know about adversary capabilities: intelligence**. It is not possible to plan and prepare for all possible futures; nor is it possible for an adversary to exercise all of the opportunities to which they might take advantage. Thus, with good intelligence, the United States can focus its investments on the most likely cases. Strategic issues should command top level focus in the Intelligence Community, and the attention of some of its best resources. Improvements are also needed in foreign and domestic intelligence collection, analysis, and support; countering foreign intelligence; net assessments and gaming; and methods for improving intelligence related to the threat of weapons of mass destruction (WMD).
- **Fighting through asymmetric counterforce**. While the range of potential asymmetric attacks is wide, this study identified three as particularly challenging: conducting military operations in WMD environments, countering attacks on U.S. and allied space capabilities, and cyber warfare against information networks. DOD needs to take steps to enhance the capabilities of general-purpose forces to operate in an environment where WMD have been used. Further, the ability to operate in and from the global commons—space, international waters and airspace, and cyberspace—is critical to DOD's ability to conduct operations and project power anywhere

in the world. Thus, the Department must act to mitigate vulnerabilities in these areas.

- **Strategic communication—another instrument of U.S. power**. Defending U.S. interests against future adversaries will require more than just military might—involving other instruments of U.S. power such as diplomacy, economic and financial sanctions, and strategic communication. Strategic communication is vital to America's future and must be transformed at strategic and operational levels. The range of future threats varies greatly and requires a strategic communication instrument with sustained impact and far greater capacity to understand, engage, and influence global populations on issues of consequence—an instrument that emphasizes actions that are consistent with what national leaders say.

Taken together, the issues addressed in this study point to the fact that the cost to deter or defeat future adversaries is rising—costs defined not only in financial terms but also along other dimensions to include military lives, civilian lives, money, civil liberties, daily comfort, economic health, and global reputation. Thus, instruments of national power, other than military, will assume greater importance.

The nation is unprepared and is making little progress in reducing these costs. But circumstances can be materially improved. The United States can achieve its national objectives by taking a combination of actions that will have an impact on costs—actions that are detailed in the recommendations of this report. DOD must begin to act, even as it fights the current war, to make sure it is ready for the next war, one that could well be even more stressing than the war the nation fights today.



Dr. Craig Fields
Co-Chair

Mr. Richard Haver
Co-Chair

Table of Contents

Volume I. Executive Summary

Volume II. Main Report

Major Themes....xi
Preface....xiii

Part I. The Future of War as We Know It....1
Chapter 1. Why Do We Have a Military?....3
Chapter 2. The Past: Fads and Phases in Warfare....16
Chapter 3. The Role of Technology: Weapons that Change War....26
Chapter 4. Present Concerns: What Now?....28
Chapter 5. The Future: What is New?....34
Chapter 6. Homeland Defense: What is Needed?....54

Part II. Unconventional Weapons and Technology Proliferation....61
Chapter 7. Technology of Unconventional Weapons....63
Chapter 8. Red Objectives and Attack Options....68
Chapter 9. How Blue Can Respond....94
Appendix II-A. Supporting Data....105

Part III. Nuclear Proliferation: A Special Case....115
Chapter 10. A Core Emerging Challenge....117
Chapter 11. Needed Military Capabilities in a More Proliferated World....136
Chapter 12. Toward More Effective Proliferation Prevention....161
Appendix III-A. Proliferation Contingencies 2027....171

Part IV. Unconventional Operational Concepts and the Homeland....201
Chapter 13. One Game: Defending the Homeland....203
Chapter 14: DOD Roles and Responsibilities....210
Chapter 15. Assuring Deployment and Supply....220
Chapter 16. Building the National Team....239
Appendix IV-A. Relevant Legislation and Directives for DOD in Homeland Security and Defense....263
Appendix IV-B. Selected Excerpts from the "Strategy for Homeland Defense and Civil Support," June 2005....268

Part V. What We Know and Don't Know about Adversary Capabilities: Intelligence 273
Chapter 17. What We Know and Don't Know 275

Part VI. Fighting Through Asymmetric Counterforce 287
Chapter 18. The Asymmetric Challenge 289
Chapter 19. Combat Operations in a WMD Environment 292
Chapter 20. Countering Attacks on U.S. and Allied Space Assets 308
Chapter 21. Cyber Warfare Against Information and Networks 319
Chapter 22. Crosscutting Observations 341

Part VII. Strategic Communication: Another Instrument of U.S. Power 343
Chapter 23. The Importance of Strategic Communication 345
Chapter 24. What is Strategic Communication and Why Does it Matter? 353
Chapter 25. The World is Changing 363
Chapter 26. Technology is Changing 380
Chapter 27. Engaging National Capability 401
Chapter 28. Conclusions and Recommendations 422
Appendix VII-A. Executive Summary and Recommendations from the 2004 DSB Report on Strategic Communication 438
Appendix VII-B. Recommendations from the 2001 DSB Report on Managed Information Dissemination 446
Appendix VII-C. Government and Independent Organization Studies of Strategic Communication and Public Diplomacy, September 2001–October 2007 450

Terms of Reference 455
Study Participants 461
Presentations to the Study 469
Glossary 481

Major Themes

Nations and powerful non-state actors, weaker in conventional weaponry, will face the United States with unconventional weaponry. The most challenging are:

- nuclear weapons, worsened by proliferation
- self-replicating biological weapons
- cyber weapons to disrupt net-centricity, including in space

They will also exploit vulnerabilities in our homeland security by:

- attacking our homeland to disrupt military deployment and supply
- dividing our joint forces between domestic civilian relief and foreign military operations

We are unprepared:

- At best, our policies and actions will be severely constrained.
- Worse, we will enter the fray and then quit when we come to appreciate the full cost of success.
- These costs are defined not only as financial costs, but also along broader dimensions, such as military lives, civilian lives, money, civil liberties, daily comfort, economic health, and global reputation.

Instruments of national power other than the military, such as strategic communication, will assume greater importance.

Preface

U.S. conventional military capability remains unmatched by any state. U.S. military operations since Operation Desert Storm have demonstrated an overwhelming ability to continually grow conventional capability and outmatch opponents. As a result, no adversary—peer, near peer, or powerful non-state actor—with objectives in conflict with U.S. interests will oppose our nation with conventional military means. The United States is too strong and capable. Yet, this strength in the conventional arena does not mean that the nation is unmatched across the spectrum of conflict.

At one point in time, for example, the Soviet Union challenged U.S. interests with a strong nuclear capability and significant conventional strength as well. While that threat no longer exists today in the form it once did, the proliferation of nuclear weapons opens the possibility that U.S. interests and conventional capability could again be threatened by such weapons in some region of the world. The proliferation of other weapons of mass destruction—biological, chemical, and radiological, among others—should be expected as well, adding to potential future threats.

Moreover, the proliferation of technology, technical information, and technical skills facilitates access to a range of weaponry that can be used to attack the United States both at home and abroad by means other than conventional. These asymmetric tools of war may well be employed using non-traditional concepts of operation. And the battlefield may no longer be limited to regions afar, but may include the U.S. homeland. Furthermore, the proliferation of technology has, to a certain degree, "lowered the bar" such that future adversaries will not be limited to nation states, but will extend to non-state actors such as terrorists, insurgents, and groups not bound by geography and the traditional trappings of statehood. This outlook suggests that U.S. interests could be threatened by adversaries in the future that, in the past, would never have been labeled a "peer" or "near peer"—that, in fact, might never have been anticipated as adversaries at all.

How to contemplate this future, over the next two decades, was the focus of the Defense Science Board 2007 Summer Study. The question asked by the study was this:

Is the United States maintaining its capability to deter and defeat a nation or non-state actor who might employ unconventional and conventional means, in non-traditional as well as traditional ways, to thwart U.S. interests?

The study concerns itself with challenges the U.S. military might face in the future for which the nation is less well-prepared. One such challenge is the possibility of going to war abroad in the face of significant devastation in the homeland. Such a circumstance would put competing demands on the military—dividing forces between homeland operations and combat abroad—and possibly constrain our nation's ability to project military force in support of national interests.

Homeland devastation, caused by malicious or natural acts, is but one scenario. Precision attacks on domestic infrastructure critical to military operations—such as bases, depots, ports, airfields—as well as components in the private sector on which the military relies, such as commercial communications or contractor factories, can disrupt military deployment and supply. Other scenarios could involve blackmail through an arsenal of nuclear weapons or skillful use of the media to circumscribe U.S. military options. In any regard, devastation of the homeland could well demoralize the American public, potentially changing the behavior of the U.S. government in response to public pressure.

The question addressed in this study is broad and touches on the full spectrum of warfare, using the full spectrum of weaponry, against the full spectrum of potential adversaries. But to conduct such a study without limits was not possible. Thus, in an effort to limit the scope to some degree, the focus of the study included the following:

- U.S. national interests that may demand use of military force
- nations and powerful non-state actors
- homeland defense as needed to ensure military prowess in war
- nuclear proliferation and coercion, attribution, consequence management, fighting through a limited nuclear attack on our forces
- asymmetric, unconventional weapons
- weapons smuggled into the U.S. homeland, weapons of mass destruction produced in the United States
- transformation in the face of adversary unconventional weapons and/or operational concepts
- capabilities rather than scenarios

What is left out? Outside the scope of this study are U.S. national interests that do not demand use of military force or instruments of U.S. power other than military force. The study does not focus on *ad hoc* terrorist groups or criminals. It does not specifically consider stabilization, reconstruction, nation-building, peacekeeping, humanitarian missions, or continuing counterterrorism operations—though some if its recommendations could improve U.S. capabilities to conduct such operations as well. It also leaves aside the scenario of all-out nuclear war. As the study focuses on asymmetric, unconventional weapons, traditional order of battle is not addressed, nor is ballistic missiles, cruise missiles, or air and maritime defense of the homeland. Current readiness, recruitment, and retention challenges are also left for others to examine.

Methodology

Despite efforts to narrow its focus, the scope of the study remained robust, presenting the challenge of how to approach the investigation into U.S. capabilities, capability gaps, and necessary actions to improve the nation's ability to prevail against the future described herein. Thus, the subject matter was divided into six topic areas, with no attempt to ensure that they were mutually exclusive:

1. unconventional weapons and technology proliferation
2. nuclear proliferation: a special case
3. unconventional operational concepts and the homeland
4. what we know and don't know about adversary capabilities: intelligence
5. fighting through asymmetric counterforce
6. strategic communication: another instrument of U.S. power

Each of these topics is addressed in Parts 2 through 7 of this report.

Accommodating such a future will not be easy. Nor will predicting it. And the consequence of being wrong could be severe. Notwithstanding this point, history can offer perspective, and it is useful to ask how the past might be able to inform the future. The critical question may well be whether the future is likely to look so different that it invalidates current defense programs or concepts of operation that have been central to the American way of war. Thus, this report begins, in Part 1, with an assessment of the future of war with the aim of identifying what might be new in the future—"game changers" to which the nation must respond, and ideally anticipate.

Part I

The Future of War as We Know It

Chapter 1. Why Do We Have a Military?

The first step in reviewing whether the U.S. military is properly postured for the future is to consider and/or validate the reasons why the nation has a military force. In the largest sense, the answer is obvious: to help achieve national objectives, when other instruments of national power have proved unsuccessful. Yet, what are those national objectives, and how do they translate into military missions for which the armed forces must prepare?

Military Objectives

Protecting Ourselves: The Homeland Defense Mission

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

Throughout the latter half of the 20th century, the United States faced little direct threat to the homeland other than 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 in 2001.

In the aftermath of September 11, 2001, the nation has begun to reconsider both the threats to its homeland and the appropriate military countermeasures to those threats. If the threats were conventional bombardment and/or invasion of the continent, there would be little difficulty defining the role of the Department of Defense (DOD) and the military force it manages. The difficulty arises when valid threats appear to come from non-state actors, loosely networked, and potentiated by weapons of mass destruction, or at least weapons of mass disruption. At issue is the ambiguous, officially unresolved, expectations of the military in the event when remediation and, perhaps, internal peacekeeping are the order of the day.

For the case of serious devastation to the homeland, DOD is neither especially well-postured nor especially resourced as the "first responder of last

resort." While much of DOD's materiel and soldiery are sufficiently versatile to be able to mount a credible response, nonetheless, an attack on the homeland poses a serious complication. That complication—a tenet of this study—is that *a U.S. military response to a domestic calamity, inflicted purposely by an adversary, contends directly with the nation's ability to project force and deal directly with that adversary or associated adversaries.* Whether an adversary attack on the homeland is targeted at the U.S. population and its critical infrastructure, or its military garrisons and lines of supply, such attacks could constrain and perhaps fatally compromise the nation's ability to project force as required. As will be discussed in this report, the ability to strike seriously at the U.S. homeland, once reserved for the high-end adversary, may now be within reach of lesser states and stateless, networked adversaries as a result of globally available technology, transport, and connectivity.

Influencing the Behavior of Others: A Force Protection Mission

The United States is anxious to live at peace within the international community, prosper, and encourage others similarly. It respects and guarantees the rights of its citizens and encourages other countries to do likewise. It seeks to accomplish these things through moral leadership and the use of "soft power." On occasion, soft power falls short and the U.S. military is called upon to:

- **Deter, dissuade, and/or compel its adversaries**. The specter of the U.S. military can be required to convince others to refrain from doing something they might otherwise be tempted to do, and sometimes to help urge them to do something they are otherwise disinclined to do. Attacking the United States or its allies is the most obvious case for deterrence or dissuasion. Encouraging others to act responsibly within the family of nations generally results in compliance.
- **Defend allies**. Direct engagement by U.S. military force may be required to defend its allies and their worthy interests. In this context, defense may necessarily involve the projection of U.S. force. An adjunct, possibly an alternative, is providing defensive weaponry, a theme revisited in this report.
- **Secure markets**. Although the United States does not consider itself "mercantilist," free market competition and access to foreign markets for competitive U.S. industries, goods, and services is essential to economic well-being and to the economic benefit of all nations.

- **Secure supplies**. The obverse of access to international markets is access to international raw materials and component goods and services, which is equally important for economic health and, as above, for international prosperity.
- **Free the oppressed**. As the United States has matured as a nation, its concern over the rights of its own citizens has elevated to a larger concern over the rights of all peoples—all equally entitled to life, liberty, and the pursuit of happiness. This concern with human rights is, at once, both altruistic and pragmatic.

This catechism of national objectives, as stated, largely reflects the Westphalian tradition of thinking of international actors as nation-states—although, admittedly, the last concern with human rights does not respect that tradition. At the dawn of the 21st century, the United States recognizes that there are other actors on the international stage with whom it must contend. Islam, as its name advertises, is a nation but not a state in the sense of Westphalia. Whether, and to what extent, this type of adversary may lead our nation to modify its characterization of national objectives will be answered in time.

Helping Allies Defend Themselves: A Military Assistance Mission

While direct military engagement may, in some cases, be required of the United States to defend its allies, this course of action need not, and should not, be the first option. Military assistance, training, and joint exercise are also part and parcel of defending allies. Providing military materiel, whether through grant, purchase, or "lend lease," can be an important ingredient in the recipe for defending allies.

The nation's processes of relentless research and development; intelligence-informed threat and capabilities analyses; and quality production, deployment, training, and maintenance make U.S. weaponry nonpareil. The larger portion of this effort is geared to equipping the nation's war-fighters with offensive weaponry—the capability to project force when and where needed. Yet, providing "defensive" weaponry to allies seems a more attractive option. Done well, it may obviate the need for direct engagement of U.S. military forces. It can provide a distributed deterrent, with less concern that a headstrong ally might needlessly embroil the United States were it to provide weapons better suited to offense.

Defensive weaponry is attractive for the homeland defense mission as well.

Comforting the Needy: A Humanitarian Mission

Humanitarian missions, while not the premier reason for maintaining military force, nonetheless serve both to reinforce the nation's position of moral leadership and pragmatically to calm turbulent waters in addition to fulfilling a commitment to life, liberty, and pursuit of happiness to all people.

Such missions are also known as "operations other than war" or "security, stability, transition, and reconstruction operations."[1] They generally involve a crisis that has overtaken a large population whose local government is unable to meet basic needs due either to disruption or displacement. The root cause might be specific events like war, famine, or natural disaster, and certain populations are historically more vulnerable to such events as a result of overpopulation and under-developed infrastructure. Technological disasters such as Chernobyl or Bhopal may foreshadow future after-effects related to weapons of mass destruction (WMD) bear relationship to an aspect of the homeland defense mission.

A "Peer" by Any Other Name

Who might cause the United States to back away from a legitimate national objective? By definition, the answer is a "peer competitor" or a "near peer." A peer competitor, in the national security sense, is any nation whose capabilities are such that in a supreme test of wills with the United States, the outcome is uncertain. *The peer relationship—military and/or economic—might be symmetric, where their capabilities mirror those of the United States, or asymmetric, where their strengths play to U.S. weaknesses.*

A peer's instruments of national power need not be at parity with the United States, even in the symmetric case. It is not a question of whether, in a supreme test of wills, the United States could prevail. Rather it is a question of whether the U.S. can prevail at an acceptable cost. *History shows that in a contest between nations the winner is not necessarily the most endowed nation, but the one whose government can extract the necessary treasure and commitment from its people.* What appears to be different today, and likely to be so in the future, is that adversaries who might not have been labeled a "peer" or "near peer" in the past,

1. Former "stability and support operations."

by dint of available technology and homeland insecurity, could raise costs to a level where they prevail and the United States does not.

China, the "Elephant in the Room"

China, the world's most populous nation, is poised to become the world's largest economy. Yet China is not the only "elephant in the room." Even in conventional terms, a resurgent Russia or a surging India might qualify.

By 2025 the number of English–speaking Chinese is likely to exceed the number of native English speakers in the rest of the world. More honor students (top quartile) are currently in school in China than the total number of students in the United States. If you are "one in a million" in China, then there are 1,300 other people just like you (in India, 1,100). According to *The World Factbook*, the current population of China is 1,321,851,888 (Central Intelligence Agency, July 2007 est.) This August the one-millionth auto rolled off the Chevy assembly plant in China. It took 6 years to produce the first half-million, and just a year-and-a-half to produce the second half million.

For centuries China stood as a leading civilization, outpacing the rest of the world in the arts and sciences, but in the 19th and early 20th centuries, the country was beset by civil unrest, major famines, military defeats, and foreign occupation. After World War II, the Communists under Mao Zedong established an autocratic socialist system that, while ensuring China's sovereignty, imposed strict controls over everyday life and cost the lives of tens of millions of people. After 1978, his successor, Deng Xiaoping, and other leaders focused on market-oriented economic development and, by 2000, output had quadrupled. For much of the population, living standards have improved dramatically and the room for personal choice has expanded, yet political controls remain tight.[2]

In what may prove a mastery of understatement, the DOD, in its annual report to Congress, remarked that "China's rapid rise as a regional political and economic power with global aspirations is an important element of today's strategic environment—one that has significant implications for the region and the world." The report goes on to state that the People's Liberation Army (PLA) is transforming from a mass army designed for protracted wars of attrition on its territory to one capable of fighting and winning short-duration, high-intensity

2. https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html

conflicts against high-tech adversaries dependent on "informatization." China's ability to project power is presently limited but it seems only a matter of time.

Significantly, China is perhaps the most assiduous student of U.S. military doctrine and operations, adopting and adapting, copying and countering, looking to play the game and to change the game. Fortunate for the United States, and like our nation, China is a prolific publisher of its military thinking.

The "Cost Equation" and Asymmetries

The cost of a military adventure is reflected along several dimensions, not all easily denominated in dollars and cents. One of those dimensions is human lives—U.S. combatants, theirs, and innocent civilians.[3] Others include international standing, the cost of materiel expended, the opportunity cost of manpower employed, and the loss of civil liberties and economic well-being for the civilian population. Table 1-1 illustrates the ways in which an asymmetric adversary would impose untenable costs on the United States, and the technology "drivers" that facilitate the imposition of such costs.

The current situation is that U.S. costs are increasing while the adversary enjoys a declining cost. The adversary enjoys a world awash in conventional weapons—a buyer's market, bargain prices. Commercial technologies obviate his development costs, and he requires a less diverse arsenal of weapons and tactics because the battlefield is known and local. The adversary devalues life; bears lower costs for training, rations, and quarters; brings mass to the force-on-force equation; and uses "human guidance" rather than more expensive technical guidance. Moreover, the adversary accepts more readily the use of weaponry that may endanger its user—*e.g.*, chemical, biological, and/or radiological weapons. This is not the case for the United States.

3. *Cf., CRS Report for Congress—American War and Military Operations Casualties:* Lists and Statistics, Order Code RL32492

Table 1-1. Imposing Untenable Costs on the United States through "Irregular Warfare" and Associated Technologies

"All's Fair in …War"	Technology Drivers

▪ Unconventional warfare—no holds barred—a time-proven technique against an otherwise superior conventional force
  ▪ Recent Lebanon example—Israel v. Hezbollah
▪ Threaten a long, protracted war of attrition
▪ Raise the level of violence and brutality
▪ Exploit the "home-field" advantage
▪ Expand and escalate by targeting U.S. homeland and key allies
	▪ Commercial off-the-shelf (COTS) information and communication technologies adaptable to coordinate military operations
	  ▪ Satellite and cellular phones, and internet
	  ▪ Commercial encryption
	  ▪ Personal Global Positioning System
	  ▪ Personal digital assistants (PDAs) w/ maps and images
	▪ COTS sensor technologies
	  ▪ Arrays of unattended sensors for tactical warning
	  ▪ Night vision devices
	▪ Adaptable weaponry
	  ▪ Shoulder-fired surface-to-air missile (SAM) and anti-armor
	  ▪ Integration of COTS sensors into seekers–"fire and forget"
	  ▪ Innovative explosives–thermobaric and fuel-air mixtures; new energies
	▪ Next-generation improvised explosive devices (IEDs)
	  ▪ Explosively formed penetrators (EFPs), sensors and networks–smart and mobile
	▪ Lethal "non-lethals"
	  ▪ Long-range acoustics, millimeter wave and laser dazzlers
	▪ WMD, esp. biotechnologies

In material terms, "war U.S.-style" is becoming increasingly costly. The United States employs higher and higher cost weaponry. Consumables are often too expensive for live-fire training. Often, more specialized elements require a more diverse arsenal, which complicates logistics and affords a smaller and smaller inventory, which means that stockpiles can be exhausted and stockpile replenishment may have a long lead-time. The United States also takes it upon itself to bear the high cost of cleanup—it almost seems as if to the vanquished go the spoils.

With respect to the human toll on innocent civilians, the U.S. strategy is to reduce "collateral damage." Through better command, control, communications, computing, and intelligence, surveillance, and reconnaissance (C4ISR); targeting; and precision weapons the United States has been able to reduce civilian casualties (Figure 1-1). The asymmetric adversary, however, is frequently disposed to try and force the United States to increase, rather than decrease, the grisly toll. In this endeavor, the adversary is often assisted by a media attuned to

the horrors of war. In applying such a cost-incurring strategy, the adversary has learned that one "on-camera" casualty is worth a multitude of dead and injured unseen in the living room.

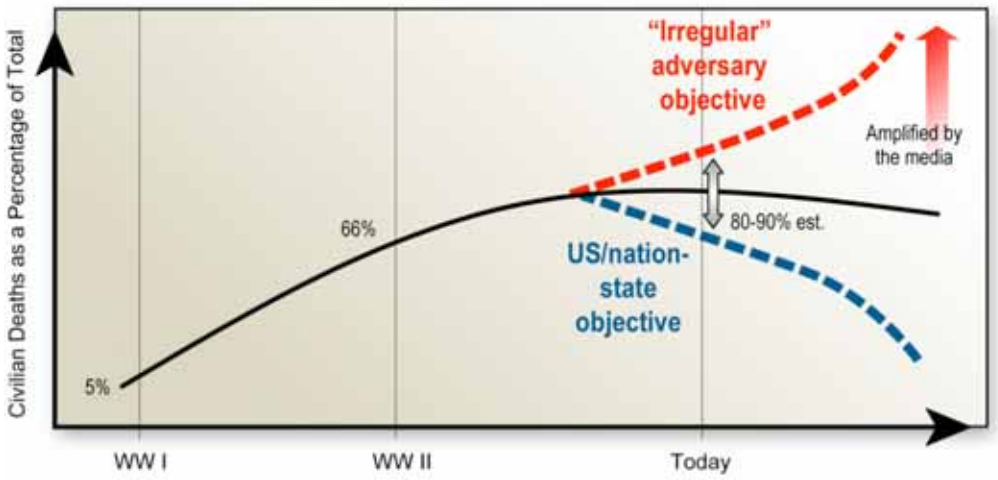


Figure 1-1. The Impact of War on Civilians and the Larger Geo-political Impact

Not infrequently, international clashes have been decided fatefully by one opponent imposing untenable costs on the other. The application of cost-incurring strategies is no stranger to the United States. On occasion, the nation has practiced it successfully, beginning with the Revolutionary War.[4]

The United States has also imposed costs on a strategic adversary on a grander scale. A grand example was the continuing development of penetrating aircraft, which caused the Soviets to spend hundreds of billions on air defense. Another example was the (first) intervention in Afghanistan when the administration abandoned a policy of playing the game of Cold War geopolitics according to the rules of the Brezhnev Doctrine and challenged it both directly and indirectly. Having identified the Soviet economy as the "strategic center of gravity," the United States "adopted an asymmetric and cost-incurring strategy to exploit the mismatch between the large and growing U.S. economy and the much smaller Soviet economy."[5] The Strategic Defense Initiative (known also as "Star

4. A subsequent section of this report comments at length on the frequency with which smaller, less well-endowed nations prevail over stronger opponents.
5. Mackubbin T. Owens, *The "Correlation of Forces," Then and Now, http://www.ashbrook.org/publicat/oped/owens/04/cof.html Feb2004*

Wars") would raise the arms race to a new plateau the Soviets could not afford to reach. These measures, *inter alia*, spun the Soviet Union into tactical retreat, which "soon constituted a strategic retreat of a kind that Lenin or Stalin could never have imagined, culminating in the collapse of the Soviet Union itself."

But, the United States is not the only successful practitioner of cost-incurring strategies. Witness the Vietnam War. Now, too, the nation finds itself on the receiving end with radical Jihadists, on the one hand, seeking to diminish U.S. influence in the Middle East, and China seeking to diminish U.S. influence in Asia by adopting an "anti-access" strategy.

In a sense, the meaning of victory remains constant: the achievement of one's target political objectives. What changes is the expansiveness of those objectives. The United States must constantly re-evaluate those political objectives to determine which are unobtainable without resorting to military power, but perhaps too costly for military solution. Learning how to wield better all other instruments of national power would seem like an excellent idea. Winning without fighting is surely preferable to the other alternatives, fighting without winning, even fighting and winning.

Potential Military Applications

No matter how desirable a set of "scenarios" may be for planning, the scenarios themselves have modest positive value and may even have negative value. Scenarios, intended only as notional examples, tend to take on an undeserved reality. As a compromise, Table 1-2 offers a smorgasbord of characteristics that help map the terrain of conflict. In this table, the "class" of crisis maps to a major military mission or objective. The characterization and examples of adversaries is self-explanatory. The attention of the reader is directed at the right-most column, which illustrates the kinds of things that might change the cost equation in conflict with the United States.

Table 1-2. The Spectrum of Crises: Types, Adversaries, Examples, and Complications

Class	Nature of Adversary	Example	Changing the Cost Equation
Classic defense of ally	Large rogue	Korean War	WMD coercion
	Regional hegemon	▪ China invades Taiwan ▪ Russia invades Ukraine ▪ Turkey invades or coerces Kurdistan	▪ Access denial ▪ Strikes and blockade ▪ WMD coercion
Seize and protect critical resources	Islamist revolutionaries	Saudi Arabia, Kuwait	With and without WMD threats by third party
Invasion and regime change	Potentially large or populous state well prepared for irregular warfare	Iran	▪ C4ISR vulnerabilities ▪ Potential for long-term stabilization
Invasion and stabilize	Islamists, revolutionaries, etc.	Egypt and/or Saudi Arabia	*Global* Islamist Jihad
Deal with and recover from attack on homeland	State or non-state actor	Islamists with WMD	▪ Multi-modal ▪ Multiple, near simultaneous

Toward a (New?) Theory of (New?) War

War has been classically defined as the violent conflict between states where each tries to impose its political objective upon the other. While violence is timeless, states, which have been the critical actors for half a millennium, are themselves a relatively recent invention in the history of human conflict. Contemporary developments, however, have brought into question both the state-based nature of war and the need for physical violence. Non-state actors and cyber-based economic disruptions may change the character of warfare in this century.

Still, war as an extension of politics always has a purpose. Appreciating this purpose helps predict an opponent's strategy, tactics, and operations. Understanding the "why" helps anticipate the "who" and the "how." Absent this understanding, analyses of future threats tend to focus on worst case scenarios regardless of how likely they might be.

The United States is a nation-state with a superb conventional military atop a deep economic base. The concern, in this study, is only with adversaries capable of inflicting strategic damage—having the means, ways, and will—thereby, putting the outcome of any conflict in question. When a strategic adversary is a classical peer or near-peer it will have a national footprint and be more likely to directly engage U.S. military force. Other adversaries, classically "non-peer," may never present coherent forces against which the United States could strike and are more likely to attack soft targets rather than risk major losses by attacking hard targets.

Actors in war consist of a government, its people, and its military. In a peer, or nation-state, these three elements are distinct and clearly defined. Indeed, the law of war stipulates that the combatant forces—i.e., the military—be schooled in the law of war, be uniformed—i.e., identifiable—and be under positive command and control. Non-peers, like terrorist networks, observe none of these niceties. They may try to blend into the civilian, non-combatant population. Indeed, the only difference may be recruitment, which can wax and wane, giving comfort to the enemy or joining in directly. Instead of centralized leadership, such adversaries may act on general guidance from the center or merely presume their leaders' intent. Their hierarchy may be flat and all command and control may be local. In the extreme, non-state actors operating independently in tune with a common ideology, pose a conundrum: nothing to hold at risk in the service of deterrence, and no head to decapitate.

Losing a war is the failure to achieve one's own political objective and/or being on the receiving end of an adversary's agenda—failing to impose your will or finding yourself subject to his will. All losses are political, whether the result of physical or economic damage or, more rarely, simply the triumph of an opponent's message. Conversely, winning a war is the achievement of the political goal at an acceptable cost. As described elsewhere, victory does not always go to the better endowed, but more often to the more resolute. Of course, not all wars end with the clarity of a winner and a loser. Neither may win, both may lose, each can become exhausted—a mutual loss of will.

Despite the popular distinction between symmetry and asymmetry, no adversary knowingly plays his weakness into an opponent's strength. Symmetric conflict is merely a miscalculation.

Target: United States

Seen through hostile eyes from without, the United States has three primary "weaknesses" or handicaps:

- plentiful soft civil and economic targets both here and abroad as a result of global presence
- a feedback loop from its citizens to their government
- a culture that places a high value on life—ours and theirs

Current and potential adversaries need not—indeed do not—have such handicaps and the consequences for misunderstanding this can be dire.

In this spirit, consider the relative appeal of various weapons to the non-peer adversary. Figure 1-2 illustrates the cost-benefit calculation for a non-state actor using a biological weapon. Biological warfare agents, never extensively used previously, pose the threat of an autonomous self-replicating agent—a new category of low-cost stealthy threats that can be released remotely, spread indefinitely, and overwhelm the present health care system (this phenomenon will be discussed in more detail in Part II of this report).

Note: PHS: Public Health System; FRP: Federal Response Plan; NDMS: National Disaster Medical System

Figure 1-2. The Cost-benefit Calculation for a Non-state Actor Using a Biological Weapon

The psychological impact of such an attack could be enormous as citizens, themselves, become unwitting, unwilling weapons. Quarantine can be a force multiplier for the adversary: its potentially enormous economic impact can be greater than the immediate threat itself. Whether or not the United States chooses to quarantine itself, other countries will not hesitate. The progression of biotechnology continually lowers the threshold for developing such a weapon, and many deadly agents exist readily in nature. (Similar analyses could be made for nuclear or other weapons systems or attacks.)

Thus, the United States must do a better job of seeing itself as the target sought out by its adversaries and appreciating the calculus they employ in planning their attacks and adapting their tactics.

Chapter 2. The Past: Fads and Phases in Warfare

The style and sequence of armed conflict can be described in many ways. Indeed, published students of military history often provide distinctive sequences of phases that characterize the evolution of warfare and not all of them agree. These differences largely reflect the discontinuities in the style and substance of armed conflict—the essence of this chapter. Sometimes the discontinuities are easily recognized; more often, they are apparent only in retrospect and from a distance. This point is important in that it reflects the difficulty that nations face in noticing ongoing, significant change and reacting to it in a timely way—in essence, the difficulty embodied in anticipating the next discontinuity and appreciating its timing.

National Security Policy Phases

Writing in 1954, Samuel P. Huntington argued that the history of the United States could be divided into three broad national security policy phases, each identified by broad, enduring national security policy objectives. To remain relevant each of the military services had to modify their "strategic concepts" to conform to the requirements of each unique era. Huntington described these eras as following:

1. **Continental Era** (1783–1889) where the objective was to secure the continent and preserve the Union. The United States abstained from entangling alliances, engaged the rest of the world with naval forces only, and the dominant service was the Army.
2. **Oceanic Era** (1890–1946) where the objective was to secure the maritime approaches to the hemisphere to allow more active participation in world affairs. During this period, the United States began to send large expeditionary forces overseas. The dominant service was the Navy.
3. **Transoceanic Era** (1947–1990) where the objective was to deter and contain a hostile ideological continental peer located across the oceans. It was an era replete with entangling alliances as the United States began to base combat forces overseas. The dominant service, initially, was the Air Force.
    - In 1961, the "dominant service resource allocation model" is replaced by a standing joint forces resource allocation model. The planning,

programming, and budgeting system "locks in" the 1/3-1/3-1/3 resource allocation model.

- By 1973, the U.S. armed forces shift from a conscription force to a standing all-volunteer, professional total force (active and reserve components).
- By 1986, the search for the best means to achieve unified action of the armed forces ends with the passage of the Goldwater-Nichols Act.
- In 1989, the era ends unexpectedly with the demolition of the Berlin Wall and, a year later, VII corps is on the way to fight in the first Persian Gulf War.

While not part of the Huntington framework, the **Global Era** describes well the aftermath of the Transoceanic Era. During this era, the United States has assumed a new "joint expeditionary posture" with fewer forward-based forces and most of its combat power based on sovereign soil. The nation's exterior basing network resembles the British "coaling station" network with Europe as a "strategic trampoline" and over 90 status-of-forces agreements and numerous "gas-and-go" agreements. Global strike forces now focus on conventional attack and the United States maintains a global command, control, communications, and intelligence (C3I) network providing support to the operational/tactical warfighter.

Through all of these phases, the United States maintained an expeditionary posture. But the use of the military became more frequent, with less "slack time" through each succeeding era, as shown in Figure 1-3. The U.S. national security aperture has progressively widened from a continental, to oceanic, to transoceanic, to global focus. Economic and technological globalization has led to global problems such as proliferation, terrorism with global reach, and radical extremists loosely but globally networked. Moreover, the lack of a peer military threat has allowed an unprecedented operations tempo and ever more frequent major combat operations.

Since the creation of the nation, the U.S. military has been called upon many times. They have fought with distinction in many places and under many conditions. Overall, neither the frequency of deployment nor the locale appears to be predictable, as borne out in Figure 1-4. Contemporaneous events, equally unpredictable, overall, are the forcing factor.

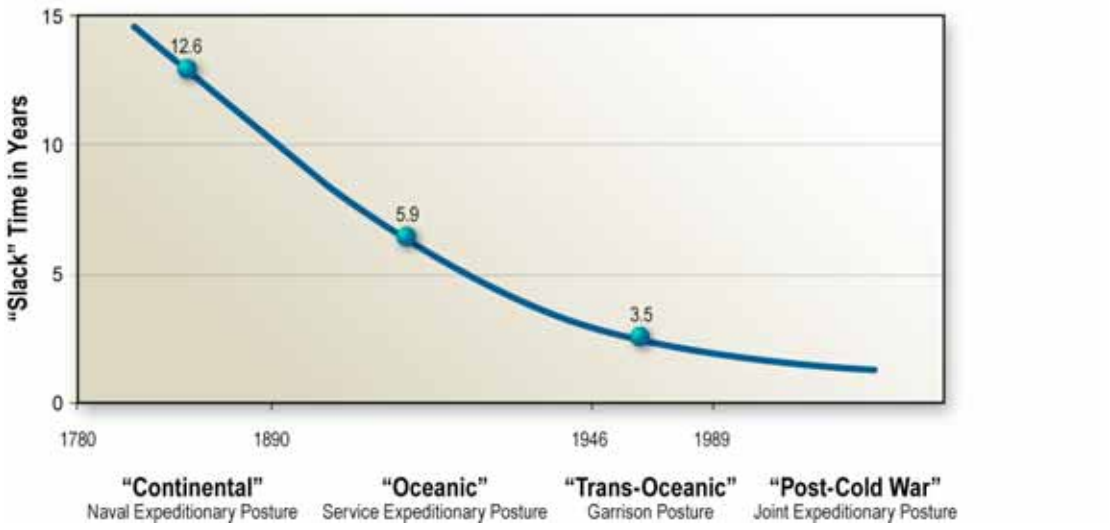


Figure 1-3. The Increasingly Frequent Deployment of U.S. Forces and the Consequent Reduction in "Slack Time"

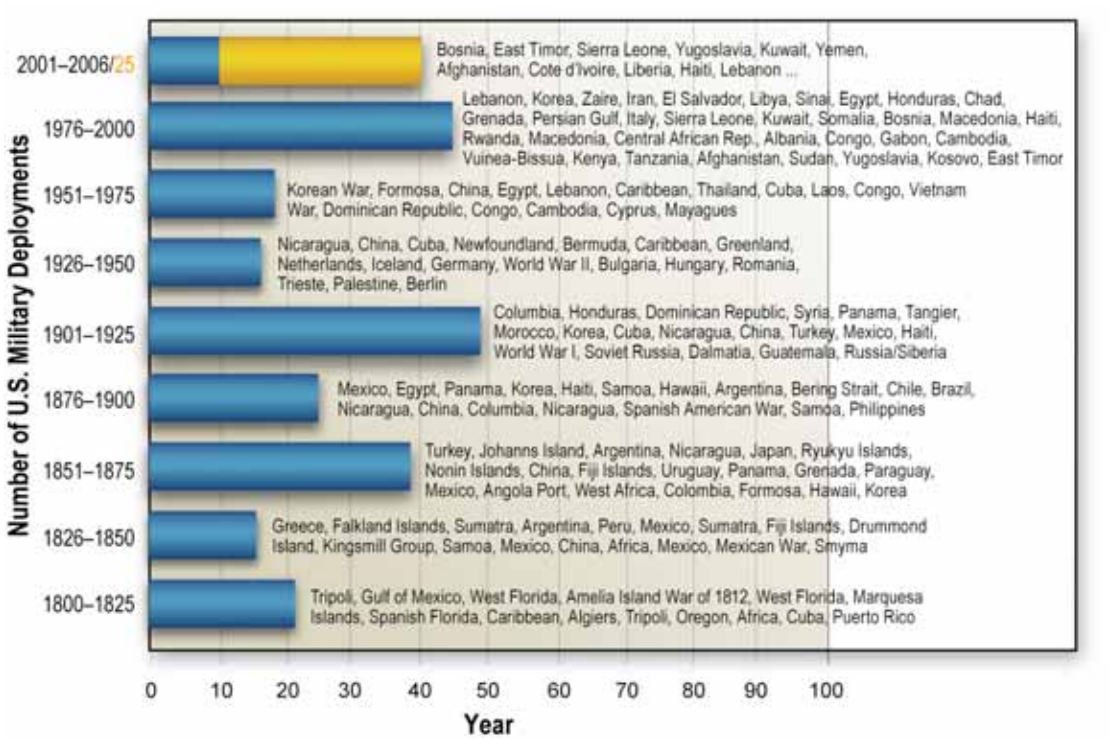


Figure 1-4. U.S. Involvement in Military Action, 1800–2006

The Revolution in Military Affairs

"Generations" of Warfare

The four generations of modern war, according to its author,[6] began with the Treaty of Westphalia in 1648, which ended the Thirty Years' War and established a "state monopoly" on war. Previously, many different entities had fought wars—families, tribes, religions, cities, business enterprises—using not just armies and navies but also, for example, bribery and assassination. For much of the intervening years, state militaries have found it difficult to imagine war in any way other than fighting state armed forces similar to themselves. In his book, Lind describes the four generations of war as follows:

1. **The First Generation** of modern war, roughly 1648 to 1860, was war of line and column tactics, formal battles, and an orderly battlefield—one that created a military culture of order. Much that distinguishes "military" from "civilian"—uniforms, saluting, gradations, and rank—developed during this era to reinforce the culture of order. Alas, in mid-19th century, rifled muskets, then breech loaders and machine guns, made the old line and column tactics first obsolete, then suicidal. Ever since then, the contradiction has grown between the orderly military culture and the increasing disorderliness of the battlefield.

2. **Second Generation** warfare answered this contradiction by the end of World War I with mass firepower, mostly indirect artillery fire. The goal was attrition, and the doctrine was summed up by the French as, "The artillery conquers, the infantry occupies." Centrally-controlled firepower, infantry, tanks, and artillery, were choreographed in a "conducted battle" where the commander was the "conductor" of the orchestra.

   Second Generation warfare came as a great relief to soldiers (or at least their officers) because it preserved the culture of order. Focusing on rules, processes, and procedures, obedience trumped initiative and discipline was imposed top-down. Having learned Second Generation warfare from the French during World War I, it remains the American way of war—"putting steel on target," though aviation has supplanted artillery as the source of most firepower—despite the Marine's formal doctrine, which is Third Generation maneuver warfare.

---

6. William S. Lind, *Understanding Fourth Generation War,* 15 Jan 2004, www.antiwar.com.

3. **Third Generation** warfare, also a product of World War I, was developed by the German Army, and is commonly known as Blitzkrieg or maneuver warfare. Here, the emphasis is not on firepower and attrition but speed, surprise, and mental as well as physical dislocation. Tactically, in the attack a Third Generation military seeks to get into the enemy's rear and collapse him from the rear forward. Instead of "close with and destroy," the motto is "bypass and collapse." In the defense, it attempts to draw the enemy in, and then cut him off. War ceases to be a shoving contest, where forces attempt to hold or advance a "line;" third generation warfare is non-linear.

   Not only do tactics change in the Third Generation, so does the military culture. A Third Generation military focuses outward, on the situation, the enemy, and the result the situation requires, not inward on process and method. Orders themselves specify the result to be achieved, but not, generally, the method ("Auftragstaktik"). Initiative is more important than obedience (mistakes are tolerated, so long as they come from too much initiative rather than too little), and it all depends on self-discipline, not imposed discipline.

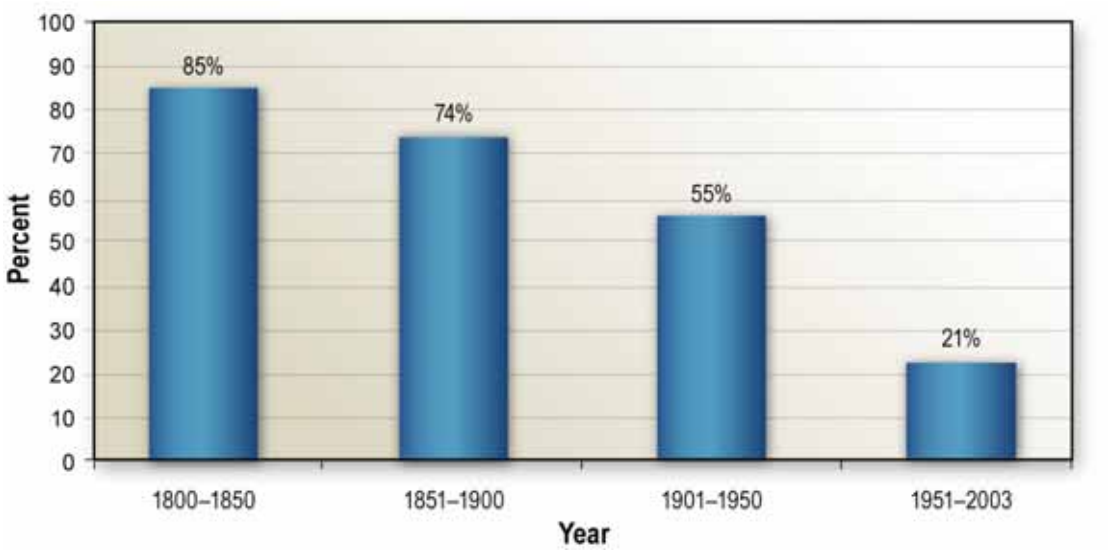
4. **Fourth Generation** war undoes the state monopoly on war and is marked by a return to a world of cultures, not merely states, in conflict. Here, invasion by immigration can be at least as dangerous as invasion by a state army. Nor is Fourth Generation warfare merely something that is imported, as was the case of 9/11. At its core lies a universal crisis of legitimacy of the state, and that crisis means many countries will evolve Fourth Generation war on their soil.

One key to success in Fourth Generation war may be "losing to win." Where the initial invasion destroys the state, it provides fertile ground for Fourth Generation forces. In a world where the state is in decline, if you destroy a state, it is very difficult to recreate it. While war against another state may be necessary, one should seek to preserve that state even as one defeats it. Grant the opposing armies the "honors of war," tell them what a fine job they did, make their defeat "civilized" so they can survive the war institutionally intact, and then work for your side. This approach would be similar to 18th century notions of civilized war and contribute greatly to propping up a fragile state. Humiliating the defeated enemy troops, especially in front of their own population, is a serious mistake.

Victory to the Mighty, or to the Resolute?

It is relatively easy to rank the military prowess, size, and resources of contenders, but it is a good deal harder to predict the outcome of any match. Victory does not always favor the largest, best-endowed side. Frequently, it comes down to "will," which may be uncorrelated with raw capability. Weaker opponents win a surprising number of times, as Figure 1-5 shows.

- Since World War II, weaker opponents have outdone stronger opponents in 39 percent of wars (Sullivan).[7]
- Over the past 200 years, weaker opponents have outdone stronger foes 41 percent of the time (DeMesquita).[8]



Source: Jason Lyall, Princeton University and Lt. Col. Isaiah Wilson III, U.S. Military Academy at West Point. The *Washington Post*

Figure 1-5. How Likely is it that Powerful Countries can Defeat Insurgencies?

7. Patricia L. Sullivan, "War Aims and War Outcomes: Why Powerful States Lose Limited Wars." *Journal of Conflict Resolution,* June 2007, Vol 51, No. 3: 496–524.
8. Bueno de Mesquita (2000).

The United States has

- won 81 percent of interventions where cooperation was not required
- won 44 percent of interventions with political aims; withdrew without achieving political objectives 56 percent of the time[9]

Based on these statistics, one may conclude that powerful nations tend to "win" when aims can be achieved by brute force, but more often "lose" when victory requires an opponent's "cooperation"—i.e., "winning their hearts and minds." As Richard Nixon declared in an earlier time, the war is not a test of power; it is a test of will and character.

Even earlier, C.E. Callwell,[10] a colonel in the British army, wrote in 1896 that a powerful force can easily lose if it does not fully understand the enemy, fails to describe clear objectives, or, in the worst case of all, pursues military objectives that do not contribute to the conflict's political goal. A larger obstacle to "winning" wars against insurgents—"small wars," as he called them—is that mere victory is not enough: the enemy must be thoroughly destroyed to the last, which means enormous civilian casualties. For most democracies, he explained, this is unacceptable. The level of violence and barbarism it would take to beat an insurgent force is an action most democracies would refuse to take. This keeps victory out of reach.[11]

How do Strong Nations Miscalculate?

At the risk of being repetitive, the outcome of a "war" depends not only on the relative military capabilities of the combatants, but also on their respective commitments to the war aims—their "resolve." It is relatively easy to measure and compare military capabilities, but much harder to estimate the respective resolve of the combatants. Resolve is increasingly important if the intent is not to annihilate the adversary or exact spoils of war but to change his mindset—i.e., to impose a new political agenda.

Historically, strong states appear to have focused on their might and neglected to account accurately for their will and, especially, the adversary's. The cost of victory is increasingly harder to estimate accurately as relative resolve becomes a

9. Patricia L. Sullivan, June 2007.
10. C.E. Callwell, *Small Wars,* 1896
11. *Cf.* Larry Kahaner, http://www.hnn.us/articles/31296.html

more influential factor in the outcome of a conflict. Generally, resolve needs to increase when an opponent's "cooperation" is needed, say, to achieve political objectives. If resolve is misestimated, powerful nations can be pushed beyond their cost tolerance and forced to withdraw. Thus, the probability that a strong state will prevail over a weak adversary declines as the need for cooperation to achieve aims increases.

Psychological research shows that cognitive biases in how people process information and evaluate risk predispose political leaders to favor military action over diplomatic solutions.

Such impulses may incline national leaders to

- exaggerate the evil intentions of adversaries
- misjudge how adversaries perceive them
- attribute aggressive behavior of the other side to deep hostilities, excusing their own provocations as being "pushed into a corner"
- be overly sanguine when hostilities start
- be overly reluctant to make necessary concessions in negotiations

These biases have the effect of making wars more likely to begin and more difficult to end. As has been noted: for the weaker, not losing is winning; for the stronger, not winning is losing. Of course, the preferred paradigm should be winning without fighting.

1990s: Happy Times for Military Planners

As a result of the Soviet Union's collapse and the U.S. victory in the first Gulf War, the 1990s gave rise to an era of strategic optimism. Analysts concluded that because of its edge in emerging technologies, especially information technologies, the U.S. position in the world was unassailable for the foreseeable future. As well, there was no "peer competitor" on the horizon capable of replacing the Soviet Union as an existential threat to the United States.

This apparent national security situation led U.S. planners in many cases to adopt simplified—if not simplistic—defense planning assumptions:

1. Challenges to U.S. security would arise primarily from regional powers and involve regional/theater contingencies featuring conventional major combat operations.

2. These likely adversaries would be smaller, less capable versions of the U.S.S.R.
3. The U.S. monopoly in strike, information technology, and stealth would constitute a barrier to entry for adversaries and would continue into the foreseeable future.

These assumptions led to major changes in U.S. force structure, including the "conventionalization" of the U.S. strategic bomber force and a shift in the focus of space and C3I programs from the strategic level to the operational/technological level. Planers assumed that since future wars would be short, "strategic speed" had become critical. Thus joint planners stressed such concepts as "rapid halt," "rapid decisive operations," "shock and awe," and "10-30-30." One consequence of perspective was a lack of focus on stabilization operations, also referred to as Phase IV.

Speed, Stealth, Precision, and Information

At the close of the last century, the peerless performance of the U.S. military was conditioned largely by speed, stealth, and precision. All three were enabled, in one way or another, by the information revolution—a revolution the DOD helped bring about. The troika of speed, stealth, and precision all embodied important physical aspects:

- Speed was the result of materials engineering and fabrication improvements but even these derived, in part, from advances in computational power and complexity. As important, speed of response resulted not only from V and ΔV but also from better, quicker, more universally available targeting information from our C4ISR capabilities.
- Stealth, too, rested on powerful design computational capabilities as well as materials.
- Precision most clearly resulted from navigational (GPS) capabilities as well as benefiting enormously from C4ISR.

DOD investments in command and control, communications, computing and remote sensing paid huge dividends in improved military capability. The investment horizon stretches back at least to 1943 when ENIAC—the first large scale, electronic, digital computer—was built for trajectory computations. There were many milestones along the way. Many, if not most, were funded by the Department, including the ARPANET and a succession of ever faster

supercomputers to feed the cryptologic maw. Among the innumerable competitive advantages to U.S. forces which leverage these investments include the following:

- information sharing across services and echelons
- pervasive communications, which enable coordination of activities across services and units
- common situational awareness, which promotes understanding across battle elements
- assistance in accurate and rapid decision-making
- precision geo-location and persistent sensors, which enable accurate tracking and targeting
- sensor-to-shooter links—and, in some cases, sensor-to-seeker links—that enable real-time tracking and targeting

These, in turn, support tactics based upon speed of maneuver and synchrony of action across service elements.

On the commercial front, as well, DOD utilization of Internet and commercial satellites and networks enabled rapid and effective access not only to information but also to the commercial transportation industry for movement of equipment and troops and access to other commercial services, such as SCADA [supervisory control and data acquisition] systems, that support warfighter. The U.S. reliance on commercial-off-the-shelf components also underscores U.S. reliance on technology. Further the indefatigable use of information technology—some would say overly dependent—has surely not escaped notice by potential adversaries.

Chapter 3. The Role of Technology: Weapons that Change War

While politics, religion, and the like may set the course of war, unequivocally technology can change the course of the war, as illustrated by these examples[12]:

- Catapults, invented by the Greeks in 400 B.C., were used in ancient and medieval times to hurl stones, spears, and other objects at fortifications. Te first war of the engineers?
- The Trojan Horse, in legend, epitomized the steady evolution of denial and deception. The stealth bomber of its day, or merely a glorified siege tower?
- Crossbows, invented in China and perfected in medieval Europe, propelled arrows with tremendous force as far as 350–400 yards and allowed soldiers to fire from great distances and avoid close contact with the enemy. Alternatively, the English long-bow—perhaps the AK-47 of its day—could deliver twice as many aimed shots per minute and permitted greater maneuverability.
- Gunpowder and cannons developed in the 1300s could demolish castle walls and blast through wooden ships.
- Rifled barrels and spin stabilization enabled longer range accuracy and the construct still competes well with "fin stabilization," first proven in the bow and arrow.
- Machine guns and "repeating rifles" like the Gatling gun and the Spencer Carbine first used in the American Civil War allowed for rapid, continuous fire, eliminating frequent reloading. Subsequently, the Maxim gun helped reverse the fortunes of the fixed defender.
- Minié Ball, a conical bullet with a hollow base that expanded when fired, used in the 19th century, which markedly improved precision over the round "musket ball."
- Tanks—armored combat vehicles equipped with cannon and machine guns—ended trench warfare with their caterpillar traction that could

12. Martin Van Crevald. Technology and War from 2000 B.C. to the Present. New York: The Free Press, 1989. Other examples selected from various Google searches.

bulldoze over trenches. First used at the end of World War I, they symbolized modern warfare.

- Combat aircraft, both bombers and fighter planes, changed the nature of war during World War II. Air superiority became critical to victory. "Strategic" bombardment of civilians reached new heights. In the Pacific, aircraft changed the nature of naval warfare.
- Submarines, too, changed the nature of naval warfare, which dramatically became three-dimensional. Submarines performed tactical missions such as enforcing blockades and denying access, and played a strategic role as a stealthy (and survivable) leg of the triad.
- Radar and navigation aids of the Second World War elevated aerial bombardment and air defense to a new plateau.
- Radio frequency command, control, and communications enabled battlefield coherence and paved the way for massed effects without necessarily massing men and machines into an inviting target.
- Nuclear weapons, developed in 1945, allow for massive destruction and, as with chemical and biological weaponry, became subject to treaty limitations.
- Smart bombs (or precision-guided munitions) hit their targets much more frequently and cause both fewer casualties and less damage to civilian areas.

Indeed, as described at the end of the previous chapter, at the turn of the century the pre-eminence of the U.S. military was based on a troika of speed, stealth, and precision. For the future, it seems clear that the information revolution has not played itself out, biology is resurgent, and nanotechnology is poised. Directed energy has been, and remains, an area of anticipated development.[13] How these will translate into changes in military fortune is legitimate speculation.

13. *Cf.* Douglas Beason, Los Alamos National Laboratory.

Chapter 4. Present Concerns: What Now?

The sovereignty of a nation-state, supreme within its borders, depends on the ability to defend those borders. Increasingly, sovereignty is challenged by new developments:

- "recognition of human rights as norms transcending internal laws;
- weapons of mass destruction that render the defense of state borders ineffectual for the protection of the society within;
- global and transnational threats such as environmental insults, migration, population expansion, disease, or famine;
- world economic regime that effectively curtails states in the management of their economic affairs; and
- global communications network that penetrates borders electronically and threatens national languages, customs and cultures."

The counter to some of the most pressing challenges to sovereignty may not be traditional military might, as the examples below delineate.

Trends

One commentator on the evolution of modern warfare and U.S. defense planning focuses on trends he believes have sufficient momentum that they will persist into the future.[14] Among the trends he identifies are:

- **Demographics**. Demographic decline and collapse of public health in Russia as unlikely to be reversed in one generation, which argues against a resurgence of Russian national power in the near term. Similarly, the aging and contraction of Japan's population suggests declining power. Consider, too, that the countries across the Mediterranean from Europe are growing in population, and there are already large Islamic populations in Europe with higher birth rates than the non-Islamic populations.

---

14. Stephen Peter Rosen, "The Future of War and the American Military—Demography, technology and the politics of modern empire", *The Harvard Magazine*, May-June 2002, http://www.harvardmagazine.com/on-line/050218.html

- **Technology**. Advances in information technology will continue, along with a diffusion of the ability to construct nuclear, biological, and chemical weapons.
- **Politics**. The dominance of democracies and international institutions in Europe seems likely to insure relative international peace, while the comparative rarity of stable democracies in Asia—from Turkey to Korea—together with the social dislocations associated with the process of industrialization and economic growth, suggest a more turbulent future for that populous continent.

Information Technology

The U.S. military, as never before, is dependent on information technology. Much of this is embedded in C4ISR systems without which our present methods of war prosecution might falter. As we learn daily, both military and commercial cyber space is vulnerable and defending it is daunting. Technological advance consistently seems to favor offense over defense. To make matter worse, despite hand wringing, the United States continues to allocate its scarcest resource—the most highly skilled—to computer exploitation and attack, rather than to defense.

Successful attacks on information systems are categorized according to whether the confidentiality of the data was breached, the integrity of the data compromised, or the availability of the data lost. Yet much of what plagues NIPRNET (the unclassified, but sensitive internal DOD network) today, is unauthorized access to data and occasional attempts at "denial of service"—that is, attacks on confidentiality and sometimes availability. In some ways, however, attacks on data integrity, particularly unrecognized attacks by the "high end" adversary, could represent the graver threat to military operations. Graver, still, than remote hacks via NIPRNET are supply-chain attacks and threats from recruited insiders. The consensus is that we have not really experienced, or perhaps not recognized, these yet. In the event, the result might be disruption of C4ISR services to the warfighter, leading to:

- degraded communications
- imprecise geo-location
- inaccurate and/or tardy targeting
- misinformation
- delayed and/or incorrect decision making at all levels

The net effect would likely be to jeopardize speed of maneuver and synchrony of action. The effects are undeniable and the attraction to the adversaries irresistible. It is essential that the United States establish the capability to "fight through" such calamities. More realistic exercises that force alternate courses of action would be a first step, as the Defense Science Board has recommended repeatedly.

Is Combat Force Sized to the Mission(s)?

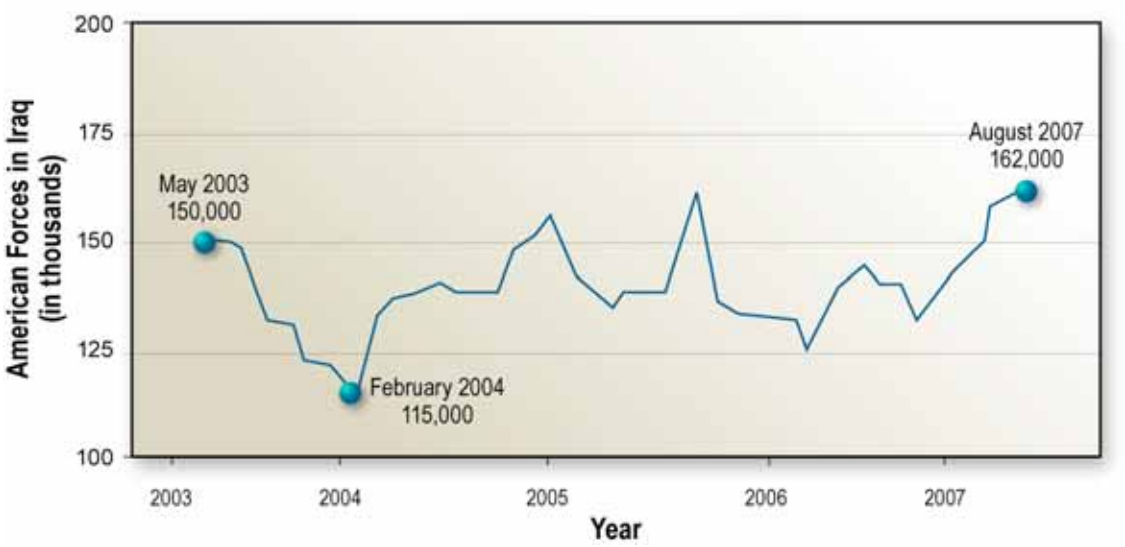
When a challenge to U.S. interests arises that requires military force, the nation must be ready to act when needed, not worry about raising the required number of combat troops once such a crisis presents itself. When U.S. combat forces are deployed, they need to be sent in sufficient quantity to indicate that the United States means business.

The current U.S. military deployment in Iraq focuses attention on whether U.S. forces, overall, are sized properly for the missions they are likely to be called upon to execute. It also focuses attention on whether force policy and force composition are adequate. Even if the size of the current force is adequate, at more than a million members, whether enough of the force is trained for the right missions is in question. Today, there is more "tail" than "tooth"; few forces are trained for stabilization and reconstruction; and members of the reserve components are being used at unprecedented levels, while many likely assumed they would not be deployed for years on end. Different missions call for different force inventory (such as a greater number of soldiers, properly trained and prepared for years of occupation).

The immediate concern, illustrated in Figure 1-6, is that keeping well in excess of 100,000 troops in Iraq through 2008 will severely strain the military. Indeed, coupled with the desire to ensure that all active-duty Army units get at least 12 months[15] at home between deployments, the Army already has found it necessary to extend tour length in Iraq from 12 to 15 months. The Army National Guard and the Army Reserve are still slated to serve 12-month tours. All reserve component personnel, including the Army National Guard, will now

15. Secretary Gates is quoted as hoping to achieve a "rotation goal for army active duty forces of 12 months deployed and 24 months at home." BBC News, http://news.bbc.co.uk/1/hi/world/americas/6546925.stm

be mobilized for a maximum of 12 months at a time, with the goal of five years at home before their next mobilization.



Note: All numbers are end-of-month estimates or latest available for current month.

Source: The Brookings Institute

Figure 1-6. Troop Strength in Iraq

There are proposals to increase the size of the land component, the Army and Marines, by as much as 100,000 troops to supplement the existing 500,000 plus troops. In February 2007, the Secretary announced that DOD will be increasing the permanent end strength of the Army and Marine Corps by some 92,000 over the next five years. According to some, that is the minimum required to maintain presence in the world's hot spots—Iraq and Afghanistan today—and be prepared to defend U.S. interests around the world wherever challenged. That challenge might come elsewhere in the Middle East or in Korea, Taiwan, or the Horn of Africa, or in some location not yet on the radar screen. As previously stated, available forces would need to meet such challenges; and it is unlikely that strategic warning or foresight would allow time to recruit, train, and equip new forces.

Underscoring the contention that the U.S. Army is undersized, last year, the Pentagon reportedly was forced to deploy the 82nd Airborne Division's "ready brigade" to Iraq. This is the unit that is supposed to be on call to respond to a crisis anywhere on a moment's notice. Indeed, Secretary Gates, himself, admitted that he had "…two concerns about the state of the U.S. military. One was that the Army and the Marine Corps were not big enough to accommodate the multiple

missions that they had been given over the past dozen years or so. The second was the use and condition of the National Guard."[16]

A substantial fraction of today's military burden is borne by guard and reserve forces, themselves hard-pressed to fulfill their assignments. Indeed, there has been a dramatic shift over the last decade in the role and capabilities of the National Guard. As Secretary Gates confirmed, "For much of the last century, the Guard was largely considered a strategic reserve, standing by in case of a mass mobilization. It was not a priority for funding and equipment, even though its members had served in every conflict from the Revolutionary War onwards. Since September 11, we've seen a remarkable transformation of the Guard—from a strategic reserve to a fully operational reserve that is an integral, indeed an indispensable, part of America's pool of forces used in Iraq, Afghanistan, and elsewhere in the broader Global War on Terror."

These positive changes notwithstanding, a larger problem looms. As the Defense Science Board has observed previously, although the U.S. military may manage to reduce the duration of the initial combat phase, so-called "Phase IV" operations have proved more resistant and historically such operations average around a decade in length. Were the U.S. military to engage more frequently than once a decade—as it has, recently—then the cumulative requirement for U.S. military forces would rise monotonically (and endlessly). Of course, a helping hand from allied and coalition forces can ease this burden, but it still appears crushing.

Recently, Army Lt. Gen. Douglas Lute, President Bush's new war adviser,[17] said in an interview that frequent tours for U.S. forces in Iraq and Afghanistan have stressed the all-volunteer force and made it worth considering a return to a military draft.[18]

---

16. Secretary of Defense, Robert M. Gates, speaking before the Senior Leadership Meeting of the National Guard, 27 February 2007, http://www.defenselink.mil/speeches/speech.aspx?speechid=1128
17. Deputy national security adviser with responsibility for ensuring efforts in Iraq and Afghanistan are coordinated with policymakers in Washington.
18. National Public Radio's "All Things Considered," 10 August 2007, http://www.foxnews.com/story/0,2933,292949,00.html

American Victory versus American Liberties

There has always been a tension between steps the government takes to secure the homeland and the individual liberties of its citizens—the challenge of mobilizing a free society.

- During the Civil War period what has been called a constitutional dictatorship suspended civil liberties, including *habeas corpus*.
- During World War II, a crisis government subjected its citizens to rationing, price controls, and blackouts, and interned many of them.

Under massive assault, a democracy will turn to extreme measures it would not ordinarily use in peace times, infringing on civil rights and suspending due process. When the crisis is declared over, the liberties are returned. This begs the question, of course, of who decides when or whether the crisis is over?

Chapter 5. The Future: What is New?

As skeptics predicted, and events such as 9/11 and the war in Iraq have demonstrated, adversaries have adapted to American power by adopting "asymmetric" responses to U.S. advantages. The result has been the emergence of trends, as described in this chapter, which undermine older U.S. planning assumptions and require rethinking the character of future war.

Technical Innovation—Military Revolution

As discussed previously, the technology vectors that loosely characterized the ascendancy of the U.S. military at the end of the 20th century are "speed," "stealth," and "precision," along with the general application of information technology to command and control and to situational awareness. It is likely that none of these vectors has played itself out, as yet. Inevitably, however, the United States will begin to face diminishing returns and, worse, potential adversaries will threaten to catch up. Worrisome, too, would be counter-stealth advances and, of course, threats to U.S. information dominance by attacking the nation's information technology infrastructure. Perhaps worst of all would be technological advances in the development, manufacture, and dissemination of WMD agents, although all the steps are probably within reach of a determined adversary currently.

Nation-State versus Stateless Nation

As Bobbitt has so clearly stated, for five centuries it has taken the resources of a state to destroy another state.[19] Only states could muster the huge revenues, conscript the vast armies, and equip the divisions required to threaten the survival of other states. Indeed, as Bobbitt points out, posing such threats, and meeting them, created the modern state. In such a world, every state knew that its enemy would be drawn from a small class of nearby potential adversaries with local interests. But this is no longer true, owing to global interests, global reach, advances in international telecommunications, rapid computation, and methods of mass destruction.

---

19. Philip Bobbitt, *The Shield of Achilles—War, Peace and the Course of History,* 2002.

Others have remarked similarly, noting that in the 20th century—through the world-war period and super-power confrontation—wars between nation-states vastly overshadow other armed conflicts within the territories of existing states or empires.[20] Indeed, at the turn of the 20th century Hague conventions codified the rules of war on the presumption that conflicts were to take place primarily between sovereign states. There was to be a bright line between war and peace—conflicts starting with a declaration of war and ending with a treaty of peace. A similar immutable distinction could be made between combatants—"uniformed" and thus recognizable as belonging to an organized armed force—and non-combatants, civilians who deserved protection in time of war, insofar as possible.

Changing Character (not Nature) of War

In the 1990s, it was not unusual for planners to claim that emerging technologies had changed "the very nature of war." But the nature of war—as best described by the Prussian "philosopher of war," Carl von Clausewitz—remains constant. The essence of war is the use of force by one actor to impose his will on an adversary—not an inanimate object, but an active will—who is trying to do the same to the former. Thus, adversaries respond to our actions by acting in unpredictable ways.

On the other hand, the "character" of war can continuously evolve. Thus, a weaker adversary can adopt various modalities of war to engage and defeat a stronger power. Success in war has traditionally gone to the most adaptive side that can bear the costs of the conflict.

Multi-Dimensional Warfare

Nevertheless, war, properly understood, is always multidimensional. In the era of state-on-state warfare, the traditional or conventional category was central, but combatants also pursued strategies to exploit irregular capabilities—guerrilla warfare, insurgency, or disruptive attempts, such as acts of terrorism, to undermine an enemy's public support for the war. But a particular form of multidimensional warfare may constitute the most demanding challenge to American planners in the future: "complex irregular warfare."

---

20. Eric Hobsbawn, *The Future of War and Peace, see also The Age of Extremes: A History of the World, 1914-1991.* New York, N.Y.: Random House, Inc. 1996.

Complex Irregular Warfare

Characteristics of complex irregular warfare include the likelihood that future adversaries will be "hybrids." These hybrid threats will seek to raise the potential cost of U.S. military action by adopting aspects of all of the warfare categories.

An example of a prototype hybrid is Hezbollah. During the 2006 war with Israel, Hezbollah exhibited both state-like capabilities—long-range missiles, anti-ship cruise missiles, sophisticated anti-armor systems, armed unmanned aerial vehicles, and signals intelligence—while still skillfully executing guerrilla warfare. Combining the two approaches complicates U.S. planning and execution.

But hybrid warfare is not only a phenomenon associated with the "low end" of the spectrum of conflict. There is no reason that a future peer competitor would restrict military competition with the United States to only the "traditional" category. It would logically also try to confront the United States asymmetrically in those areas where the United States is perceived to be less capable than in the traditional category. The publication in China several years ago of *Unrestricted Warfare* indicates the potential of hybrid complex irregular warfare at the "upper end" of the spectrum of conflict.

"Lawfare"

In general, complex irregular warfare exploits the political effects of a conflict, seeking to undermine the legitimacy of U.S. military actions. Thus it exploits "lawfare," the use of the rules of warfare against the United States (while ignoring these rules themselves), by, for example, taking refuge among the civilian population in an attempt to maximize civilian casualties. Such casualties are magnified by the proliferation of media assets on the battlefield, to the advantage of our adversaries. Complex irregular warfare is, above all, a battle of perceptions.

History of the Law of War

Rules regulating the practice of warfare date back to ancient societies.[21] However, these regulations were more a matter of custom and philosophy than

21. *International Law Reports,* vol. 110, Elihu Lauterpact, C.J. Greenwood, A.G. Oppenheimer (eds), Cambridge University Press, 1998, p. 429 (recounting a passage in the Hindu epic *Mahabharatha,* in which the hero Arjuna refuses to use a weapon of mass destruction because to so would be contrary to religion and the laws of war).

of law, and the brutality of the battlefield often did not reflect humanitarian constraints.[22] As Christianity took root in Europe, canon lawyers and philosophers began to systematically explore theories of just war. In 1625, in the midst of the devastating Thirty Years War, Hugo Grotius published his watershed work, *De Jure Belli ac Pacis* (*On the Law of War and Peace*), which set the theoretical tone for modern international law, setting its foundations upon natural law while providing a structure that housed the pragmatic application of political affairs.[23]

Legal codification of the laws of war is thought to have begun in 1863, during the American Civil War with the Lieber Code, adopted as General Orders no. 100 of the Union Army.[24] In Europe, the massive suffering of nearly 40,000 soldiers wounded at the battle of Solferino inspired the Swiss businessman, Henri Duant, to found the Society of the Red Cross (later, the International Committee of the Red Cross).[25] The Red Cross drew up the first Geneva Convention in 1864, which set out rules for the care and treatment of wounded soldiers; ten nations became signatories by the end of that year.[26] The Geneva Conventions evolved and expanded, and, along with other treaties like the Hague Conventions of 1898 and 1907, became the authoritative source of the laws of war.

Contemporary Problems

Two major problems confront the United States in its campaign against international terrorism, commonly referred to as the Global War on Terror (GWOT). The first is how to apply the traditional laws of war to an unconventional conflict. The second, and related problem, is the complications caused by the attempts by various actors (including U.S. lawmakers, international governments, and non-governmental organizations and associations) to bring the laws of war under the rubric of the criminal justice system.

---

22. *Ibid.* at 430. The Second Lateran Council of the Catholic Church condemned the use of the crossbow and siege machine as "deadly and odious to God," but the Church's finding had little effect on the battlefield.
23. Arthur Nussbaum, *A Concise History of the Law of Nations,* New York: Macmillan, 1947, pp.2-3.
24. Howard S. Levie, "History of the law of war on land," *International Review of the Red Cross*¸ no. 838, p. 339, (2000), available at http://www.icrc.org/Web/Eng/siteeng0.nsf/html/57JQHG.
25. "From the Battle of Solferino to the First World War," website of the International Committee of the Red Cross, available at http://www.icrc.org/Web/Eng/siteeng0.nsf/html/57JNVP. "From the Battle of Solferino to the First World War," website of the International Committee of the Red Cross, available at http://www.icrc.org/Web/Eng/siteeng0.nsf/html/57JNVP.
26. *Ibid*

In the wake of the 9/11 attacks, President Bush issued a military order that provided for the apprehension and trial by military commission of terrorists and co-conspirators responsible for the attacks.[27] The administration claimed that al Qaeda terrorists and Taliban fighters were not protected by the Geneva Conventions because, as a terrorist organization, they were not members of the "High Contracting Parties," that are signatories to the Conventions.[28] In the U.S. Supreme Court case, *Hamdan v. Rumsfeld*,[29] the Court disagreed with this position, and held that all persons detained by the United States in the GWOT are protected by Common Article 3 of the Geneva Conventions. The Court also held the military commissions' process to be invalid, and invited Congress to participate in setting up a framework for such commissions that would be legitimate.

The *Hamdan* decision is widely criticized because many believe it misapplies Common Article 3, which was designed for conflicts "not of an international nature." The Bush administration, and many experts, claimed that the GWOT was an international conflict, but the Court disagreed, writing that international conflicts can only be waged between nation-states.

As an answer to *Hamdan*, Congress enacted the Military Commissions Act of 2006, establishing a process for military commissions for the detainees at Guantanamo Bay, Cuba.[30] The most controversial provision of the act is the limitations on U.S. courts to hear habeas corpus petitions by the detainees. The act provides the U.S. Court of Appeals for the District of Columbia with exclusive jurisdiction to review final decisions by the military commissions, and challenges by detainees as to whether the Combatant Status Review Tribunal properly found them to be enemy combatants.[31] The challenges to the constitutionality of the Military Commissions Act of 2006 will probably rest on whether or not detainees have a right to habeas review in U.S. courts.

---

27. Military Order, Detention, Treatment, and Trial of Certain Non-citizens in the War Against Terrorism, 66 Fed. Reg. 57, 831-834 (Nov. 16, 2001).
28. High Contracting Parties are the signatory nations of the Convention. The Taliban fighters were determined not to be prisoners of war because they did not follow the requirements to distinguish (*i.e.*, identify) themselves in battle. *See* Third Geneva Convention Relative to the Treatment of Prisoners of War, Art. 4(A) 1-2, belligerents (those taking part in hostilities) are required to be either a member of the regular forces, or to (1) be apart of a chain of command, (2) wear a fixed distinctive sign recognizable from a distance, (3) carry arms openly, and (4) comply with the laws of war.
29. 126 S. Ct 2749 (2006).
30. Pub. L. No. 109-366, 120 Stat. 2600 (2006.
31. The CSRTs were set up to comply with article 5 of the Third Geneva Conventions that requires a hearing to determine the status (*e.g.*, lawful combatant, unlawful combatant, non-combatant) of those captured

The second problem with applying the laws of war in the GWOT is an attempt to undermine the use of the traditional laws of war, and replace them with criminal trials. Since the beginning of the GWOT, there have been those who insist that terrorist detainees should be treated as criminals rather than belligerents, and such voices have gained volume in recent times.[32] The argument is that trying terrorists as criminals rather than belligerents would de-legitimize both their actions and their cause, while at the same time providing a transparent and politically advantageous legal process; whereas treating them as warfighters provides them with undeserved prestige, and trying them by commissions undermines the United States' reputation as a nation of justice.

The problem with this conflated approach is multileveled. First, criminal trials involve complex rules of evidence that would undermine many attempts to convict a person captured on the battlefield or captured using classified evidence and protected sources. Putting the warfighter into the position of forensic expert in the middle of mortal combat would be an undo burden. To expect soldiers in battle to have to simultaneously concern themselves with rules of evidence would force another level of risk into an already life-threatening situation and would be unacceptable. In addition, given that Americans are outraged when common criminals walk free on legal "technicalities," is it hard to imagine that they would be willing to let a terrorist walk free because the circumstances of his capture did not meet the intricate standards of evidence, such as reading them Miranda rights on the battlefield?[33]

Secondly, the laws of war are designed to reward those who follow them and punish those who do not. If suspected terrorist detainees were provided criminal trials, they would be receiving far more protections than captured belligerents who follow the rules of war and are held as prisoners of war. Therefore, the laws of war do not require charges to be filed in order to hold captured enemy belligerents because the purpose of detaining belligerents is to keep them off the battlefield, not to try them. Lawful belligerents have a legal right to kill, and

---

32. For instance, a recent *New York Times* op-ed piece by former NATO commander General Wesley Clark and law professor Kal Raustiala called for terrorists to be treated as criminals, *see* "Why Terrorists Aren't Soldiers," Wesley Clark and Kal Raustiala, *New York Times* , Aug. 8, 2007. *See also* "Bush Advisors Weigh Closing Guantanamo Bay Prison Sooner," David Stout, New York Times, June 22, 2007.

33. Mary Jo White, former United States Attorney for the Southern District of New York, speaking from her experience prosecuting the terrorists of the 1993 World Trade Center bombing, stated in a conference that military commissions are preferable to criminal trials because of the criminal justice system is not equipped to handle the classified evidence needed to convict terrorists. *George Washington Law Review Symposium,* Oct. 19, 2006.

therefore cannot be tried for killing the enemy, if done in the course of adhering to the laws of war. In addition to the tit-for-tat protection of the warfighter, one of the main goals of the laws of war is to establish constraints on warfighting to protect civilians. Combatants who hide among the civilian population ultimately draw fire upon innocents. Were terrorist detainees granted all the protections of a criminal trial, it would ultimately undermine the incentive to follow the laws of war and their humanitarian purpose.[34]

Future of "Lawfare"

Although the enemy has changed drastically, this study is not recommending a change in the laws of war, but rather a change in the nation's approach to understanding, promulgating, and applying them. DOD could adopt important policy changes to enable these goals.

Asymmetric, Cost-Incurring Strategies

Access Denial

Other characteristics of future war include the adoption by adversaries of asymmetric "access denial" strategies to undermine the cornerstone of U.S. global military power: the ability to project and sustain substantial military forces at great distances from the continental United States. In general, there are a number of points at which an adversary may attempt to derail U.S. power projection.

As the United States is deciding to project power, an adversary may attempt to deter, by threatening actions that would make the cost of power projection too high. As the United States is deploying its forces to ports and airfields, an adversary may attempt to disrupt the deployment by means of terrorist attacks, sabotage of transportation means, and the like. As the United States is transporting its forces to the theater of action and attempting to debark, an

---

34. *See* William H. Taft, IV, "The Law of Armed Conflict After 9/11: Some Salient Features" 28 *The Yale Journal of International Law.* 319, 320-1 (2003) ([I]t is important to recall why the Convention lays down such specific criteria for determining which combatants are entitled to the status of POW [prisoner of war] . . . Jean Pictet . . . called Article 4 of the GPW [Geneva Convention Relative to the Treatment of Prisoners of War] "in a sense the key to the Convention." . . . [W]hile Article 4 expressly entitles the legitimate soldier to the GPW's protections, it real beneficiaries are the civilians who make up the mass of our societies. It *requires* soldiers to adhere to certain basic principles, such as distinction and compliance with the law, which serve first and foremost to protect civilian populations).

adversary will try to deny entry to the U.S. force by military and political means, *e.g.*, attacks and threats against U.S. allies in the region. And as U.S. forces establish a lodgment and begin offensive operations, an adversary will seek to defeat U.S. forces.

Additionally, there are two "indirect" ways, already referred to, in which an adversary may attempt to derail U.S. power projection. One, a major focus of the overall study, is to cause a domestic calamity, which would force the President to divide forces between combat abroad and support at home. Another, also a major topic of this study, is to disrupt supply so that sustained effective presence abroad is impossible.

"360 Degree Warfare"

In the past, adversaries have focused their efforts on the last two points, denial, and defeat. But in the future, an adversary's most cost-efficient actions may be to deter and disrupt the projection of U.S. forces. This possibility is the result of another emerging characteristic of future conflict: "360 degree warfare."

In the past, war has usually been characterized by the existence of "fronts" and secure "rear areas," whether at the strategic, operational, or tactical level. Of course, airpower provided the means to attack the enemy's rear and long-range airpower and missiles threatened to extend the ability to attack the rear to the homeland, as illustrated in Figure 1-7. Nonetheless, actual attacks against the strategic rear of both sides were deterred by the likelihood of mutual destruction.

Figure 1-7. Challenges from All Directions

While guerrillas, insurgents, terrorists, and other armed groups have sought to wage a "war without fronts," the strategic emergence of true 360 degree warfare is a recent development. 9/11 indicated that the ability of the United States to deter attacks against its homeland is no longer assured. Iraq and Afghanistan illustrate that our adversaries have adopted this approach at the operational and tactical levels of war as well.

Here warfare is characterized by distributed, weakly connected battlefields; unavoidable urban battles; and unavoidable collateral damage exploited by adversary's strategic communication and highly vulnerable rear areas. On such battlefields, friends and enemies are commingled and there is a constant battle for the loyalty of the population.

Future Weapons, Future Battlefields

Self-Replicating Agents

Biological weapons have never before been used extensively and they pose a new kind of threat: the autonomous self-replicating agent. Along with cyber threats, biological weapons represent a new category of low-cost, stealthy threats that can be released remotely and spread indefinitely. Such biological weapons directly impact the U.S. health care system, which is already strained. The psychological impact is enormous as citizens become weapons. In addition, quarantine is a force multiplier for the adversary with potentially grave economic impact that can be greater than the threat itself. Whether or not the United States chooses to quarantine itself, other countries will not hesitate to quarantine us. The progression of biotechnology continually lowers the threshold for developing such weapons, and many deadly agents exist readily in nature.

Ultimately, weapons used in strategic ways could force the United States to change its foreign policy, so it is necessary to understand "what war we are in." No matter the outcome, as the Iraq deployment winds down, the enemy will have to shift to other U.S. targets and strive for an effect that dwarfs 9/11. Self-replicating agents, whether they are biological or cyber, could have considerable appeal.

Cyber Space

Adversaries are aware of America's dependence on the application of information technology to warfare. U.S. forces depend on ever-improving C4ISR, precision navigation, and targeting and communications, as depicted in Figure 1-8.

They are essential to the speed and accuracy of maneuver tactics. They are equally an important part of strategic decision-making, for which "situational awareness" is the mantra. Adversaries see U.S. success in using information technology as an Achilles' heel, and attacking these assets is especially attractive because it can be done "on the cheap."

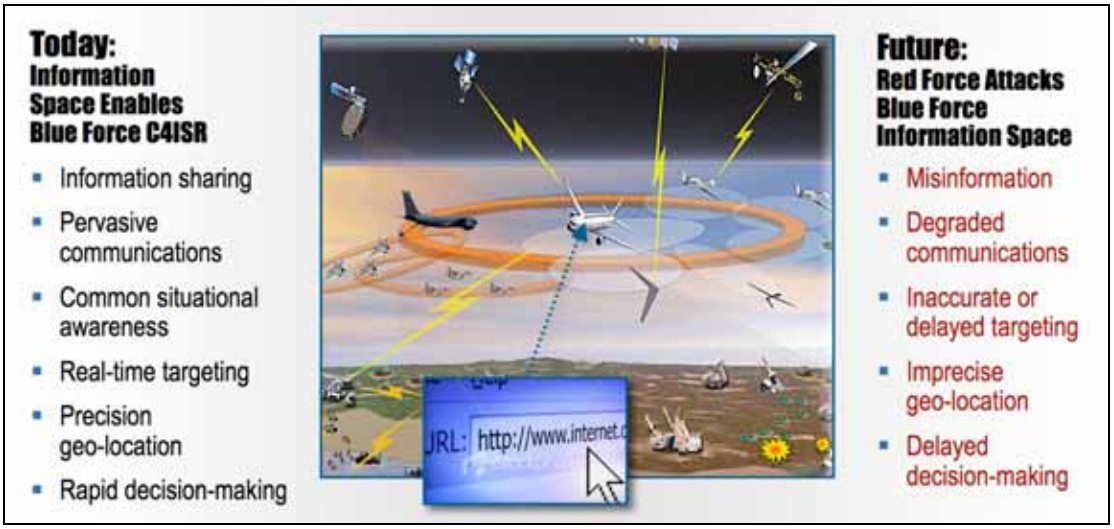


Figure 1-8. Information Space becomes a Battleground—Enabler Today, Target Tomorrow

The barriers to entry even for high-end cyber warfare capabilities are low—no fissile material needed, no expensive enrichment plants required. And, it is safer, too. No radiation hazards with which to contend, no strategic weapons that can be held at risk, and relatively little chance of attribution beyond a reasonable doubt.

The catalogue of concerns includes kinetic and/or directed energy anti-satellite (ASAT) attacks; ground system disruption; hackers, insiders and supply-chain operations; jammers and "dazzlers."

In a real sense, the United States is a victim of its own success, employing information technology, perhaps to the point of over-dependence, and cashing in untold savings through the use of COTS technology increasingly made by or within reach of potential adversaries. It would appear that we are so wary of having to give back some fraction of the savings, some portion of the efficiencies, that we may delude ourselves into thinking "it couldn't really happen." But, some argue, it is already happening, citing recent attacks on Estonian information infrastructure, the seemingly irresistible daily attacks on

DOD's information systems attached to the Internet, and Islamist radicals' attempts to target U.S. soldiers at Ft. Dix, *inter alia*.[35]

Space

Space is an interesting place. It is relatively hard to reach, and the further you go, the bigger it gets. It is hard to hide in space and it is hard to hide from space. Most of all, space is an as-yet untested battlefield.

Whether or not space is the final frontier, the recent Chinese direct-ascent anti-satellite demonstration should make it clear that it is the next battlespace. The successful test should have come as no surprise. The Defense Department's 2003 annual report to Congress on "The Military Power of the People's Republic of China" stated that Beijing "is believed to be conducting research and development on a direct-ascent ASAT system that could be fielded in the 2005-2010 timeframe."

Curiously—some would say, preposterously—the Chinese Foreign Ministry asserted that the test was not targeted against any country and does not pose a threat to any country. Still, the United States is highly dependent on fragile space architecture, with vulnerabilities known only too well to military planners, and this has not escaped the notice of others. Dependence on satellites for communications, intelligence, and ballistic missile defense may be seen as an inviting vulnerability of the United States.

Despite the obvious asymmetric threat invited by our overwhelming reliance upon space-based assets, China's ASAT test fundamentally contradicts its adamant opposition to American withdrawal from the ABM Treaty and the subsequent deployment of a ballistic missile defense shield. Both China and Russia have sought to limit American space capabilities by proposing an international ban on weapons in space in order to deter a new "space race" and prevent American hegemony in space. Surely disingenuous, China's Foreign Ministry replied to U.S. and Japanese concerns about its ASAT test by stating: "Since other countries care about this question and are opposed to weaponization of space and an arms race in space, then let us join hands to realize this goal."

---

35. The concerned reader is referred to the *Defense Science Board 2006 Summer Study on Information Management for Net-Centric Operations.*

However, an "arms control regime" prohibiting the "militarization" of space would present a nearly insurmountable verification challenge and would only serve to handicap the United States and others who would adhere to their treaty obligations. At least two potential adversaries, Russia and China, are known to have demonstrated ASAT capability. General Maples, Director of the Defense Intelligence Agency, testified before the Senate Intelligence Committee in January 2007 that "while Russia and China continue to be the primary states of concern regarding military space and counter-space programs … several countries continue to develop capabilities that have the potential to threaten U.S. space assets and some have already deployed systems with inherent anti-satellite capabilities … [including] kinetic or directed energy weapons capabilities."

There should be no doubt about the U.S. position in space. Just a year ago America's space policy was revised. An unclassified version, released, marks a significant paradigm shift in the traditional rhetorical ambiguity surrounding the weaponization of space. Among the new principles set forth by the amended space policy was the declaration that the "Freedom of action in space is as important to the United States as air power and sea power … and [America] rejects any limitations on the fundamental right of the United States to operate in and acquire data from space ... or the development of new legal regimes or other restrictions that seek to prohibit or limit U.S. access to or use of space." Moreover, the United States "will dissuade or deter others from either impeding those rights or developing capabilities intended to do so; take those actions necessary to protect its space capabilities; respond to interference; and deny, if necessary, adversaries the use of space capabilities hostile to U.S. national interests." The revised policy charges the Secretary of Defense with ensuring "force enhancement, space control, and force application missions."

Exploiting Media Proliferation

As previously pointed out, when "winning" involves capturing hearts and minds, victory will prove elusive if military force is the only advantage held by the United States. In a succession of studies, the Defense Science Board has argued for a more robust—well-resourced, well-led and well-executed—program of "strategic communication," *i.e.,* strategic influence. In this study, as well, strategic communication is an important facet.

Information technology today is revolutionizing world media every bit as consequentially as did Johannes Gutenberg's introduction of moveable, re-usable type to Europe in the mid-fifteenth century.[36] Printing soon became the principal means of mass communication. It put more knowledge in the hands of more people faster and more cheaply than ever before. As a result, reading and writing spread widely and rapidly. This is another example of technology lowering the barriers to entry, just as the Internet has done most recently for publishing. Even in the more traditional "broadcast" media, trail-blazers like CNN and Al Jazeera have changed the playing field.

These new media are no respecters of national boundaries and the pervasive technology, coupled with a Constitutional "right" to information, enable adversaries to reach the mind of the U.S. public as never before. At the same time, America faces more competition in reaching its target audiences abroad. Efforts at psychological operations and strategic influence are often deemed embarrassing and charges that the entertainment media are deliberate tools of "cultural imperialism" cause discomfort. The media, like cyberspace and outer-space, are tomorrow's battlefields, for which the nation must prepare.

Whom Does the Next Generation Technology Favor?

The United States perceives itself as the master of high technology and generally presumes that as technology has worked to its advantage in the past, so must it work in the future. Table 1-3, however, suggests that this may not always be the case. One reason technology has favored the United States has been its expense and the nation's willingness to invest. As technology becomes ever more affordable, barriers to entry for an opponent fall away. In some cases, what was exclusively a military technology moves into the commercial mainstream and is available to an adversary, "off the shelf." Moreover, there are certain technologies—WMD-related, principally—from which the United States refrains as a matter of policy, which in some cases is formalized in treaty obligations. Finally, many, if not most, of the military technological advances favor the offense rather than the defense. And, because America does not envision itself as the aggressor, it suffers by comparison except insofar as an offensive capability serves as a deterrent.

---

36. Although printing with moveable type reportedly existed in East Asia since at least the 700s.

Table 1-3. Who Does the Next Generation of Technology Favor?

Modality	Net Advantage		Comments
	Us	Them	
Biological		√	▪ They value life less ▪ US has no offense by policy ▪ US defenses are minimal
Cyber		√	▪ Low barriers to entry ▪ Defensive technology not keeping up with offensive ▪ US depends more ▪ Media for propaganda, command and control, and recruiting
Nuclear		√	▪ US posture frozen in time ▪ Adversaries modernizing with a vengeance ▪ Adversary willingness to cross nuclear threshold ▪ Technology proliferation
Chemical		√	▪ They value life less ▪ US has no offense by policy ▪ MOPP [military oriented protective posture] constrains operations
Radiological		√	▪ They value life less ▪ US has no offense by policy ▪ MOPP constrains operations
Robotics	√		▪ We value humans more
EMP		√	▪ US more dependent on vulnerable infrastructure
Directed Energy and Lasers		√	▪ Declining barriers to entry ▪ Commercial off-the-shelf availability of high-powered lasers ▪ US restrained by policy against blinding
Innovation Explosives		√	▪ They value life less ▪ They benefit from increased energy density ▪ New category of casualty with increased strategic consequences

Paradoxically, there is a brighter side to this situation: another of Murphy's laws states that each new, technologically enabled capability brings with it new vulnerabilities. Of course, this plagues the United States mightily, but as our nation anticipates when an adversary begins to rely on high technology, we should be quick to exploit the attendant vulnerabilities.

Potential "Game Changers"—Countering Critical U.S. Military Capabilities

Paying tribute to the U.S. superiority in conventional, high-tech warfare, potential adversaries seek to negate any advantages we might have and to use disruptive strategies to frustrate our ambitions. They seek either to counter our critical military capabilities or to circumvent them. Some military powers, with substantial technological capacity in their own right, may seek to acquire disruptive capabilities that directly counter critical U.S. military capabilities. Others—armed groups and less advanced militaries—would more likely focus on irregular warfare and information operations to disrupt our operations and remove support for our campaigns. And, of course, rising military powers may straddle both camps. In the series of accompanying figures (Tables 1-4 to 1-6), organized according to a particular U.S. military capability, we array the strategies and the technologies which enable them.

The ability to project force is our premier military capability and any adversary would be highly motivated to diminish that capability by raising the price of access. The associated technologies present a familiar shopping list, as Table 1-4 illustrates.

No adversary could fail to appreciate the degree to which the U.S. military depends on C4ISR, nor could they overlook the crucial enabler, U.S. space operations. This very dependence suggests vulnerability to a determined adversary. Some of the technologies to counter the U.S. advantage, like direct-ascent ASAT operations, present a high barrier to entry. Others, like denial and deception and attacks on information infrastructure, represent lower cost endeavors. Evidence suggests that aspiring peer nations will attempt to employ a gamut of counters (Table 1-5).

Table 1-4. Countering Critical U.S. Military Capabilities—Force Projection

Raise the Price of Access	Technology Drivers

▪ Increase risk to U.S. naval and air operations entering contested area
▪ Dissuade allies and partners who can provide basing and support to U.S. operations
▪ Speed up their operations, slow down ours, and present *fait accompli*
  ▪ Interrupt timely U.S. deployment
  ▪ Compel U.S. force to operate further from it's intended target
▪ Seek to destroy high-value (iconic) asset–*e.g.,* aircraft carrier–for both tactical and strategic benefit
	▪ Over-the-horizon (OTH) reconnaissance and targeting
	▪ Range and lethality of anti-ship and land-attack weapons
	▪ Emergent undersea threats
	  ▪ Autonomous mobile and deep-water mines
	  ▪ Long-endurance, quiet submarines
	▪ Range and seeker capabilities of air defense weapons
	  ▪ Energetic propellants
	  ▪ Lightweight materials
	  ▪ Autonomous seekers
	  ▪ Guidance, control and radar
	▪ Swarm tactics with associated technologies
	▪ Low observables–"stealth"

Table 1-5. Countering Critical U.S. Military Capabilities—Information and Space Operations

Bring Down the "Network"	Technology Drivers

▪ Degrade our information systems
▪ Disrupt our Command and Control
▪ Deny U.S. surveillance and reconnaissance
▪ Deceive U.S. intelligence
	▪ Counter-space advances
	  ▪ ASAT
	  ▪ Ground systems disruption
	▪ Threats to information networks
	  ▪ Distributed Denial of Service (DDS) and remote corruption
	  ▪ Insider and supply chain attacks
	  ▪ "Backhoes"
	▪ Electromagnetic pulse and directed radio-frequency energy
	▪ Laser "blinding" and/or damaging ISR sensors
	▪ Threats to related infrastructure
	  ▪ SCADA systems (*cf.* Idaho National Labs)

Disrupting U.S. precision strike capabilities does double duty for the opponent. It helps protect his military assets and it precipitates larger numbers of innocent casualties and collateral damage that work to his advantage in undermining our nation's willingness to persevere. The technologies and countermeasures are varied; again, some are high cost, others more affordable (Table 1-6). An aspiring peer could be expected to pursue the entire spectrum. This inevitably leads to the easy availability of more affordable counters on the international arms markets.

Table 1-6. Countering Critical U.S. Military Capabilities—Precision Surveillance and Strike

Increase the "CEP"	Technology Drivers

▪ Reduce U.S. standoff range, force "close-in" engagement
▪ Remove the risk to strategic retaliatory systems
▪ Disperse, intersperse, camouflage and conceal targets
▪ Confound U.S. guidance systems
	▪ Range and lethality of air defense systems
	▪ Multi-sensor and data fusion capabilities to detect and locate
	▪ Mobility of weapon systems
	▪ Deep-dig
	▪ Multi-spectral camouflage
	▪ Veridical decoys
	▪ Emerging electromagnetic challenges
	  ▪ GPS jamming
	  ▪ AESA [active electronically scanned array] radars for aircraft and sensor jamming
	  ▪ Directed energy weapons
	  ▪ Laser blinders

But, of Course, We Will Still Have Nukes …or Will We?

Some take comfort in thinking that the United States can always fall back on its nuclear weapons if required. The nation may be tempted to take ultimate refuge in the idea that, should U.S. conventional capabilities be seriously disrupted, or attacks on the homeland threatened, it can rely on its nuclear weaponry.

From World War II on, the United States (and the Soviets) turned out thousands and thousands of nuclear weapons, from small atomic demolitions to megaton warheads. None, however, have been used since 1945. What follows is a brief tour, since that time, with respect to nuclear weapons:

Yesterday, though nuclear weapons threatened Armageddon, leaders found ways to manage those risks, to stabilize the security environment and, indeed, to turn back a broader interest in nuclear weapons.

- **American Monopoly**. Massive retaliation, New Look emphasizes strategic bombers, land and undersea-based ballistic missiles; assumed aggressive tactical and operational use of nuclear weapons results in new organizations such as the Pentomic Division.

Over time, possessors came to see such weapons as useful only for purposes of deterrence and defense, and worthy of extreme caretaking. They rebuffed interest from non-state actors and from states seeking shortcuts and they undertook cooperative action to reduce common risks.

- **Strategic Parity**. Flexible Response and Mutual Assured Destruction (assured second strike); Non-Proliferation Treaty regime. Because of the escalatory ladder, interest in operational/tactical nuclear warfare declines.

Today, things are more fluid. Some covet nuclear weapons as a tool for inducing U.S. restraint—and, indeed, for attacking it outright, if reports from al Qaeda are to be believed. They may also see nuclear weapons as useful for attacking U.S. allies, friends, and interests in regions of their vital interest, and as essential for creating new security orders fitting their own images.

- **Unconsummated Revolution**. A search for nuclear substitutes at the operational/tactical level of war; precision-guided munitions with conventional warheads obviate the need for tactical nukes.

Tomorrow, if nuclear weapons are broadly accepted as quintessential tools of asymmetric conflict, their use could become conventionalized, threatening U.S. security and international stability. The future likely will have more nuclear capable actors than today and the question, of course, is: Will the future bring terrible nuclear calamities or new stability?

What *should* the United States do about the future? What *can* we do about the future? As the "world's only superpower" the United States has a preeminent interest in managing the moment in ways that focus on the new opportunities for stability. The U.S. Nuclear Posture Review in 2001 prescribed a rapid evolution in the U.S. strategic posture to remain relevant in a changing international environment. It called for a transformation of the U.S. nuclear deterrent that has not yet begun some seven years later.

Heretofore, the nation has dwelt almost exclusively on "red force" changes—that is, on changes that affect how the adversary might contest U.S. objectives—and changes largely driven by technical rather than political trends. This following brief section, however, about the evolving nuclear posture in the United States, is less about the technology than the policies that constrain that technology.

Some may think that the United States possesses, and shall continue to possess, so vast and capable a nuclear arsenal that it provides a hedge against nearly any defense planning assumptions gone wrong and will ensure America's unchallenged position as world leader. The astute reader may recognize the parallels between this supposition and the Russian view that they, too, hold the same preeminence despite their recent diminution. Which of these two views is more naïve than the other? Any comparison would have to take into account dimensions other than nuclear, of course, but it should also review what is being done to the respective nuclear arsenals. The Russians are rumored to be modernizing their inventory with a vengeance. The United States, by contrast, is frozen in time.

In the not too distant future, the United States may be one of several dozen nuclear weapons-capable states (as will be discussed further in Part 3 of this volume). According to the International Atomic Energy Agency there are presently 66 countries that have nuclear activities safeguarded by that agency. Many of these 66 have a "high latency" for weapons—that is, they could have nuclear weapons sooner rather than later, should they so choose. Meanwhile, the will of the Congress ordains that the United States may find itself with:

- **The oldest nuclear arsenal**. As the only one of the original five nuclear weapons states that has not set its post-Cold War agenda and begun the process of modernization, the United States will have nuclear weapons optimized for yesterday's environment, and with declining performance margins. The point to be made about the old arsenal is not that it is less optimized, but rather that it was exquisitely optimized for a world that has not existed for almost two decades. The current environment demands different characteristics for effective assurance, dissuasion, and/or deterrence (*e.g.,* applications in limited strike scenarios where lower yields with higher accuracies and end-to-end control). The Service Life Extension Program is not "transformation," and the Reliable Replacement Warhead merely perpetuates the 1991 force.

- **An arsenal of uncertain reliability** (presently high, but inevitably declining). The "stewardship" concept may be sound but it is hard to calibrate without testing, from which the nation is proscribed by law and treaty.
- **A smaller nuclear arsenal**. Presently still one of the largest, with 1,700–2,200 strategic weapons "on station."
- **An inadequate infrastructure**. The United States is not able to enlarge its arsenal in a timely fashion in response to a changed environment, nor is it able to change out the arsenal in any timescale of less than 25 years—even under the most optimistic scenarios. (This is true in large part because of a lack of a true production capability for pit production—a situation that has existed for 15 years.)

The question that must be asked—but one whose considered answer is beyond the present scope—is whether the state of the U.S. nuclear arsenal will do the job(s), to include: deterrence, extended deterrence and assurance, dissuasion, employment, and defeat of hard and deeply buried targets. That is, does the nation's nuclear posture lack the credibility needed for U.S. dissuasion objectives or will it encourage others to aspire to nuclear parity?

Chapter 6. Homeland Defense: What is Needed?

The United States can depend on its great military prowess to protect its primary interests in the international arena. It does not, nor can it ever, have the military power to protect or pursue all of its interests. Indeed, the increasing cost of military inventions—in terms of blood and treasure, international reputation, and internal schisms within the nation—all point to an era in which the other instruments of influence and power will be even more important than in the past. This is a consequence of the changed nature of war.

Another consequence of the changed nature of war is the notion, described in the previous chapters, of the homeland as battlefield, requiring a capability to respond to a homeland crisis while at the same time deploying forces to deal with an adversary abroad. While clear in its importance, the challenge is managing the varied players and responsibilities involved when the homeland is the theater and ensuring strong capabilities government-wide to address the challenge after next.

The Interagency and Homeland Defense

Defending forward—*i.e.*, projecting force—is the focus of the Department of Defense and its military departments. Roles and mission, responsibilities, and authorities are unambiguous once war is the chosen instrument. Command and control—unity of command—is the watchword. Because the mission is contingency, the "day job" involves organizing and equipping, with adequate time and resources allocated to planning, training, and exercising. With the National Guard and reserve structure, the bench is designed to be deep and the ability to surge is designed in. Obligation to duty is paramount.

Not so with defense of the homeland in all its manifestations (Figure 1-9). Multiple jurisdictions, departments, and agencies, government and non-government, are involved. Roles and missions overlap and responsibilities and authorities are sometimes maddeningly indistinct. A complex coordination schema

substitutes for unity of command.[37] There is little reserve for contingencies, and planning, training, and exercising for exigencies is modest. As a consequence, two troubling complications arise for DOD:

1. DOD's force projection mission depends on a secure, fully functional "rear."
2. DOD—vacillating between timidity and temerity—anticipates, then largely ignores, the fact that it might have to step in, in extremis.

Figure 1-9. Comparison of Organizational Strengths Across the Continuum from Civil to Military Preparedness

"Civilian Defense Corps"

Consideration should be given to conceptualizing an integrated corps of civil agencies and "civilians," organized, trained, and equipped using best practices of the uniformed military, as an alternative or adjunct to U.S. military operations at

37. *Cf. The National Incident Management System, FEMA 501/Draft August 2007,* "When an incident occurs within a single jurisdiction and there is no jurisdictional or functional agency overlap, a single IC [incident commander] should be designated with overall incident management responsibility by the appropriate jurisdictional authority. (In some cases where incident management crosses jurisdictional and/or functional agency boundaries, a single IC may be designated if agreed upon.) Jurisdictions should consider pre-designating ICs for pre-established IMTs [incident management teams] in their preparedness plans." [emphasis added].

home. Properly led and resourced, this "U.S. Civilian Defense Corps" would be prepared to take on all languishing homeland defense missions, freeing the military to concentrate on its force projection role and "securing the rear" to ensure that deployment, sustainment, and reach-back could operate without serious interruption.

Note that this is several steps beyond the National Incident Management System (NIMS).[38] In its most ambitious instantiation, the Civilian Defense Corps would include, *inter alia*, all first responders and would have adequate reserve forces on which to draw when surge was required. An obligation to duty would be required. Special care would be taken in the management of these reserves to ensure that reservists were not "double-counted" as part of military reserves. It is clear that major legislation would be required and thorny issues—such as states' rights—would have to be addressed. This is not a proposal to be taken lightly. This Corps is nothing short of a capability for national mobilization, but desperate times could call for desperate measures.

Bring "Jointness" to Civilian Agencies

Again, a step beyond NIMS as currently envisioned, the U.S. Civilian Defense Corps construct would emphasize more integration vice coordination across the operational elements of relevant federal departments and agencies. By example, it would encourage "jointness" in sub-federal organizations, as well as establish the utility of vertical integration of federal and sub-federal operational elements. Table 1-7 illustrates how disjoint things are now.

The impact of events like Katrina are multiplied several fold, not for lack of resources, but for lack of authority, initiative, and training to use them in a timely and coordinated manner. Certain assumptions also hinder domestic rescue operations:

- Current doctrine only requires Disaster Medical Assistance Teams to be self-sustaining for 72 hours.
- The National Disaster Medical System is designed for evacuation but not quarantine.
- Most participants in the NIMS are part-time employees with episodic training and other obligations.

---

38. *Cf.* Homeland Security Presidential Directive-5 (HSPD-5), Management of Domestic Incidents, 28 February 2003.

Table 1-7. Emergency Support Functions and Responsible Agencies

Agency	Emergency Support Functions														
	#1– Transportation	#2– Communications	#3 – Public Works and Engineering	#4 - Firefighting	#5 – Emergency Management	#6 – Mass Care, Housing, and Human Services	#7 – Resources Support	#8 – Public Health and Medical Services	#9 – Urban Search and Rescue	#10 – Oil and Hazardous Materials Response	#11 – Agriculture and Natural Resources	#12 - Energy	#13 – Public Safety and Security	#14 – Long-term Community Recovery and Mitigation	#15 – External Affairs
USDA			S		S	S		S		S	C/P	S		P	S
USDA/FS	S	S	S	C/P	S	S	S	S	S	S			S		
DOC	S	S	S	S	S		S		S	S	S	S	S	P/S	S
DOD	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
DOD/USACE			C/P	S	S	S		S	S	S	S	S	S	S	
ED					S										S
DOE	S		S		S		S	S		S	S	C/P	S	S	S
HHS			S		S	S		C/P	S	S	S			P/S	S
DHS	S	S	S		S	S	S	S	S	S	S	S	C/P/S	S	C
DHS/EPR/FEMA		S	P	S	C/P	C/P			C/P	S				C/P	P
DHS/IAIP/NCS		C/P										S			
DHS/USCG	S		S	S				S	S	P			S		
HUD					S	S								P	S
DOI	S	S	S	S	S	S				S	P	S	S	S	S
DOJ	S				S	S		S	S	S	S		C/P/S		S
DOL			S		S	S	S	S	S	S	S	S		S	S

Source: National Response Plan, 2004
Note: C = Emergency support function coordinator; P = primary agency; S = support agency

The creation of DHS was an important effort to bring together disconnected federal organizations under one roof. Events like Katrina have demonstrated, however, that tying them all together under an overarching bureaucratic envelope is not enough to ensure their timely, coordinated deployment. Instead, it has become clear that the nation needs a new, single, responsible organization with both political authority and boots on the ground to lead the charge during a mega-disaster. The key is to combine the best of the civilian and military world. The civilian side has expertise, authority, and responsibility; the military, however, has discipline, organization, and resources. A blend of the two combined with novel approaches to training creative intelligence and moral courage will create a new force that can not only prevent natural events from becoming economic disasters but also unnatural events from becoming strategic blows.

Crisis Deployment by Other Government Agencies

Within the seeds of this idea is the solution to another problem that vexes the DOD and confounds military deployments—the transition in "Phase IV" operations. Depending upon the engagement, at the end of the decisive combat phase there is often the need to move into stabilization and reconstruction activities. Increasingly, the U.S. military is consciously planning and training for this aspect of the mission but this phase requires integration with, and hand off to, other federal agencies. Even with the best of intentions, this has proved difficult because those other federal partners are not well organized, trained, and equipped to project and sustain their capabilities during the immediate post-combat phase. The nature of the U.S. Civilian Defense Corps that is envisioned here would be better suited to equal partnership with the DOD in this context.

Quite apart from Phase-IV operations, this Corps might also be available to "project" its capabilities abroad to shoulder its fair share of the humanitarian assistance mission now borne almost exclusively by the U.S. military. Curiously, this brings us full circle:

> The irony is that when a humanitarian crisis occurs abroad we send the military: a single, coherent organization with a clear command structure and highly trained full-time professionals that are able to sustain themselves in-country indefinitely. When a disaster occurs within the U.S., authority is divided between local, state, and federal entities, and resources and responsibilities are divided between a myriad of organizations.

An Alternative to Simply Defending Critical Infrastructure

In a simple sense there are two strategies for ensuring a functional infrastructure against the potential of an attack by a competent, motivated, adversary:

1. Spend scarce resources on the defense of the present infrastructure.
2. Invest resources in replicating, diversifying, and enlarging the infrastructure—making it highly redundant and with excess capacity—so that it has the resiliency to withstand attack.

Economically, the latter course makes more sense because it strengthens the nation substantially absent an attack, yet may provide the same measure of assured functionality in the event of an attack.

The threats and remedies surrounding Y2K provide a good example. Indeed, money was spent on remedial efforts, but considerable sums were spent on replacing vulnerable legacy systems with new systems, hardware, and software, which were flawless. It was the latter expenditure that provided substantial benefit to the nation at large.

How does this apply to the Department of Defense investment?

- Where the DOD depends on civilian infrastructure, it should consider investments in redundant capacity that is "uncorrelated" as an alternative or adjunct to investments in defense to assure survivable capacity.
- The DOD should rank high those developments that seek survivability by opening up new parts of the spectrum, geography, etc.

While this is a "big" idea, it is not an especially "new" idea. Today's interstate highway system, as some remember, had as its genesis the "National Defense Highway System." Since it was signed into law in 1956 by President Eisenhower,[39] DOD has continued to identify and update defense-important highway routes.

---

39. President Dwight D. Eisenhower understood the value of roads. In 1919, as a Lt. Colonel, he was aboard the U.S. Army's first transcontinental convoy, a 2-month journey from Washington, DC, to San Francisco, CA, to assess the readiness of military vehicles to make such a long trip. During World War II, Gen. Eisenhower saw the advantages Germany enjoyed because of the autobahn and noted the enhanced mobility of the Allies when they fought their way into Germany. http://www.tfhrc.gov/pubrds/06mar/07.htm

The National Defense Highway system was designed to move military equipment and personnel efficiently. Similarly, when the Department decided that its radio-frequency communications were too easy to intercept and/or jam, it moved to higher frequencies. This opened up a new spectrum that enabled wireless and handheld commercial devices, which most of us rely upon as much for business and personal communications as we do the interstate system for personal and business transportation needs.

Part II

Unconventional Weapons and Technology Proliferation

Chapter 7. The Technology of Unconventional Weapons

The technology equation, between the United States and potential adversaries, is, as the previous section described, a key element in evaluating U.S. capabilities to effectively and successfully wage war in the future. Access to technology will have a critical impact on the future battlefield. Few nations will attempt to fight the United States' vast conventional arsenal and will instead turn to unconventional weapons. As later sections of this report will discuss, adversaries will likely make use of these unconventional weapons using unconventional tactics, techniques, and procedures in hopes of gaining an asymmetric advantage against the United States.

Because of the importance of technology proliferation, this study placed significant effort on understanding adversary use of various technologies in developing weapons, the technical issues underlying such development, and how the United States might combat their use.[40] Eight destructive modalities were evaluated: nuclear, radiation dispersal devices (RDD), biological, cyber warfare, chemical, high explosives (HE), electromagnetic pulse (EMP), and directed energy (DE).

As shown in Figure 2-1, each modality was examined in a systematic way. The assessment initiated with a "Red" perspective—with experts for each technology considering how Red objectives could be best achieved using this technology and what advantages and disadvantages that would offer relative to other forms of attack. In essence, modality experts attempted to "sell" their capabilities to, or seek investment from, an adversary board of directors. In addition, they evaluated what would be required to provide the intended capabilities.

---

40. This analysis was conducted by the summer study's technology assessment panel. It members were selected for their collective depth of understanding of technology in the eight destructive modalities evaluated in this chapter and its accompanying appendices. The panel organized itself into teams according to the eight modalities, but functioned as an integrated group to address cross-modality attacks and to avoid the perils of stovepipe thinking.

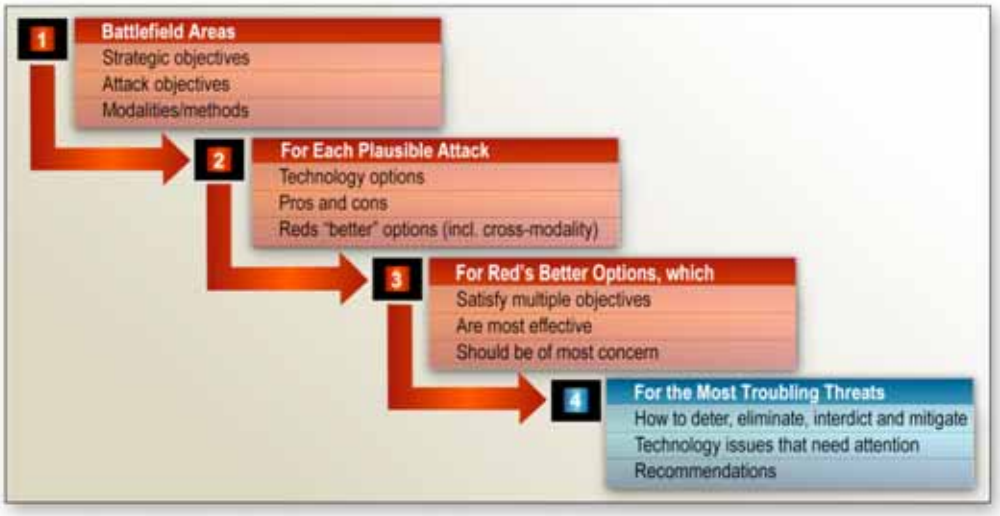


Figure 2-1. Technology Assessment Methodology

With these individual modality assessments as a foundation, the logic path outlined in Figure 2-1 was pursued—a path consistent with the "battlefield areas" within the scope of the study: asymmetric warfare, overseas asymmetric conflict with unconventional opponents, disruption of U.S. deployment and supply, and attacks on the U.S. civil infrastructure and population. The steps of the evaluation are as follows.

- **Step 1**. Define a representative set of Red strategic objectives. For each objective, derive a number of supporting tactical objectives. In each case, the goal was to responsibly cover the possible spectrum; no attempt was made to be all inclusive.
- **Step 2**. Determine options for accomplishing each tactical and strategic objective with the technology of a particular modality, as applicable. The selection of these options was based on expert judgment rather than quantitative analysis. With these single attack options defined, it was clear that multiple attacks (sequential, concurrent, or complementary) would multiply the effectiveness of a single attack.
- **Step 3**. Identify the "best" options for meeting Red's strategic objectives. All of the defined options served as the realm of "the possible," from which a Red "board of directors" (a group of modality experts) identified the best, taking into account cost, risk, ease of execution, availability of critical resources, effectiveness, and so on.

- **Step 4**. Identify topics of major concern for "Blue" in terms of damage to the military or the economy, as well as psychological impacts to the national fabric. In this step, the study team shifted to a Blue perspective to determine how the nation could best prepare for, prevent, mitigate, and recover from the attacks considered most disruptive.

The results of this analysis are described in the following two chapters, with chapter 8 addressing the Red objectives and options for attack, and chapter 9 recommendations for Blue. Greater detail is available in appendices corresponding to each of the modalities.[41] An objective of this assessment was not only to understand the realm of the possible in terms of adversary use of available technology, but also to provide a sense of priorities among the modalities—that could be used as a basis for decision-making and investment priorities.

Modalities

A variety of methods are available to terrorists to attack the United States or its interests. For example, Figure 2-2 illustrates the vast amounts of stored energy that might be accessible to an adversary, ranging from a nuclear device to the potential destruction of major dams, unleashing the enormous energy of their waters. Innovative uses of high explosives can sometimes rival chemical, biological, nuclear, and radiological weapons in destructive power.

Figure 2-2. Stored Energy in Two Different Modalities

41. An overview and background for each modality is provided in appendices in the classified volume of this report. Appendices address the following: basic science, delivery and damage/disruption mechanisms, difficulty/ease of developing and executing, range of the possible based on technology, range of the probable based solely on technology, red payoff (pros) and challenges (cons), other factors of importance, and recommendations for Blue actions to counter Red.

Figure 2-3 provides a top level view of the modalities evaluated in this study. The relative positioning of these eight forms of attack is based on judgment and depends a great deal on the objective of the attack, the nature of a Red scenario, and many other factors. The arrangement (from left to right) of the likelihood that an adversary would choose a particular modality is subjective because this depends on the adversary class that can range from small insurgent groups to nation states. The modalities, arrayed from bottom to top, are according to the effective disruption; this ranking depends on a variety of possible Red objectives. Nonetheless, this albeit oversimplified figure provides a useful perspective on the attractiveness to Red and the potential disruptiveness to the nation of each of the modalities—which in turn can be useful in prioritizing the Department's attention and investment decisions.

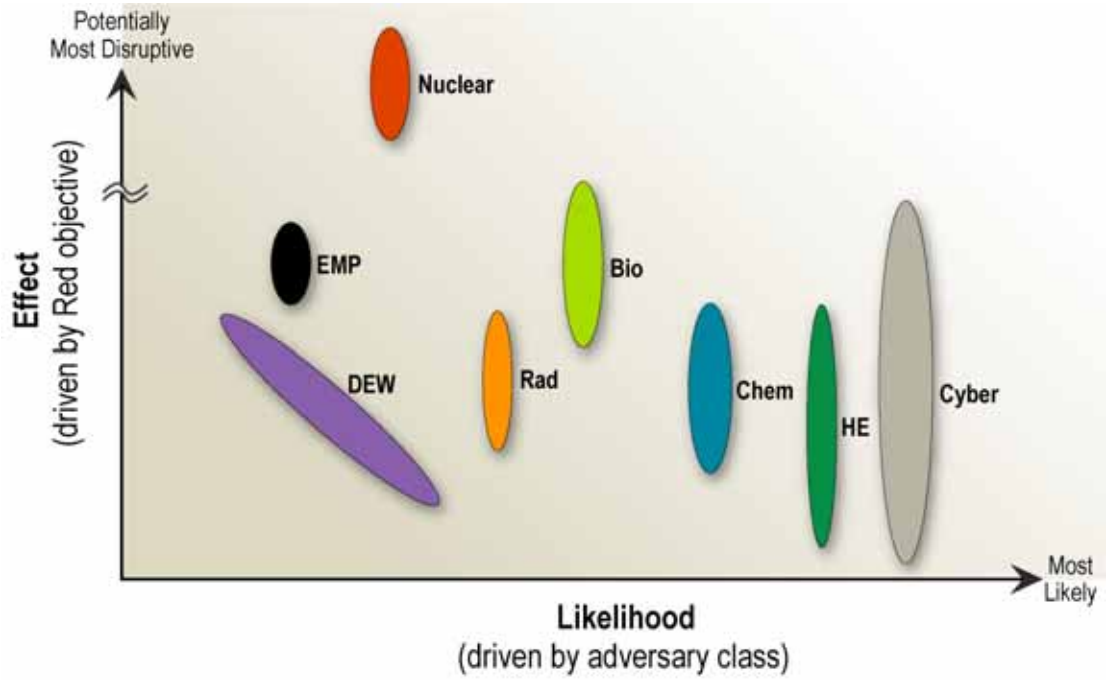


Figure 2-3. Subjective Assessment of Single Attack Modalities

As illustrated in Figure 2-2, an innovative use of high explosives (*e.g.,* the 9/11 attack) can provide much more disruption and damage than might initially be obvious—for that reason it is shown in Figure 2-3 as a large range in potential damage in the space plotted. Likewise, cyber warfare, because of the globalization of information technology, is not only likely but observed frequently today and, by its very nature, has tremendous potential for disruption and damage. In some scenarios and for some objectives, cyber attack may be the most effective of all.

The assessment presented here indicates that:

- Nuclear is in a class by itself (denoted by the broken scale) among single attacks.
- Cyber attacks should be particularly worrisome, both because of their potential damage and their growing accessibility.
- Biological attacks could be extremely effective.
- High explosives are today's weapon of choice for many adversaries and, used innovatively, can result in serious consequences, both tactical and strategic.

Chapter 8. Red Objectives and Attack Options

Given a basic understanding of each modality, the question of most concern is, "what would Red do if X were available?" There is no single answer to that question, but it is clear that Red's potential use of any of the modalities ties intimately with its objectives in carrying out an attack. Red's choice might be dramatically different if the goal is to wage a campaign of continual harassment tied to a long-term objective of politically exhausting the United States versus the creation of a single catastrophic "spectacle" event aimed at extracting maximum loss of life. Examining the linkages between objectives, modalities, and attacks is one way to shed light on this area.

Single Modality Attack Options

The study team performed an analysis for each modality to determine its potential in serving some representative strategic and tactical Red objectives. The methods for employing these modalities were also considered. These objectives were arrayed on three "battlefields," as follows: (1) overseas asymmetric conflict, (2) disruption of the deployment or supply chain supporting force projection, and (3) attacks on the civil population and infrastructure of the continental United States.

The overseas asymmetric conflict was further subdivided into those of a peer or near-peer, and those of an unconventional opponent—that is, one that is not territorial- or state-based. This same distinction was not made in the attacks on the U.S. homeland because in most cases, a serious physical attack on the U.S. homeland attributed to a peer or near-peer state would almost certainly lead to immediate conventional warfare. Non-attributable or less serious attacks were assumed to be perpetrated by an unconventional opponent. Situations in which state-backed attacks were accomplished by proxy through an unconventional player were treated as if the unconventional opponent perpetrated that attack unilaterally. An inherent challenge for Blue in this case would be to understand the motivator, supplier, or financier of such attacks.

For each of the battlefield or conflict areas, a number of high-level, representative strategic objectives were considered; they are summarized in Table 2-1. In turn, for each of the strategic objectives, tactical objectives were derived. The panel considered each tactical objective to determine where a

particular modality could contribute substantially to achieving that objective. Those cases in which a modality team found an effective use for their modality to achieve a given tactical objective were noted in the intersections of Tables 2-2 through 2-11, each representing one of the strategic objectives described in Table 2-1. Each of Tables 2-2 through 2-11 list the eight modalities across the top and the tactical objectives down the left side. The intersections describe how each particular modality would be employed to satisfy the tactical objective that was being served, along with the form of the attack that would best apply.

Many of the table entries are necessarily shortened and may appear cryptic in this format. The intent of this exercise is not to provide details, but rather to indicate the process that was followed. As such, the results are displayed in a very summary fashion prior to filtering to a set of particularly interesting cases. It is important to note that no such exploration as this can ever be complete, comprehensive, or definitive. Rather, the goal in the selection of strategic and tactical objectives and threat use was to identify reasonably representative sets that would enable further analysis.

Overseas Asymmetric Conflict with a Peer or Near Peer

In this situation, Blue finds itself drawn into an unconventional confrontation with a major state player, either because of ongoing activities by Red, or because of ongoing activities by Blue to which Red feels the need to respond. Identified in Table 2-1 are three potential strategic objectives underlying Red's hostile interaction with Blue:

1. A desire to increase Red's hegemony in some new region of the world, in which there is an existing Blue relationship that Red would seek to diminish
2. A perceived need by Red to preserve its strategic lines of communications in a region close to home or to prevent (or counter) what it views as Blue interference in a region it considers its own
3. A desire to erode Blue or Blue's allied political support for continuation of an ongoing war effort with a client state or another friendly player in some region of the world

Table 2-1. Red Strategic Objectives

Overseas Asymmetric Conflict		Attack on the Homeland	
Peer or Near-Peer	Unconventional Opponent	Deployment and Supply Disruption	Attacks on U.S. Civil Infrastructure and Population
Increase hegemony in new region [Table 2-2]	Erode political support for continuation of Blue war effort [Table 2-5]	Diminish ability to deploy troops and equipment [Table 2-8]	Severely damage U.S. economy, political function and lifestyle [Table 2-10]
Maintain Red SLOC and/or prevent Blue interference in regional activities [Table 2-3]	Create stalemate, limit escalation, prevent U.S. "victory" [Table 2-6]	Reduce ability of supply and support infrastructure to service war effort [Table 2-9]	Unite true believers, recruit new members from greater international community [Table 2-11]
Erode political support for continuation of Blue war effort [Table 2-4]	Take away U.S. strengths, willing to risk major escalation [Table 2-7]		

Table 2-2. Near-Peer Player Increasing Hegemony in New Region

Threat Mobility / Red Attack Objective	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Increase anti-American sentiment in region			Kill tens of civilians through HAZMAT spill, blame it on U.S. showing "evidence"				Periodic attacks in marketplaces and religious buildings, show evidence of U.S. involvement	Jam local TV and radio, spread "evidence" of U.S. involvement
Make dominant group more dependent on Red aid and support		Create limited outbreak of disease, support with medical aid	Create casualties using persistent chemicals, support with medical aid				Periodic attacks on infrastructure targets and repair efforts to make Blue look impotent	Disrupt financial or other networks, blame U.S., send in technicians to restore, prop up economy with competitor loans and investment

Note: SLOC - Strategic Lanes of Communication; RDD - radiological dispersion device; EMP - electromagnetic pulse; DE - directed energy weapons; HE - high explosives; HAZMAT - hazardous materials

These objectives are discussed in the three subsections that follow. A number of tactical objectives that were seen as representative in supporting these higher level strategic objectives are identified, and examples of how various threat modalities could be employed to service the tactical objectives are listed within the tables.

Increase Red Hegemony in New Region

Two attack objectives support the goal of increasing Red hegemony in a new region. The first, aimed at increasing anti-American sentiment in the region, uses any of three destructive modalities to create havoc without leaving any Red "fingerprints," and then lays blame on the Blue with false "evidence." In the second, Red creates harmful or disruptive situations in an area in which conflict is ongoing between two parties, after which Red comes to the aid of the party they see as dominant and which will eventually emerge victorious and in control of the area. In both situations, Red would employ strategic communication through the Internet and other media to support its objectives of enhancing its own image while diminishing Blue's. Table 2-2 outlines the interaction of the modalities with the two tactical objectives.

Near-Peer Maintaining Strategic Lines of Communication or Preventing Blue Interference Close to Red Home

Three Red attack objectives are identified in support of this strategic objective. All are aimed at reducing Blue's ability to fight in the region. The first, destroying or reducing Blue's ability to see and communicate, attempts to take away one of the fundamental strengths of Blue and one upon which many of Blue's most modern weaponry and war fighting tactics depend most. Both the second and the third attack objectives play upon the fact that Blue is attempting to maintain a fighting military presence far from home, both on the sea and in support bases on land. Reducing either capability will seriously impede Blue's ability to conduct sustained military operations in the region. The matrix of how modalities might serve these three attack objectives is provided in Table 2-3.

Near-Peer Eroding Political Support for Overseas War Effort in which Blue is Engaged

Four attack objectives are considered. The first two are both aimed at making it difficult for Blue to bring resources into the area and play to Blue's political desire to get in and out of overseas actions quickly. The two differ only in Red's willingness to escalate the level of action and hostility, the second one based on a willingness to take more provocative action. The third is more political in nature, focusing on creating civilian turmoil and resistance while the fourth relies on a form of brinksmanship, demonstrating Red's willingness to "play on the edge" of all-out war. Table 2-4 displays the interplay of modalities and the four listed tactical objectives.

Overseas Asymmetric Conflict with an Unconventional Opponent

The situation for Blue is similar to that described in the previous section, except here the opponent is an organization without a fixed geographic or state base. This type of opponent could take the form of a terrorist organization, such as al Qaeda, or an insurgency, such as the conflict in Iraq today. The assumption is that Blue is engaged with a group of this type overseas and that Red, with no realistic chance of militarily defeating Blue, is focusing on Blue's political staying power. Three strategic objectives are described:

1. Eroding the political support for Blue's continuation of the war effort
2. Preventing Blue from achieving a clear victory and bogging Blue down in a stalemate situation
3. An escalation of item 2 by going further with more provocative acts aimed at diminishing Blue's fighting ability

Erode Political Support for Continuation of Blue War Effort

The strategic objective is the same as it was for the near-peer, except that in this situation, Blue is directly involved militarily with Red. All six of Red's tactical objectives are aimed primarily at political objectives, although the first three are based on direct physical attack of the troops or their families. The tactical objective/threat modality matrix for the unconventional opponent is provided in Table 2-5.

Table 2-3. Near-Peer Maintaining SLOC or Preventing Blue Interference

Threat Mobility / Red Attack Objective	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Destroy U.S. ability to see and communicate					HANE, destroy LEO satellites	Jam communication satellites and GPS; blind UAVs	ASAT; shipboard and ground LRSAM buildup; destroy undersea cable	Computer network attacks
Reduce local U.S. surface combat (ships) capability	Tactical nuke attack of CBG				HANE, destroy LEO satellites		Shipboard and ground LRASCM buildup; Complex mines	Computer network attacks
Attack regional military support bases	Ballistic missile delivered attack on Guam, Japan, etc.		Deliver persistent agent attack on Guam, Japan, etc.				Ballistic missile delivered attack on Guam, Japan, etc.	

Table 2-4. Near-Peer Erode Political Support for Continuation of Blue War Effort

Threat Mobility / Red Attack Objective	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Hamper/deny entry into area			Disperse persistent agent over critical U.S. entry SPODs and APODs	Disperse over critical U.S. entry SPODs and APODs		Jam comms and ISR assets	Sea mines; crater airfields; ASCMs	Computer network attacks to disrupt C4ISR
Hamper/deny entry into area, Phase II – major escalation			Disperse persistent agent over civilian targets		High altitude blast to destroy LEO satellites		ASAT (kinetic attack)	
Create civilian turmoil and resistance to U.S. presence in regional U.S.-friendly nation	Threaten use if escalation becomes out of control	"Demo" attacks in selected areas (sick but not fatal)	"Demo" attacks in selected military areas (painful but not fatal)				"Protest" IED and suicide bomb attacks in civilian areas	
Demonstrate willingness to escalate to the brink of all-out war	Threaten use if escalation becomes out of control		Direct attack on deployed troops			Jam comms and ISR assets	Full sea blockade, selective bombing	Military network attacks, some modest CONUS infrastructure attacks

Note: RDD - radiological dispersion device; EMP - electromagnetic pulse; DE - directed energy weapons; HE - high explosives; HANE - high altitude nuclear explosion; LEO - low earth orbit; GPS - global positioning system; UAV - unattended aerial vehicle; ASAT - anti-satellite weapon; LRSAM - long range surface-to-air missile; CBG - carrier battle group; LRASCM - long-range anti-sub/ship cruise missile; SPOD - sea port of debarkation; APOD - air port of debarkation; ISR - intelligence, surveillance, and reconnaissance; ASCM - anti-sub/ship cruise missile; C4ISR - command, control, communications, computer, intelligence, surveillance, and reconnaissance; LEO - low earth orbit; ASAT - anti-satellite weapon; IED - improvised explosive device; CONUS - continental United States

Table 2-5. Unconventional Opponent Erode Political Support for Continuation of Blue War Effort

Red Attack Objective \ Threat Mobility	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Kill 100s of deployed troops in protected base		Contaminate food and water	Disperse upwind				Truck bombs or suicide bombers	
Seriously impede effectiveness of combat forces		Visibly debilitate troops				Disrupt or jam comms	IEDs and truck bombs	Attack computer networks
Seriously demoralize combat forces or their families		Visibly debilitate troops		Area denial in operational base			IEDs, truck bombs, mines goad U.S. into tactical response with major negative strategic consequences	
Create civilian turmoil and resistance		Dispersal in market places, mosques	Periodic attacks in civilian areas				Suicide bombers in civilian areas	
Get U.S. press to write negative accounts of U.S. involvement			Periodic attacks including civilians				IEDs, truck bombs, mines & suicide bombers	
Raise specter of mass casualties	Threaten use in region or U.S.	Threaten use in region or U.S.						

Note: RDD - radiological dispersion device; EMP - electromagnetic pulse; DE - directed energy weapons; HE - high explosives; IED - improvised explosive device

Create a Stalemate Situation and Prevent Blue Victory while Limiting Escalation

Here, Red is attempting to bog Blue down in an unwinnable conflict in the hope that a continued effort with seemingly little gain will strain Blue's political staying power to the breaking point. Red understands that if the conflict escalates sufficiently, Blue can bring in sufficient resources to militarily defeat Red. Thus, believing that time is on his side, Red wants to avoid acts that provide Blue political cover for major escalation.

The first six attack objectives are focused on Blue directly, while the seventh threatens Blue's coalition support with the use of WMD or actually carries out lesser attacks on allied infrastructure. Table 2-6 provides the interaction of all seven tactical objectives and the potential use of the eight threat modalities.

Create a Stalemate Situation and Prevent Blue Victory—Willing to Risk Escalation

The situation and objective is identical to the previous one except for a difference in Red's calculus about the impact of potential escalation. Here, Red believes that victory for Blue is impossible, even with a significant degree of escalation. Thus, Red feels less constrained in terms of the level of attack he is willing to mount. Table 2-7 contains by reference all of the objectives and attack elements of Table 2-8 and adds three new objectives.

Attacks on the Homeland to Disrupt Blue Deployment and Supply

In this battlefield situation, Red is attempting to hamper Blue's ability in the homeland to provide logistics, materiel, and troop support for an ongoing conflict overseas. Because, in the view of this study, physical attacks on U.S. soil by a major state adversary would almost certainly escalate to full-scale warfare, this battlefield is primarily concerned with unconventional opponents. Exceptions, for example, where the stated use of a modality by a near-peer is not necessarily likely to lead to full-scale war, are noted in the tables.

Two strategic objectives are identified for Red: to diminish Blue's ability to deploy troops and equipment from the continental United States, and to diminish the ability of Blue's supply and support infrastructure to service the war effort

Table 2-6. Unconventional Opponent Creating Stalemate Situation—Unwilling to Risk Escalation

Threat Mobility / Red Attack Objective	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Maintain high personnel attrition rate		Infect food and beverage					IEDs, truck bombs, suicide bombers	
Seriously impede effectiveness of individual combat forces		Repeated use in varying ways		Corrupt APODs and SPODs	Disable C4ISR	Blinding of ISR, jam GPS	Above plus mortar and shoulder fired SAMs	Corrupt ground networks and C4ISR
Disrupt SLOC				Corrupt SPODs	Disable navigation		Sea mines, small boat swarms, ASCMs against capital ships	
Isolate combat forces from integrated command structure					Disable C4ISR	Destroy GPS		Corrupt ground networks and C4ISR
Inhibit local civilian work force from support operations		Infect bases of operations	Expose bases of operations	Corrupt APODs and SPODs			IEDs, truck bombs, suicide bombers and mortar attacks	
Deny U.S. Precision					Take out Comm. Sensor, GPS receivers	Blind ISR, jam radars and comm		Take down or corrupt computer networks
Hold allies hostage to continued U.S. support	Threaten use	Threaten use	Threaten use				Blow up SWET or transport facility	

Note: RDD - radiological dispersion device; EMP - electromagnetic pulse; DE - directed energy weapons; HE - high explosives; IED - improvised explosive device; APOD - air port of debarkation; SPOD - sea port of deparkation; C4ISR - command, control, communications, computer, intelligence, surveillance, and reconnaissance; ISR - intelligence, surveillance, and reconnaissance; GPS - global positioning system; SAM - surface to air missile; SLOC - strategic lanes of communication; ASCM - anti-sub/ship cruise missile; SWET - sewers, water, electricity and trash

Table 2-7. Unconventional Opponent Creating Stalemate Situation—Willing to Risk Escalation

Threat Mobility / Red Attack Objective	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Everything in table 5 plus the following:								
Disrupt SLOC			Attack ports, panic civilian workforce					
Disrupt staging of air attack	Attack carrier battle group and local air bases		Attack local airbases	Corrupt local and foreign air bases		Jam radars and navigation		Disrupt local air traffic control
Signal national resolve, fracture allied participation, eliminate local civilian support	Low yield on isolated military target or in demo area	Attack allied population center	Attack allied population center	Attack allied industrial or economic center			Increased civilian attacks	Corrupt allied financial infrastructure

Table 2-8. Diminish Blue Ability to Deploy Troops and Equipment

Threat Mobility / Red Attack Objective	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Disrupt, disable transportation system in CONUS						Jam GPS receivers in critical areas	Attack transportation infrastructure	Corrupt air traffic control, communications, personnel and logistics tracking
Attack ports and airfields of embarkation		Bio attack of airport hubs, panic civilian workforce	Chem attack, disrupt civilian workforce	Shut down critical APOE or SPOE			Attack transportation infrastructure	Corrupt national and local air traffic control networks
Attack garrison bases, nearby military families		Attack bases and host cities	Attack bases and host cities	Attack bases			Conventional HE attacks on base support and host cities	Attack computer network

Note: RDD - radiological dispersion device; EMP - electromagnetic pulse; DE - directed energy weapons; HE - high explosives; SLOC - strategic lanes of communication; GPS - global positioning system; AROE - air port of embarkation; SPOE – sea port of embarkation; CONUS - continental United States

Diminish Blue's ability to deploy troops and equipment

Three attack objectives are attributed to Red. Two of them are focused on the physical ability of Blue to move people and equipment around the United States and to air or sea lift them out of the country.

The third is aimed at creating chaos within the military support bases either directly or by attacks on military dependents and other civilians living in nearby host cities. The attack objective and modality matrix for this strategic objective is provided as Table 2-8. Only the counter network operations are considered appropriate to a near-peer, state-based opponent.

Reduce Ability of Blue Homeland Supply and Support Infrastructure to Service War Effort

Here, Red is attempting to defeat Blue's military support infrastructure. Two of the supporting attack tactics are identical to the case above, in which the movement of people and material is the target, since the attacks here focus on the transportation infrastructure. Two other attack objectives, however, are different and focus on the defense industry, both conventional and nuclear, and the civilian work force upon which much of the military support infrastructure is dependent. The matrix is provided in Table 2-9. The near-peer would be the only adversary with the capacity to attack GPS satellites with directed energy (in this case high power microwave) and might also engage in counter network operations against Blue. With the exception of the directed energy attack, the unconventional adversary might engage in all of the attack objectives.

Strategic Attacks on U.S. Civilians and Infrastructure

In this last battlefield situation, Red is directly attacking Blue's homeland in an attempt to accomplish either (or both) of two strategic objectives:

- Inflict severe damage on the U.S. economy, political function, and/or civilian lifestyle
- Further unite true believers in Red's ideology and recruit new members from the international community by demonstrating Red's ability to "destroy" the infidel

Both of these objectives strike at the heart of Blue society. If the attacks that service these objectives are perpetrated by a near-peer, state-based entity, it is highly likely that all-out war would quickly result.

Thus, with the sole exception of influence operations, short of an ongoing full-scale war, these attacks lay in the province of an unconventional adversary.

Severely Damage the U.S. Economy, Political Function, and Lifestyle

In Table 2-10, the matrix for this strategic objective, four of the five attack objectives are ends in themselves, all designed to create havoc across the full spectrum of Blue society—very large loss of life, serious economic loss, mass panic, iconic destruction. The fifth attack objective is an enhancer for one or more of the others—to create a situation someplace in the city that drains off public safety and medical first responders to an area far from where the main attack will subsequently occur.

Unite True Believers, Recruit New Members from International Community

This is the last of the ten strategic objectives considered in this assessment. Like many of the others, it represents a means to an end—creating economic, social, or political havoc in Blue's homeland to demonstrate the strength and commitment of Red, invoke the will and support of a supreme being to Red's cause, and, in so doing, further unite the faithful and attract new like-minded members from elsewhere in the world. The matrix for this element of Red strategy is presented in Table 2-11. All of the entries are focused largely on an unconventional opponent.

One of the issues associated with this Red strategy, as well as some others, was whether or not there is a damage threshold that Red does not want to exceed. The posited argument behind this self-deterrence question is that an attack that exceeds some very high level of loss of "innocent" life loses the sympathies of even the most devoted followers and becomes counter-productive. There is, of course, no clear or even single answer to this question, but it is often raised as one of the possible answers to "why hasn't this happened yet?" If there is even a shred of merit in this argument, it should be explored and understood better so that perhaps it could form an element of Blue strategy in countering some of these threats, particularly the more devastating ones.

Table 2-9. Reduce Ability of Supply and Support Infrastructure to Service War Effort

Threat Mobility / Red Attack Objective	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Disrupt, disable transportation system in CONUS						Attack GPS satellite (near peer only)	Attack transportation infrastructure	Corrupt air traffic control, communications, personnel and equipment tracking
Attack ports and airfields of embarkation		Attacks on airport hubs	Attack that affects civilian workforce	Shut down critical APOE or SPOE			Attack transportation infrastructure	Corrupt national and local air traffic control networks
Attack critical defense industry and nuclear plants			Contaminate one or two critical sole source facilities	Contaminate one or two critical sole source facilities			Attack defense industry production plants	
Debilitating attack on critical work force, dependents		Attacks in key urban living areas	Attacks in key living areas				Repeated attacks in selected areas of U.S.	

Note: CONUS - continental United States; GPS - global positioning system; AROE - air port of embarkation; SPOE – sea port of embarkation

Table 2-10. Severely Damage U.S. Economy, Political Function, Lifestyle

Red Attack Objective \ Threat Mobility	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Kill lots of people, terrorize the U.S. population and create panic	Weapon in or near city	Release in crowds in multiple cities	Toxic chemical storage facility attack				Multiple truck or suicide bombs in urban areas, MANPAD, LNG FAE	
Disrupt/take down financial systems, institutions or major contributors to economy		Agro or feedlot attack		Wall Street or Mercantile Exchange or Federal Reserve			Multiple refineries, institutions	Corrupt, disable various financial systems
Destroy Iconic targets or render useless		Senate Office Building attack		Wall Street or Mercantile Exchange or Federal Reserve			Truck or general aviation bomb	Take down one or two financial systems
Make normal activities appear to be unsafe or very risky (some require repetition)		Infect crowds in theaters or airplanes, announce afterwards	Release in sports stadiums or in public transport system	Downtown area of any major city		Attack aircraft in flight	Public school attacks; market-place attacks	Corrupt, disable banking, healthcare, transportation or public safety systems
Diversionary attacks (to enable primary attack)			Chemical attack on other side of town				Truck or suicide bomb	

Note: MANPAD – man-portable air defense; LNG – liquefied natural gas; FAE – fuel-air explosives

Table 2-11. Unite True Believers, Recruit New Members from Greater International Community

Threat Mobility / Red Attack Objective	Nuclear	Biological	Chemical	RDD	EMP	DE	HE	Cyber
Kill lots of Americans in their homeland (some not-to-exceed upper level?)	Weapon in or near city	Release in crowds in multiple cities	Release in multiple cities – delivered agent or available HAZMAT				Multiple truck or suicide bombs in urban areas, MANPAD	
Disrupt/take down financial systems, institutions or major contributors to economy		Agro or feedlot attack	Introduce into a building HVAC in Wall St. or Chicago Merc.	Wall Street or Mercantile Exchange or Federal Reserve			Sequence of attacks in urban business areas	Corrupt, disable various financial systems
Destroy Iconic targets or create symbolic acts	Offsite attack		In symbolic place, e.g. Las Vegas, Disneyland	Wall Street or Mercantile Exchange or Federal Reserve			Truck or general aviation bomb, one of many choices	Take down one or two financial systems
Shut down nuclear complex, create havoc, demonstrate US weakness							Attack Hanford, WA	Corrupt or disable safety/control system of nuclear power plant
Perpetrate act harmful or offensive to followers and attribute to US							Snipe from inside Mosque, let US react, and blow up mosque	

Note: HAZMAT – hazardous materials; MANPAD – man-portable air defense

Multiple Modalities and Attack Options

The previous section dealt primarily with attacks built on the use of single strikes employing single modalities. This is of course an oversimplification of Red's options. If beneficial to Red's objectives, an adversary could combine modalities in either single or repeated attacks. State adversaries, or very powerful non-state adversaries that have not yet emerged, have the capability to conduct orchestrated campaigns. As a result, it may be useful for the United States to consider potential attacks from such adversaries as orchestrated campaigns and not as singular events—horrendous though a singular event may be.

One way of looking at such options is exemplified in the 2x2 matrix in Table 2-12. In this section, the attributes and downsides of each of the four quadrants of the table are briefly examined.

Table 2-12. Multiple Modality and Attack Taxonomy

		Same Modality	Different Modality
Multiplicity	Concurrent	▪ Heighten impact by creating spectacle ▪ Ex: simultaneous chemical attacks on three sports arenas and two train terminals	▪ Create synergies to increase overall effect ▪ Ex: hazmat attack, IEDs to kill first responders, and cyber attack to destroy communications and coordination
	Sequential	▪ Grow panic over time ▪ Destroy faith in government's ability to provide basic services ▪ Ex: High-explosive attacks every week at random times for two sequential months	▪ Increased impact and dread over "Sequential/Same" ▪ Ex: bio contamination of milk supply week 1, high-explosive attack on school week 2, chem in hospital HVAC week 3, and so on

Multiple Concurrent Attacks using the Same Modality

The events of 9/11 were an attack of this type. Four separate targets were attacked, three of which were carried out successfully. The purpose of such an attack structure is to raise the "spectacle" value of the event, as well as to increase the damage inflicted. The obvious downside is that such a contemporaneous multiplicity of attacks requires much greater planning, coordination, and preparation than a single attack of the same type. Because more perpetrators will be involved and because the required number of personal and electronic communications between the participants is higher, the chances of

a "leak" or simply getting caught by accident are much higher and therefore present an increased opportunity for Blue intelligence assets and capabilities. Nevertheless, al Qaeda, in particular, seems to be enamored with this kind of attack structure. Some of the vulnerabilities can be mitigated by Red if these are independent attacks intended to be executed at a pre-determined time or signal.

Repeated Sequential Attacks using the Same Modality

There is significant evidence that repetition of even relatively unsophisticated attacks can be quite effective in achieving Red objectives. There are recent examples that make this point convincingly:

- IED campaign in Iraq
- Washington D.C. sniper in October 2003
- anthrax letters in fall 2001

The current experience in Iraq indicates that roadside IEDs, vehicle-borne IEDs and/or suicide bombers will likely be the overseas asymmetric weapons of choice for insurgents, terrorists, and possibly third world states when confronting the overwhelming superiority of the U.S. military. Despite billions of dollars and several years of focused effort, Blue has made only very modest headway in eliminating this low-technology threat, owing in part to the high degree of flexibility and adaptability this weapon affords. Successes in preventing attacks have been continually offset by an increase in the number of attacks attempted and a shift to devices that extract greater casualties per successful detonation. The result is that the loss of life, both American and Iraqi, has remained relatively constant over an extended period.

Ultimately, IEDs will not stop the U.S. military from achieving significant combat objectives. Despite the tragedy they represent to the troops who fall victim to them, they inflict relatively little damage on the scale of major force-on-force engagements. However, the steady loss of life IEDs inflict has proven to be maddeningly effective for achieving the Red objectives of creating a stalemate situation and eroding political support for continuation of the U.S. presence in stability and support operations. The key impact of the IED threat accrues from frequent repetition, rather than the severity of any single event, and the ease with which enemy tactics, techniques, and procedures can adapt to stay ahead of the U.S. response. It is certainly reasonable to assume that these kinds of attacks will continue to be the method of choice for future situations that involve willing

emplacement personnel, a large supply of adaptable munitions, and political rather than purely military aims.

Beyond this current-day situation, Blue must consider how more advanced versions of improvised conventional munitions might be employed in the next 10 to 20 years as more advanced technology becomes available in the global marketplace. These future versions could consist of helicopter "mines," combinations of high explosive and chemical or biological agents, and so on. Given the demonstrated ability of unconventional adversaries to adapt very rapidly to counters to their weaponry, Blue needs to do a better job of getting ahead of the power curve, figuring out Red's "move after next," and countering it before it happens.

In the United States, both the Washington D.C. sniper attacks and the anthrax letter incidents indicate the impact that simple attacks with relatively low damage can have when repeated regularly. These attacks were effective because they targeted ordinary citizens in a random pattern. As a result, nearly every individual in the target area felt some degree of risk. The impact of a more widespread attack could be devastating, for example, if a terrorist organization announced a plan to kill a number of Americans every week as they carried out their normal daily activities. Two or three sequential weeks of adversary success would undoubtedly result in a change in current urban life and a resulting catastrophic political and economic impact.

Repeated attacks using high explosives, biological agents, or chemical agents could have a significant immediate impact on the Blue psyche and lifestyle. Extensive press coverage would be expected, and would amplify the effect. If Red claimed responsibility and were able to continue the attacks, the competence of Blue's government to protect its population, one of the most fundamental roles of government, would come into question with severe political fallout. Sequential attacks could also be effective in satisfying the objectives of raising the stature of the Red organization at home and helping it to recruit new members.

Overall, the long-term effects of such attacks are less obvious. Blue resolve may very well increase and the populace may unite around a cause to defeat the aggressive enemy, provided that he can be identified and targeted. Certainly the Battle of Britain in World War II was such an example, and in the end proved counter-productive to the enemy. This type of attack also shares the downside of requiring more planning, preparation, and coordination, and therefore increased exposure.

Concurrent Employment using Different Modalities

In cases of concurrent employment using different modalities, the Red objective is not necessarily for spectacle or mass hysteria purposes, although they may result, but rather to increase effectiveness of a single attack. Innovative uses of multiple modalities could have a synergistic effect, the most obvious ones being the combined employment of a physically destructive modality (e.g., high explosive or chemical) with cyber warfare attacks on any one of the supporting networks, including public safety communications, power grids, water supplies, hospitals, and the like. The advantage to Red is not only the added effectiveness such combinations can provide, but also the fact that skillfully perpetrated cyber operations may be difficult to detect and even more difficult to attribute. Thus, in this case, the added modality does not provide much of an added degree of exposure.

Another complementary modality is the use of public networks, most notably the Internet and the press, for Red influence operations. "Spreading the word" of further Red intentions, particularly after the successful perpetration of a damaging act, could provide effective leverage on the damage that was actually accomplished and the impact it provided. This too is a simple and cheap accompaniment to a physical act; can be carried out from any place in the world; and is unlikely, if properly implemented, to lead to increased exposure.

A third and more difficult type of concurrent combined modality attack involves the use of multiple destructive modalities. A good example is contained in some of the Department of Homeland Security planning scenarios and one that was used by the Defense Science Board in the 2005 summer study on *Reducing Vulnerability to Weapons of Mass Destruction.* In these types of scenarios, one physically destructive modality is employed as the primary mechanism, while a secondary modality, with far less destructive capability but much more easily employed, is used to hamper public safety and medical response. An example of such a multi-modality structure in the 2005 study was an attack on a large, high-pressure chlorine storage facility. The main attack was accompanied by the employment of a number of IEDs, which were remotely detonated as public safety personnel arrived to seal the immediate area and coordinate evacuation. The public safety personnel were unable to properly coordinate activities for a critical period of time and the resulting casualties were significantly heightened.

Perhaps the most serious example of concurrent employment with different modalities, is a peer or near-peer attack against C4ISR while Blue forces are engaged in an overseas conflict. A combination attack with the following

components, for example, could seriously degrade or destroy many or most C4ISR: (1) a concentrated cyber attack (denial of service, corruption of Blue data, destruction of hardware via control systems, computer network exploitation, malicious code and tampered hardware); (2) possibly nuclear EMP, jamming, and blinding Blue communications and sensor assets; (3) anti-satellite systems; and (4) selected high explosive attacks on communication nodes or command and exploitation facilities. If timed to the advantage of the opposing forces, this type of combined attack could lead to serious losses in that conflict.

Sequential Employment using Different Modalities

In this most complex attack structure, sequential employment using different modalities, the perpetrator is not building upon the natural synergies between different modalities, but is demonstrating his ability to do anything he chooses whenever he chooses. This kind of attack also builds upon the natural inclination of public safety and military organizations to try to do a better job in combating the last issue with which they dealt. This trend is evident in the Transportation Security Agency today, six years after 9/11. Thus, a series of attacks of different modalities, all aimed at children in natural settings, would likely have an even greater impact than sequential high explosive attacks. The resultant change in societal behavior, including, in particular, the impact on civil liberties and freedom of activity and life style, would be significantly greater as well.

The downside to Red is, once more, the greater degree of planning required and the increased number of personnel involved. Not only would the number of perpetrators be greater, but the fact that more than one technical specialty would be involved could lead to a greater potential for discovery. Unfortunately, human activity pattern recognition is not a well-developed competence. Further, if Red is concerned about the potential for discovery, this weakness can be ameliorated by inserting a number of "sleeper" cells, each with a capability in one modality and completely independent of other cells. The attack could be initiated using a very loosely coordinated schedule, triggered by some global signal or event.

Combining Modality Technology and Delivery Means

This last subject deals with the combination of effect and delivery, particularly, but not necessarily limited to, a less than near-peer state actor engaged in conflict with the United States. An opposing entity would most likely want to directly attack U.S. forces in theater with a combination of technologies which have a

minimal cost but maximum effectiveness. Some potential possibilities of combined delivery technologies against Air Force, Army, and Navy forces are described here:

- Attacks on naval forces at sea are possible by theater ballistic missiles using unique guidance methods. There is evidence that at least one country has deployed very large numbers of theater ballistic missiles including a subset with guidance that can terminally hone on ships.
- Torpedo attacks are also possible by various conventional and unconventional platforms using advanced acoustic guidance. In World War II, intensive submarine attacks of surface ships occurred in both the Atlantic (by German submarines) and in the Pacific (by U.S. submarines). Since then, much more capable torpedoes have been developed, as well as both nuclear submarines and submarines with air-independent propulsion.
- Jamming naval, commercial, and military satellite communication links may be combined with the disruption of Navy networks by software attacks. Much of the long-range communications for Navy ships and U.S. ground forces is carried through military and commercial satellites that are not protected from jamming. In addition, the recent attacks on the Estonian Internet system indicate the similar U.S. Internet system used by U.S. military forces is extremely vulnerable to such attacks.
- The Army depends on shipping to transport its heavy equipment to overseas theaters. World War II experience indicates the vulnerability of such transport unless a massive counter-submarine effort is employed to protect shipping vessels.
- Conventional warfare using ballistic missiles has been a factor since the V2 rocket was used in World War II. The recent massive use of unguided short-range missiles against Israel by Hezbollah from bases in Lebanon was a new threat in conventional warfare. When such missiles are equipped with GPS-based guidance and combined with easily-available imagery on the Internet and spotters on the ground, such attacks could cripple conventional land forces engaged in conventional warfare.
- Experience in Iraq over the past four years indicates that the use of IEDs to mine transport and resupply routes is extremely effective. Increasingly clever detonation triggering systems are being employed and can be expected in the future.
- Fixed Army or Air Force installations, such as logistics, maintenance, housing, and meal facilities, are characteristic of lengthy counter-insurgency operations. These locations are very vulnerable to a variety

of WMD area attacks, facilitated by the availability of civilian satellite optical surveillance imagery for targeting. One example is radioactive dust deployed from stand-off locations.

- Anti-satellite attacks on U.S. surveillance, communication, and navigation satellites are a real possibility after the 2007 test of an anti-satellite weapon by the People's Republic of China. Both low-earth-orbit satellites and higher-orbit satellites are vulnerable.
- The resupply of fuel and heavy munitions to U.S. forward air bases could be severely hampered by the use of cruise missiles launched from submarines or even from small civilian boats.

Most Effective Attack Options

Selection of "Best" Attack Options

Tables 2-2 through 2-11 examined a series of representative tactical objectives across the eight modalities examined in this study and attempted to determine how, from Red's perspective, each modality could be employed to achieve a particular objective. The intent of that analysis was to find "the most promising single modality attack options" to satisfy each tactical objective.

Armed with this identification of attack options for achieving a representative set of strategic and tactical objectives, it is possible to look across modalities and determine the attack options that make the most sense to Red. "Made the most sense" implies a filtering or screening process and, while a more detailed quantitative analysis supported by reasonable metrics was preferred, that was not practical within the constraints of this study. Therefore judgment, albeit in a structured framework, was used. The subjective filters considered in determining the best attack options included the following:

- The number of times similar applications of a given modality satisfied one of the 10 representative strategic objectives
- Operational criteria:
  - availability of resources
  - ease of implementation
  - minimum required personnel
  - effectiveness in meeting objectives

  - surety of result
  - risk of interdiction
  - ease of mitigation by Blue
- More abstract but nevertheless important factors
  - Low cost: human intensive rather than technology intensive
  - Flexible: attack approaches that offer the most operational flexibility so they can be used against more of the objectives rather than optimizing them for a one or a few
  - Scalable: attack approaches that offer the most flexibility in scale of attack; one would prefer a weapon that can be scaled from a few casualties to hundreds or more, depending upon the specific objective
  - Known: few uncertainties in terms of operations, construction, acquisition, expertise, and effects. The very nature of the known is that the risk is lower
  - Difficulty in Blue's ability to employ countermeasures: some attacks are fundamentally more difficult to countermeasure than others, as are more diverse attacks

Table 2-13 lists the 18 selected single-modality attack options, arrayed by modality, that resulted from this analysis and that appeared to be very favorable from a Red perspective. The "best way" for Red to achieve an objective will vary widely with the situation and the Blue environment so, rather than select some smaller number of the highest priority attacks, all 18 were addressed in the belief that Red, given the necessary resources and motivation, would try to develop the capability for as many of these as feasible, within the constraints of available resources.

The Role of Information Operations

Not shown in Table 2-13 are the attack options related to cyber warfare. As single-modality attacks, these are powerful weapons in themselves with the potential, for example, to disrupt both civilian and military targets. For military targets, cyber warfare attacks can feed false information to command and control structures; can neutralize Blue intelligence, surveillance, and reconnaissance advantages; and can degrade Blue precision. In a more general sense, these attacks can demoralize Blue troops and sow mistrust throughout the chain of command.

Table 2-13. Eighteen Attack Options Favored by Red

Modality	Attack Options
Nuclear	▪ Blackmail—threaten attack on major U.S. or allied city ▪ Iconic attack on military, *e.g.*, Guam, Carrier Battle Group ▪ Actual attack on major U.S. or allied city
Biological	▪ Attack military through water or food supply ▪ Attack civilians in high density urban setting ▪ Attack economy, *e.g.*, agriculture, cattle industry
Chemical	▪ Attack people in high density enclosed spaces ▪ Military area denial using persistent agent, *e.g.* APOD, SPOD ▪ Release of In Situ toxic industrial chemicals, *e.g.* chlorine storage
Radiological	▪ Denial of critical military area, *e.g.*, APOD, SPOD ▪ Denial of important economic area, *e.g.*, Wall Street
EMP	▪ High altitude nuclear effect—Van Allen Belt and/or EMP
Directed Energy	▪ Jamming critical military resource, *e.g.*, GPS, ISR, communications ▪ Blinding ISR assets ▪ Ground-based ASAT
High Explosive	▪ Conventional use, *e.g.*, mines, direct assent ASAT ▪ Campaign, *e.g.,* IED ▪ Single attacks with long economic tail, *e.g.*, 9/11, Hoover Dam

When used against civilian targets, cyber warfare can disrupt Blue civil command and control structures equally well. In addition, success in this area can corrupt financial networks and disrupt the economy. Attacks could also disable air traffic control and municipal utilities and supervisory control and data acquisition (SCADA) systems, ultimately negating public safety systems. Well-planned attacks can spread a variety of false information, may cause panic, and could lead to a number of other effects. Cyber attacks alone could, in some circumstances and with some opponents, accomplish many of the strategic objectives described earlier in this chapter.

In addition, while generating Tables 2-2 to 2-11, it quickly became apparent that virtually every attack would benefit from a coordinated attack in the influence operations area in one form or another, perhaps several. In fact, it seems almost incomprehensible that any significant opponent would fail to capitalize on the gains from such a coordinated supporting attack. A consideration of the attributes from a Red perspective reveals the following benefits:

- coordination can be relatively loose
- Blue systems have a variety of vulnerabilities
- magnification factor for sowing confusion is high
- cost is low
- risk of attribution or apprehension can be low
- the perpetrator/executor of the influence operations element can be a world away

The goals of such a supporting attack with influence operations can range from simply creating confusion and panic among the first responders and the population of the affected area, to a sophisticated attack on its own intended to seriously degrade or damage SCADA systems or even to kill numbers of people. Blue has defenses against this kind of influence operations attack but there are known vulnerabilities in the design and architecture and almost certainly some introduced by potential opponents of the United States.

The United States is probed every day via cyber warfare. Because no great disaster has occurred, some believe that Blue defenses are adequate or simply that the Red opponents haven't found the right time yet. To some extent, both are likely to be true. As with all of the modalities described here, defense is much more difficult than attack.

What the United States must worry about is the level of sophistication and the size of development efforts in cyber warfare conducted by various potential opponents. In the intelligence assessment of these factors for countries, non-state actors, and others, the study found that the United States is not alone at the top in cyber capabilities. Although the Red opponents may be relatively close in terms of sophistication, the edge may well go to the side with the hidden malicious code or unrecognized hardware tampering.

Representative Attacks

The 18 generic attacks in Table 2-13 were augmented to include two cyber attacks that could be carried out either by themselves or in combination with one or more of the 18. The two added attacks were both against computer networks. One focused on military networks, such as those that supported C4ISR or battlefield communications, and the other against important civilian networks such as SCADA or financial systems.

Each of the resulting 20 single-modality attacks was then further evaluated from a Red and Blue perspective. This assessment involved establishing the likely placement of each of the 20 attacks in a two dimensional plot—one dimension being the favorability to Red and the other being the potential damage or disruption to Blue. The former was determined by roughly quantifying the Red favorability elements discussed previously (*e.g.,* flexibility, scalability, resources required, ability to meet objectives, extent of unknowns, and so on) and the latter by establishing three Blue criteria: (1) the potential damage created by a successful and unmitigated attack, (2) the probability that the attack would be discovered and interdicted, and (3) the degree to which Blue could mitigate the effects of the attack. The results for the 20 representative attacks are plotted in Figure 2-4 for two cases: a state actor perpetrating attacks overseas and a non-state actor attacking assets in the United States.

The plots are derived in a formal yet admittedly subjective manner, and are believed to be qualitatively correct.[42] Note that the upper right hand area of the plan should be the most worrisome to Blue, as it is the area that is most favorable to Red and potentially damaging to Blue. As demonstrated in previous studies, nuclear, cyber, and biological continue to emerge as the three most worrisome modalities and deserve the most attention.

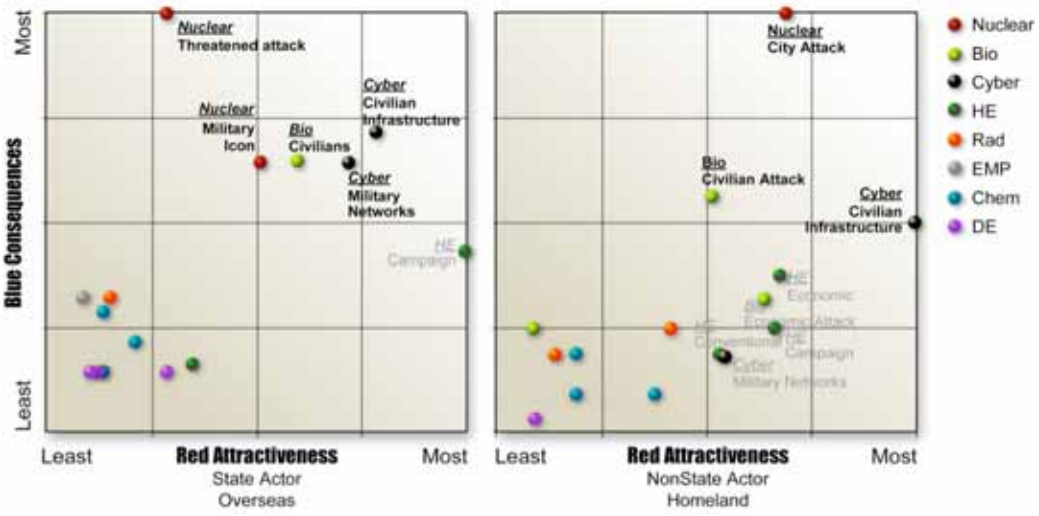


Figure 2-4. Subjective Prioritization of the 20 Generic Attacks

42. The data for these plots is included in Appendix II-A.

Chapter 9. How Blue Can Respond: Recommendations

The previous chapter identified what are believed to represent some of the most devastating potential attacks that could be undertaken using each of the modalities assessed in this study. The results of this effort point to the need for the United States to take serious and meaningful action now to prepare for, prevent, mitigate, and recover from the type of attacks described.

One of the easiest but still meaningful courses of action is to focus initially on steps that can readily be taken to prevent an easy path for an adversary to do serious damage. Perhaps the most obvious example of this type of action was discussed extensively in the *Defense Science Board 2005 Summer Study on Reducing Vulnerabilities to Weapons of Mass Destruction*—controlling all cesium in the United States, the material of choice for radiological ("dirty bomb") attacks. Figure 2-5 indicates the location of the 1,117 ^{137}Cs irradiators of 1,000 curies or more. Replacements using X-ray or ^{60}Co irradiation for these are available, and replacement of all is estimated to cost approximately $200 million.

This investment is a very small fraction of what it would cost to clean up or replace the contaminated areas from even one successful attack. It is also much less than the cost of long-term security to prevent access to these sources. Furthermore, that security typically would rely on detection followed by response from local authorities and cannot be effective against a concerted adversary. Depending on the targeted area, the impact on the United States' economy would likely be huge. For example, one of these samples, dissolved in water and sprayed uniformly could render a large section of Manhattan unusable for decades.

Taking the adversary's view for an extended period provided new insights into the likely exchanges that will come in this long war. There seem to be little difficulty and few obstacles for modestly educated adversaries in the not too distant future using available material and easily accessed or obtained facilities to execute very damaging blows to the United States—blows that could have significant impact economically, militarily, societal, and/or politically, perhaps even to the extent of ripping the national fabric.

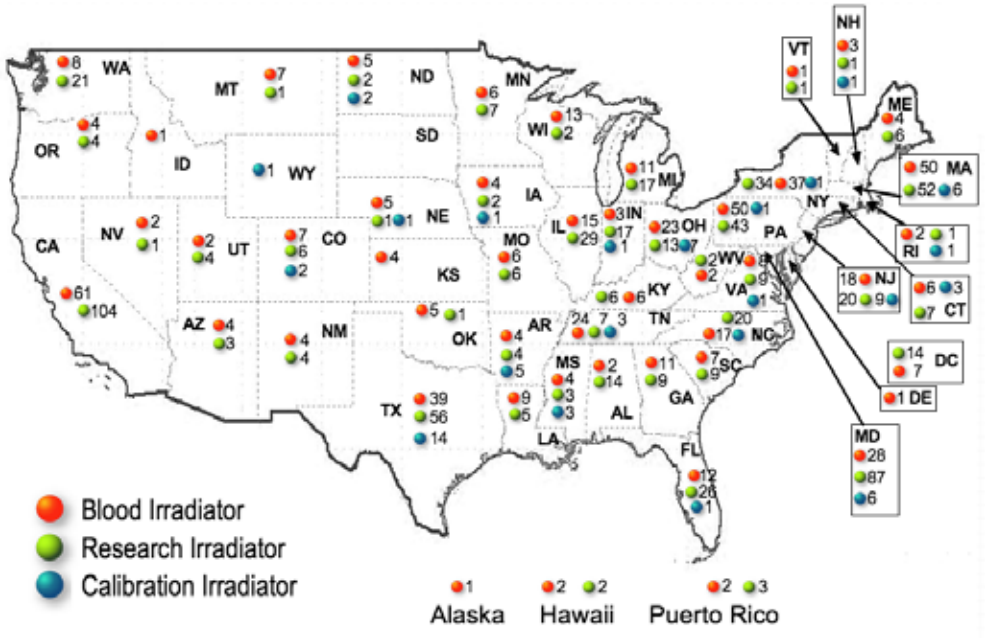


Figure 2-5. Location of Cesium-based Irradiators in the United States

Informed by the Red considerations discussed above, the final piece of this assessment returned to focus on Blue. The following conclusions and recommendations are made, therefore, from a U.S. perspective.

Each of the 20 representative attacks charted in Figure 2-4 was examined from the Blue perspective, with an eye toward ways to enhance prevention, interdiction, mitigation, and recovery, while at the same time, reducing the value (and therefore favorability) to Red. The combination of both of these effects is the essence of deterrence.

By way of example, the following response to a Red biological attack on Blue details a number of actions Blue might take to prevent, interdict, mitigate, or deter an attack on civilians in the homeland using a release of *B. anthracis* aerosol in large enclosed space. The attack could be any one of attacks listed in the **Biological** column in Table 2-10[43], as well as a biological weapon attack on civilians in high density urban setting.

43. "Release in crowds in multiple cities," "Senate Office Building attack," or "Infect crowds in theaters or airplanes, announce afterwards."

- **Prevention**. None for release in buildings or sports stadiums except portal screening for biological agent for all people, bags, and other sources.
- **Interdiction**. Networks of real-time sensors, including bioagent specific, class-specific, such as spores, generic for respirable aerosols, generic for pressurized canisters, surveillance for suspicious activities.
- **Mitigation**. Building response, purge HVAC, replace fresh air, exhaust contaminated air, rain-out bio-aerosol. Medical response, stockpile therapeutics, pre-distribute treatment, implement rapid exposure mitigation (*i.e.*, showers), assess rapid exposure, enable rapid diagnostics.
- **Recovery**. Map surface contamination to aid decontamination, use decontamination foams and sprays, purge building with antimicrobial vapor.
- **Deterrence.** Anti-microbial paints and fabrics, personal gas masks, air purifiers, and air replacement.

Priority Recommendations

A similar approach to the above for the biological attack was made for all 20 attacks in terms of examining ways to lessen the impact on Blue and the value to Red.[44] The following subsections outline some of the resulting recommendations in each of the eight threat modalities. The first three, referred to as the "big 3"—nuclear, cyber, and biological—received the most emphasis. In addition, the *DSB 2005 Summer Study on Reducing Vulnerabilities to Weapons of Mass Destruction* addressed this subject more comprehensively and should be considered complementary.[45]

44. The Blue responses to the 20 representative attacks are discussed in detail in their respective modality appendices.
45. *Defense Science Board 2005 Summer Study on Reducing Vulnerabilities to Weapons of Mass Destruction.* 2005. Washington D.C., Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

RECOMMENDATIONS: NUCLEAR

Do everything possible to prevent nuclear weapons from getting into the hands of adversaries who are not likely to be deterred by cold war approaches—including both terrorists whose values are not well understood and, therefore, not likely to be held at risk, and nation states with leadership that borders on the irrational.

The essence of prevention in this case is cutting off the supply, either by making movement of material more difficult or by enhancing Blue's ability to determine the origin of nuclear material and holding those suppliers, who may be more easily deterred, responsible. Thus, **attribution of suppliers is a critical contributor to their potential deterrence.**

Such activities include:

- supporting non-proliferation initiatives
- improving forensics, including tasking intelligence to collect samples
- continuing declaratory policy regarding passive loss of control and active support
- taking away the easy paths for moving nuclear weapons and materials around (and, in the case of fully assembled weapons, assuming the adversary will have guaranteed "salvage fuzing")

Regardless of efforts to prevent a nuclear attack on the United States, it must at least be assumed that such an attack will eventually occur. **Public education, along with prudent preparations, can limit damage and loss of life, potentially saving tens or even hundreds of thousands of lives if and when that attack happens.** The public needs to understand the actions and role of the individual. There needs to be plans and exercises in advance. If everyone understands their role, the potential for widespread panic is diminished.

This course of action has to be well thought through in order to gain public understanding and cooperation without causing unnecessary panic. Public education on the potential for nuclear attack and responding measures in terms of preparation and action, if and when an attack takes place, should be organized

along the lines of civil defense during World War II.[46] Detailed plans need to be developed for every significant population center, and resource-appropriate fallout shelters should also be designated.

If an attack occurs, the nation needs the capability to identify the parties responsible. Post-detonation attribution capabilities should enable initial assessment within 48 hours. To achieve such a capability, the following actions should be taken:

- DTRA assume responsibility for robustness of post-detonation technical forensics:
  - Identify collection and analysis limitations that compromise timeline and accuracy goals. Identify and begin implementation of programs to reduce these limitations.
  - Define and execute red team assessment of countermeasures to technical forensics.
  - Triple current DTRA funding (from ~$10 million in fiscal year 2007 to ~$30 million) for this mission.
- Task intelligence community with population of nuclear materials databases per NSPD-17, Annex IV.
- U.S. Strategic Command/DTRA plan and execute realistic response exercise with senior leadership.
- Reflect in all of the above, constraints and uncertainties of realistic attribution environments.

In the area of post-detonation consequence management, the goal is local capability for major U.S. cities for initial 1–3 days of response.

- National Guard work with local authorities to ensure detailed response plans (radiation hazards, shelter/evacuation decisions, medical surge, pragmatic decontamination for many 1,000s of people).
- Exercise with National Guard Civil Support Teams and U.S. Northern Command assets upon completion of plans.

---

46. For example, Civil Defense Wardens or Community Emergency Response Teams. See https://www.citizencorps.gov/cert/ for status.

RECOMMENDATIONS: CYBER WARFARE

Cyber warfare is potentially the most devastating modality after nuclear and is very attractive to adversaries of all sizes and capabilities. Cyber warfare could be used in single modality attacks against command and control and most of the nation's infrastructure and financial systems; the attacks in Estonia in May 2007 were examples of what could happen. In addition, its use can enormously magnify the effects of an attack with another modality or modalities. For example, cyber warfare could be used to deny first responders the ability to communicate, corrupt situational awareness, insert false reports in the media, and cause loss of faith in the U.S. government's ability to protect its population. Its use is equally applicable to causing disruption in military operations and those that enable distributed force coordination on the battlefield and in urban environments.

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD [AT&L]) and the Assistant Secretary of Defense for Networks and Information Integration (ASD [NII]) identify DOD's mission critical systems and make their protection a priority:

- Selection process—Y2K process model for identifying/ranking critical systems.
- Design and build them differently:
  - use technically diverse systems
  - create protected supply chain for essential capabilities
  - implement protected capability citadels/fail soft/wartime reserve modes
  - use red teams early and often through life cycle
  - harden with anti-tamper technology where appropriate
  - provide intelligence on adversary cyber capabilities (and industry)
- Test them differently:
  - independent red teams design and participate in tests
  - include cyber offense and defense capabilities in test and exercise plans

  - perform aggressive operational test and evaluation iteratively through life cycle, on occasion to the point of breakage
  - evaluate timeliness of recovery and remediation
- Exercise/operate them differently:
  - based upon strong, current intelligence on adversary cyber capabilities
  - in degraded modes multiple times per year
  - based upon lessons learned returned to the design, build, and test processes

Deputy Secretary of Defense educate industry CEOs on industry's cyber vulnerabilities and adversary capabilities; solicit their participation in protection and remediation activities

USD (AT&L) and ASD (NII) increase efforts on computer network defense. Carefully assess where additional resources could significantly improve Blue's defensive posture, including separate and hardened control systems, and apply appropriately.

RECOMMENDATIONS: BIOLOGICAL

Biological attacks can take a variety of forms, ranging from outdoor aerosol delivery, to widespread contact with an infected individual, to corruption of the food or water supply chain, to direct contact such as anthrax in the mail. Each of these forms may be detected when delivered, but may not be recognized until the incubation period has passed and symptoms are manifested. The wide range of possibilities makes prevention heavily dependent on intelligence, places a premium on early detection and characterization of the attack, and puts heavy emphasis on mitigation after the attack. In the longer term, it may be possible (and is the subject of a significant level of current investment) to develop vaccines and therapeutics that deal with classes of biological agents rather than each one at a time—these are called broad-spectrum drugs and have the long term potential to negate the adversary value of biological attacks.

Interdiction

- **DTRA/Joint Program Executive Office (JPEO) for Chemical and Biological Defense develop sensor networks in critical enclosed spaces of DOD (*e.g.*, critical C3 nodes) for real-time triggers/identifiers integrated with HVAC to control/contain contamination.**

Mitigation

- **Assistant Secretary of Defense for Health Affairs advance DOD medical surveillance/response program for biological attack and coordinate with civilian programs** (Center for Disease Control/Federal Bureau of Investigation/Department of Health and Human Services):
  - rapid diagnostics and networked reporting to contain/control
  - rapid distribution of treatments/prophylaxis (1–2 days)
- **Find mechanisms and institute programs to address medical surge requirements (applicable to nuclear and chemical weapons as well).** Some specific trial programs under this recommendation were provided in the *DSB 2005 Summer Study on Reducing Vulnerabilities to Weapons of Mass Destruction*. Review, assess, and implement if deemed appropriate. (Department of Homeland Security)

Attribution

- **USD (AT&L) expand earlier bio-forensics/global reference database to identify specific bio-agents and attributes (virulence, drug resistance).**

Recovery

- **Continue development of diagnostics and broad-spectrum antimicrobials/vaccines and effective decontamination systems.** (DTRA/DARPA/JPEO)
- **Educate the public so they understand actions taken and know what themselves to do to minimize their risks.** (Department of Homeland Security)

Additional Recommendations

Recommendations in other modalities are highlighted below.

RECOMMENDATION: HIGH EXPLOSIVES

High explosives have been a staple of both open conflict and terrorism for centuries and are likely to continue in that role for some time to come. They are almost certainly the most likely form of attack other than the continual use of cyber warfare. Prior to 9/11, the destructive capacity of single high-explosive events tended to be in terms of tens to hundreds of lives; with 9/11 it is now in the thousands and there is real potential for greater numbers with innovative and well-planned attacks.

- Department of Homeland Security charter a team to identify U.S. targets and approaches that, if attacked with a truck load or a regional jet aircraft loaded with high explosives, could kill thousands of people either from primary or secondary effects or significantly disable a key part of the economy. Develop protection plans for these cases. The key challenge to this tasking is to assure innovative thinking.

RECOMMENDATIONS: CHEMICAL

Chemical attacks to kill or injure people are most effective in enclosed spaces such as arenas, large office buildings, or malls. For attacks outside, generally very large quantities are required since dilution occurs rapidly. Therefore, either military delivery or access to toxic industrial chemicals is most effective. The use of persistent chemicals can be effective as an area denial attack.

- Department of Homeland Security develop and deploy detectors for chemical and biological agents that can be installed in HVAC and air handling equipment, along with flow controls, so that on detection of an agent, the air flow is managed to protect people in the spaces. Such detectors can be set to a high-false alarm rate because they will only affect the air flow until the threat is confirmed. Secure and protect all sources of very large quantities of toxic industrial chemicals in close proximity to densely populated areas, such as pressurized chlorine storage facilities or rail sidings.

RECOMMENDATIONS: RADIOLOGICAL

Radiological dispersion device weapons rely on access to radiological materials. These are generally used as an area denial weapon rather than for killing people. Limiting access and rapid cleanup for military attacks is key. For attacks on civilian urban areas, elimination of source material is currently the only practical method.

- Department of Homeland Security require protection of the major radiation sources in the United States and change from attacker-attractive materials to those that are not. For example, substitute e-beam or cobalt technologies for cesium-based sources in blood irradiation systems. Develop effective means of cleanup so that an area denied remains so for only a limited time.

RECOMMENDATIONS: ELECTROMAGNETIC PULSE AND DIRECTED ENERGY

Attacks employing EMP weapons are unlikely by any adversary other than holders of fairly large numbers of nuclear weapons. If the weapons available are few in number, it is probable that the attacker would find more lucrative uses. In addition, in many cases, cyber warfare can accomplish many of the same objectives (albeit for a more limited amount of time) and with much less uncertainty in the eyes of the attacker. **EMP is, of course, a significant threat for a peer or near-peer who is willing to risk crossing the nuclear threshold, even in this somewhat limited manner.**

Directed energy in the forms of jamming, blinding, or high-powered microwaves will almost certainly be used in limited conflicts with a peer or near-peer. It should be recognized that many U.S. systems typically include but do not implement anti-jam techniques to any great extent and thus are often vulnerable. Directed energy is more likely to be used as a secondary, complementary modality to the main thrust of an attack.

Summary

The Red-Blue perspective presented in the previous chapter included an evaluation of 20 representative attacks (Figure 2-4). Figure 2-6 shows the potential impact of the study's recommendations, assuming that the full scope of recommendations from this study are implemented (those from this chapter as well as the classified modality appendices).[47] Although these recommendations are not a panacea and do not totally eliminate the threats, by implementing the recommendations of this study, the potential consequences of these attacks can be lowered significantly and can be made far less attractive to Red. Both are important in reducing the risk to the country, either directly or through the increased degree of deterrence that may be established.

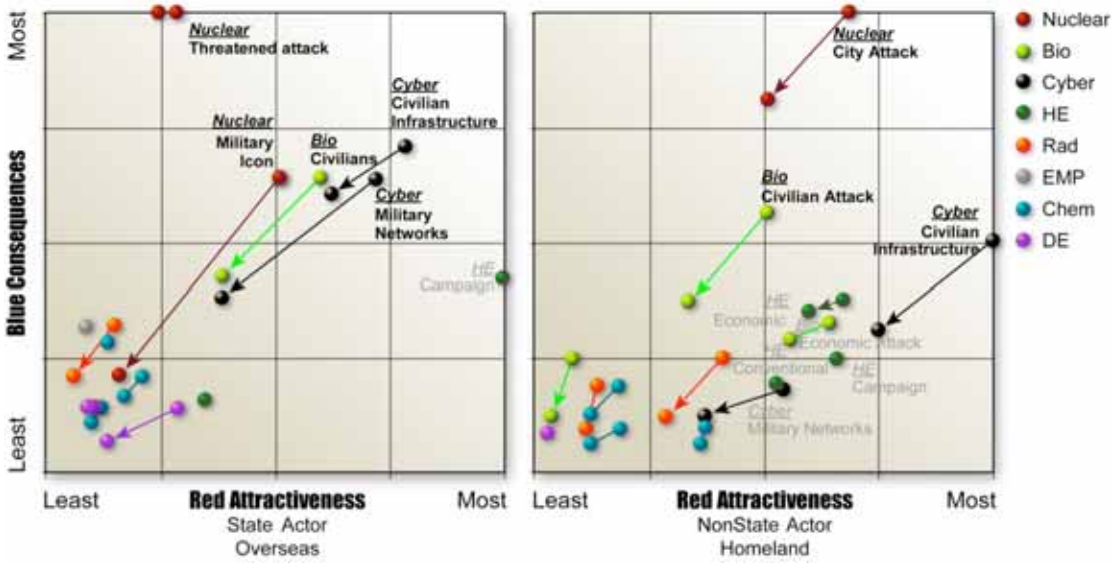


Figure 2-6. Red-Blue Perspective after Recommendations

47. The supporting data for Figure 2-7 is provided in Appendix II-A.

Appendix II-A. Supporting Data for Technology Impact Assessments

Chapters 8 and 9 each contain two "bubble charts," which attempt to portray the appeal to Red and the potential impact on Blue of 20 different attack strategies using the eight threat modalities—nuclear, biological, chemical, EMP, directed energy, radiological, high explosive, and cyber warfare—discussed throughout this report. This assessment was accomplished by establishing a representative, but admittedly inexact, placement of each of the 20 attacks in a two-dimensional plane—one dimension being the favorability to Red and the other being the potential damage or disruption to Blue. The former was determined by roughly quantifying the Red favorability elements, *e.g.*, flexibility, scalability, resources required, ability to meet objectives, and extent of unknowns. The disruption or consequence to Blue was determined by establishing three Blue criteria—the potential damage created by a successful and unmitigated attack, the probability that the attack would be discovered and interdicted, and the degree to which Blue could mitigate the effects of the attack. The data and methods used to establish the two dimensional coordinates of each of the 20 attacks are presented here. Tables 2A-1 through 2A-4 correspond directly to the four bubble charts represented as Figures 2-4 and 2-6.

Each of the tables is divided into two main sections, as indicated by the two titles—Red Attractiveness and Blue Consequences. Each relevant intersection of an attack tactic is scored according to a two-part assessment—red, yellow, green and blue—representing "Poor," "Fair," "Good," and "Excellent," respectively. In order to roll up the results into an overall assessment, the assigned colors are each given a numerical value of 1, 2, 4, and 8, respectively. This geometric, rather than arithmetic, progression is used to ensure that the relative impact of moving from one category to another stays constant regardless of which category is under consideration. In selected cases, an intermediate number was assigned; for example, a 6 may be assigned for a situation that was not really "excellent" but better than others that were listed as "good."

Red Attractiveness

The Red perspective in all of the charts considers the four principal attributes listed under Red, and within each of these attributes, a number of sub-considerations, as described below.

Flexibility

Flexibility is made up of two considerations, one numerical and one judgmental. The numbers in the *Multi-Use* column represent how many times each *Attack Tactic* appeared as a viable option in the 10 tactical objectives tables in Chapter 8 for the appropriate adversary types—i.e., state actor or non-state actor. The color scheme employed is yellow for 1, green for 2 or 3, and blue for 4 and above. The colors in the *Scalability* column are subjective assessments as to how scalable the use of a given modality is to the attack objective listed. At one end of the spectrum are nuclear attacks, which regardless of yield are of very high consequence, and at the other end of the scale are high explosive and counter network operations—both of which can be scaled from very significant down to relatively minor, if desired. The *Overall* column is simply the average color of the two preceding columns.

Operational Effectiveness

The assessment of Red operational effectiveness is made up of three considerations, all of which were determined subjectively. It is also the only set of Red considerations that are determined numerically before establishing colors. The numbers in each of the three columns represent judgment as to the probability, from 0 to 1, of each attack satisfying the criteria listed in the column heading. The *Effectiveness, Meets Objectives* entry represents the judgment of the panel that the attack strategy—supposing Blue can neither interdict the attack nor mitigate its effects—will achieve the tactical objectives. Because these assessments are from a Red perspective, the color scheme reflects that a high probability is good and a low probability is bad. *Risk of Interdiction* and *Probability of Blue Mitigation* represent the likelihood that the attack will be stopped by Blue or, if not stopped by Blue, that the intended effects will be mitigated.

In both of these assessments, low numbers are good from a Red perspective, and therefore, a probability of zero is blue, 0.25 is green, 0.50 is yellow, and 0.75 is red. The final *Overall* column is calculated as a sequence of probabilities representing the three considerations in tandem leading to a successful attack—*i.e*, the probability that the attack will meet objectives given no interdiction or

mitigation, multiplied by one, minus the probability of interdiction, multiplied by one, minus the probability of mitigation. The *Overall* assessment represents Red's expectation that the use of that modality in the way described will satisfy the objectives given whatever Blue can do to stop or mitigate it. Therefore, high numbers are good and low numbers are poor. Because they are calculated, the values may fall anywhere between 0 and 1. The color scheme represents that perspective, with red for values less than 0.25, yellow for values from 0.025 to less than 0.050, green for values from 0.050 to less than 0.75, and blue for values above 0.75.

Other Operational Issues

This assessment addresses Red's confidence in achieving the intended results. *Surety of Result* deals with the uncertainty in the linkage between the physical or direct outcome of the attack and the tactical effect that is desired, under the assumption that the attack is neither interdicted nor mitigated by Blue. *Unintended Consequences* considers effects that were not planned and may not be desirable from a Red perspective. An example might be a targeted Blue nuclear response on population centers to the use of a high altitude nuclear event by Red that was narrowly aimed at destroying some satellites. Red's calculus might assume that Blue would not respond with a nuclear ground attack to a Red event that created no physical damage on the ground, but Red would likely look hard at the downside of a Blue reaction beyond that assumption. *Knowns and Unknowns* considers the physical surety of the direct effect actually happening. A good example of "poor" in this category is the use of a nuclear event to create EMP damage to Blue.

Many orders of magnitude of uncertainty exist in both the creation of the pulse and the coupling into specific electronic equipment, and Red's enthusiasm for employing EMP as an attack tactic would certainly be tempered by this uncertainty. Contrasting with this is the use of high explosives, for which nearly all of the effects are well known as a function of size and type of explosive. Uncertainties are very small and Red can be confident that what he assumes will happen, will indeed happen, at least from a physical effect point of view. The *Overall* column presents the arithmetic average of values in the three subcategories. The color scheme is as follows: red for values below 1.5, yellow for values equal to or greater than 1.5 but below 3, green for values equal to or greater than 3 but below 6, and blue for values 6 or above.

Availability and Readiness

This assessment deals with Red's ability to acquire the necessary resources and have them available to implement an attack. Three subcategories are considered: *Resource Availability* weighs the relative availability of getting the critical modality material and any required specialized fabrication equipment or critical skills to weaponize the device; *Implementation Ease* examines the complexity involved, given the existence of the weapon, in creating an effective attack, including the steps involved, the complexity of the planning process, the need for rehearsals, and so on; *Personnel Required* assesses how many people would be involved in both perpetrating the attack and in whatever training and coordination is required, both of which have an impact on Red's assessment of potential discovery by Blue. The *Overall* column is once again the arithmetic average of the three subcategories and employs the same color scheme as in *Other Organizational Issues.*

Overall Red

Overall Red combines all of the elements under the preceding four categories. Values are calculated by multiplying the *Overall Operational Effectiveness* by the average of the *Overall* assessments in *Flexibility*, *Other Operational Issues,* and *Availability and Readiness*. This way of combining the four scores—*i.e.*, using the *Overall Operational Effectiveness* as a multiplier—seemed reasonable because if a particular attack tactic has very little or no expected operational effectiveness, other factors matter little. In averaging the other three categories, no factor dominated the others, and the values were combined in this way. The end results were normalized in all four scenarios by a factor of 1.5 to give the best attack tactic a score of 8, and these were colored using the scheme described for *Other Operational Issues*. The *Overall Red* scores as shown in the four tables are used to position the balls horizontally in Figures 2-4 and 2-6.

Blue Consequences

In assessing the potential consequences to Blue, there were three considerations. The first, labeled *Consequence*, was a judgment, qualitatively determined, as to how devastating the results of a successful and unmitigated attack would be on Blue from a variety of standpoints—economic, political, military readiness, etc.—depending upon the nature of the attack. The standard scale of 0 to 8 was used, with high numbers representing very serious consequences and low numbers less serious. Standard color-coding was applied. The values for *Probability of Interdiction* and the *Probability of Blue Mitigation* ranged from 0 to 1 and were treated as though they were probabilistic.

Here, since high probabilities are good for Blue (the inverse of the situation for Red), a zero chance of interdiction or no ability to mitigate are colored red, whereas higher numbers are yellow or green. In the same manner as in the Red assessment, the values for *Overall Blue* were arrived at by multiplying the assessed raw *Consequence* by one minus the probability of interdiction and one minus the degree or probability of Blue mitigation. Here, low numbers are good and therefore the color scheme is inverted: blue for values below 1.5, green for values equal to or above 1.5 but below 3, yellow for values equal to or above 3 but below 6, and red for values equal to 6 or higher. The *Overall Blue* score is used to position the balls vertically in Figures 2-4 and 2-6.

Data Tables

All of the assessments are determined using the techniques and scoring strategies described above. Table 2A-1 represents the 20 attacks, as they might be assessed today, for all of the attacks serving the strategic objectives of a state actor operating against the United States overseas. It corresponds to the left chart in Figure 2-4. Table 2A-3 represents the same situation, but under the assumption that all of the recommendations relating to the eight modalities have been fully implemented. It corresponds to the left side of Figure 2-6. Table 2A-2 represents the 20 attacks, as they might be assessed today, for all of the attacks serving the strategic objectives of a non-state actor operating within the U.S. homeland. It corresponds to the right side of Figure 2-4. Table 2A-4 represents the same situation, but under the assumption that all of the relevant recommendations have been fully implemented. It corresponds to the right side of Figure 2-6.

Final Note

The reader will notice that the scores under Red for *Interdiction* and *Mitigation* are the same as those listed under Blue. In hindsight, it is more likely that Red would adopt an "offense conservative" view of these probabilities *(i.e.,* Red would tend to assess them at the high end of a possible range) because Red's concern would be "what if" things went wrong for Red and right for Blue. Blue, in contrast, would adopt the opposite, or a "defense conservative" view, based upon Blue's desire to understand what might happen if Red pulled things off just right and Blue's actions didn't actually happen quite as planned. The effect of these conservative perspectives would be to move the balls in the figures slightly higher (worse for Blue) and slightly to the left (not as favorable to Red). These movements would be small and unlikely to affect the overall trends shown in the charts.

Table 2A-1. Prioritization Assessment - State Actors Engaged in Overseas Activities

		Red Attractiveness															Blue Consequences			
		Flexibility			*Operational Effectiveness*				*Other Operational Issues*				*Availability and Readiness*							
Modality	**Target of Attack**	Multi-Use	Scalability	Overall	Effectiveness, Meets Objectives	Risk of Interdiction	Probability of Blue Mitigation	Overall	Surety of Result	Unintended Consequences	Knowns and Unknowns	Overall	Resource Availability	Ease of Implementation	Personnel Requirements	Overall	**Overall Red**	Consequence	Probability of Interdiction	Probability of Blue Mitigation	**Overall Blue**
Nuclear	Threaten city	2	1	2	0.50	0.00	0.00	0.50	2	1	8	3.67	4	2	4	3.33	2.3	7	0.00	0.00	7.0
	Military icon	2	1	2	1.00	0.25	0.00	0.75	8	1	8	5.67	4	2	4	3.33	4.1	6	0.25	0.00	4.5
	City																				
Biological	Military																				
	Civilians	2	4	4	1.00	0.00	0.25	0.75	4	2	4	3.33	8	4	4	5.33	4.8	6	0.00	0.25	4.5
	Economy																				
Chemical	People in Enclosed Spaces	3	4	4	0.75	0.50	0.25	0.28	4	2	4	3.33	8	2	4	4.67	1.7	4	0.50	0.25	1.5
	Area Denial	3	4	4	0.75	0.50	0.50	0.19	2	2	2	2.00	8	2	4	4.67	1.0	4	0.50	0.50	1.0
	People in Open (TIC)	1	2	2	0.50	0.00	0.50	0.25	1	2	1	1.33	8	4	4	5.33	1.1	4	0.00	0.50	2.0
Radiological	Area Denial	1	2	2	0.75	0.50	0.25	0.28	4	2	4	3.33	2	4	4	3.33	1.2	6	0.50	0.25	2.3
	Economy																				
EMP	HANE	3	1	2	0.50	0.25	0.25	0.28	1	1	1	1.00	1	2	2	1.67	0.7	4	0.25	0.25	2.3
DE	Jamming Military Assets	3	4	4	0.75	0.00	0.50	0.38	2	8	2	4.00	4	4	4	4.00	2.3	2	0.00	0.50	1.0
	Blinding ISR	2	2	3	0.75	0.50	0.50	0.19	4	4	2	3.33	4	2	4	3.33	0.9	4	0.50	0.50	1.0
	Ground-based ASAT	1	4	3	0.75	0.50	0.50	0.19	2	2	4	2.67	2	2	4	2.67	0.8	4	0.50	0.50	1.0
HE	Conventional, e.g., mines, LEO	6	8	8	0.50	0.25	0.25	0.28	4	8	8	6.67	8	4	4	5.33	2.8	2	0.25	0.25	1.1
	Conventional Campaign, e.g., IEDs	4	8	8	1.00	0.25	0.00	0.75	4	8	8	6.67	8	8	4	6.67	8.0	4	0.25	0.00	3.0
	Single Attack with long economic tail																				
Cyber	Disrupt civilian infrastructure	2	8	6	0.75	0.00	0.00	0.75	2	4	4	3.33	8	6	8	7.33	6.3	5	0.00	0.00	5.0
	Military Networks	4	8	8	0.75	0.00	0.25	0.56	2	8	6	5.33	8	6	8	7.33	5.8	6	0.00	0.25	4.5

Not applicable | Poor | Fair | Good | Excellent

TIC - Toxic Industrial Chemicals
HANE - High Altitude Nuclear Explosion
LEO - Low Earth Orbit
IED - Improvised Explosive Device
ASAT - Anti-Satellite Weapon
ISR - Intelligence, Surveillance, Reconnaissance
DE - Directed Energy weapons
HE - High Explosives
EMP - Electromagnetic Pulse weapons
TIC - Toxic Industrial Chemicals

Table 2A-2. Prioritization Assessment - NonState Actors Engaged in Activities in the Homeland

		Red Attractiveness															Blue Consequences			
		Flexibility			*Operational Effectiveness*				*Other Operational Issues*				*Availability and Readiness*							
Modality	**Target of Attack**	Multi-Use	Scalability	Overall	Effectiveness, Meets Objectives	Risk of Interdiction	Probability of Blue Mitigation	Overall	Surety of Result	Unintended Consequences	Knowns and Unknowns	Overall	Resource Availability	Ease of Implementation	Personnel Requirements	Overall	**Overall Red**	Consequence	Probability of Interdiction	Probability of Blue Mitigation	**Overall Blue**
Nuclear	Threaten city																				
	Military icon																				
	City	4	1	2	1.00	0.00	0.00	1.00	8	4	8	6.67	2	1	4	2.33	5.5	8	0.00	0.00	8.0
Biological	Military	1	4	2	0.25	0.00	0.50	0.13	2	8	2	4.00	8	2	4	4.67	0.7	4	0.00	0.50	2.0
	Civilians	8	2	4	0.75	0.00	0.25	0.56	4	4	6	4.67	8	6	4	6.00	4.1	6	0.00	0.25	4.5
	Economy	2	2	2	0.75	0.00	0.15	0.64	4	8	6	6.00	8	8	8	8.00	5.1	3	0.00	0.15	2.6
Chemical	People in Enclosed Spaces	4	4	4	1.00	0.50	0.25	0.38	4	8	6	6.00	8	6	4	6.00	3.0	2	0.50	0.25	0.8
	Area Denial	4	4	4	0.75	0.25	0.50	0.28	2	8	2	4.00	2	2	4	2.67	1.5	2	0.25	0.50	0.8
	People in Open (TIC)	3	2	2	0.75	0.50	0.25	0.28	1	8	2	3.67	8	2	4	4.67	1.5	4	0.50	0.25	1.5
Radiological	Area Denial	4	2	3	1.00	0.50	0.00	0.50	6	6	4	5.33	6	4	4	4.67	3.3	4	0.50	0.00	2.0
	Economy	5	2	3	0.50	0.25	0.50	0.19	2	6	4	4.00	6	4	4	4.67	1.1	4	0.25	0.50	1.5
EMP	HANE																				
DE	Jamming Military Assets	2	4	3	0.50	0.00	0.75	0.13	2	8	2	4.00	6	4	4	4.67	0.7	1	0.00	0.75	0.3
	Blinding ISR																				
	Ground-based ASAT																				
HE	Conventional, e.g., mines, LEO	7	8	8	0.50	0.25	0.00	0.38	4	8	8	6.67	8	8	8	8.00	4.3	2	0.25	0.00	1.5
	Conventional Campaign, e.g., IEDs	6	8	8	1.00	0.50	0.00	0.50	6	8	8	7.33	8	6	4	6.00	5.3	4	0.50	0.00	2.0
	Single Attack with long economic tail	4	8	6	0.50	0.25	0.00	0.38	2	8	8	6.00	8	8	8	8.00	3.8	3	0.25	0.00	2.3
Cyber	Disrupt civilian infrastructure	9	8	8	0.75	0.00	0.00	0.75	4	8	6	6.00	8	6	8	7.33	8.0	4	0.00	0.00	4.0
	Military Networks	2	8	4	0.75	0.00	0.25	0.56	2	8	4	4.67	8	4	8	6.67	4.3	2	0.00	0.25	1.5

Not applicable | Poor | Fair | Good | Excellent

Table 2A-3. Prioritization Assessment—with Recommendations Implemented—State Actors Engaged in Overseas Activities

		Red Attractiveness															Blue Consequences			
		Flexibility			*Operational Effectiveness*				*Other Operational Issues*				*Availability and Readiness*							
Modality	Target of Attack	Multi-Use	Scalability	Overall	Effectiveness, Meets Objectives	Risk of Interdiction	Probability of Blue Mitigation	Overall	Surety of Result	Unintended Consequences	Knowns and Unknowns	Overall	Resource Availability	Ease of Implementation	Personnel Requirements	Overall	Overall Red	Consequence	Probability of Interdiction	Probability of Blue Mitigation	Overall Blue
Nuclear	Threaten city	2	1	2	0.50	0.00	0.00	0.50	2	1	6	3.00	3	2	4	3.00	2.0	7	0.00	0.00	7.0
	Military icon	2	1	2	1.00	0.75	0.00	0.25	8	1	6	5.00	3	2	4	3.00	1.3	6	0.75	0.00	1.5
	City																				
Biological	Military																				
	Civilians	2	4	4	1.00	0.00	0.50	0.50	3	2	4	3.00	8	4	4	5.33	3.1	6	0.00	0.50	3.0
	Economy																				
Chemical	People in Enclosed Spaces	3	4	4	0.75	0.50	0.40	0.23	4	2	4	3.33	8	2	4	4.67	1.4	4	0.50	0.40	1.2
	Area Denial	3	4	4	0.75	0.50	0.60	0.15	2	2	2	2.00	8	2	4	4.67	0.8	4	0.50	0.60	0.8
	People in Open (TIC)	1	2	2	0.50	0.00	0.50	0.25	1	2	1	1.33	8	4	4	5.33	1.1	4	0.00	0.50	2.0
Radiological	Area Denial	1	2	2	0.50	0.50	0.50	0.13	4	2	4	3.33	1	2	4	2.33	0.5	6	0.50	0.50	1.5
	Economy																				
EMP	HANE	3	1	2	0.50	0.25	0.25	0.28	1	1	1	1.00	1	2	2	1.67	0.7	4	0.25	0.25	2.3
DE	Jamming Military Assets	3	4	4	0.75	0.00	0.75	0.19	2	8	2	4.00	4	4	4	4.00	1.1	2	0.00	0.75	0.5
	Blinding ISR	2	2	3	0.75	0.50	0.50	0.19	4	4	2	3.33	4	2	4	3.33	0.9	4	0.50	0.50	1.0
	Ground-based ASAT	1	4	3	0.75	0.50	0.50	0.19	2	2	4	2.67	2	2	4	2.67	0.8	4	0.50	0.50	1.0
HE	Conventional, e.g., mines, LEO	6	8	8	0.50	0.25	0.25	0.28	4	8	8	6.67	8	4	4	5.33	2.8	2	0.25	0.25	1.1
	Conventional Campaign, e.g., IEDs	4	8	8	1.00	0.25	0.00	0.75	4	8	8	6.67	8	8	4	6.67	8.0	4	0.25	0.00	3.0
	Single Attack with long economic tail																				
Cyber	Disrupt civilian infrastructure	2	8	6	0.75	0.15	0.00	0.64	2	3	4	3.00	8	4	8	6.67	5.0	5	0.15	0.00	4.3
	Military Networks	4	8	8	0.75	0.25	0.40	0.34	2	6	4	4.00	8	3	8	6.33	3.1	6	0.25	0.40	2.7

Not applicable | Poor | Fair | Good | Excellent

Table 2A-4. Prioritization Assessment—with Recommendations Implemented—NonState Actors Engaged in Activities in the Homeland

		Red Attractiveness															Blue Consequences			
		Flexibility			*Operational Effectiveness*				*Other Operational Issues*				*Availability and Readiness*							
Modality	**Target of Attack**	Multi-Use	Scalability	Overall	Effectiveness, Meets Objectives	Risk of Interdiction	Probability of Blue Mitigation	Overall	Surety of Result	Unintended Consequences	Knowns and Unknowns	Overall	Resource Availability	Ease of Implementation	Personnel Requirements	Overall	**Overall Red**	Consequence	Probability of Interdiction	Probability of Blue Mitigation	**Overall Blue**
Nuclear	Threaten city																			
	Military icon																			
	City	4	1	2	1.00	0.10	0.10	0.81	8	2	8	6.00	1	1	4	2.00	4.1	8	0.10	0.10	6.5
Biological	Military	1	4	2	0.25	0.00	0.75	0.06	2	8	2	4.00	8	2	4	4.67	0.3	4	0.00	0.75	1.0
	Civilians	8	2	4	0.75	0.00	0.50	0.38	3	4	6	4.33	8	6	4	6.00	2.7	6	0.00	0.50	3.0
	Economy	2	2	2	0.75	0.00	0.25	0.56	4	8	6	6.00	8	8	8	8.00	4.5	3	0.00	0.25	2.3
Chemical	People in Enclosed Spaces	4	4	4	1.00	0.25	0.50	0.38	3	8	6	5.67	8	6	4	6.00	2.9	2	0.50	0.50	0.5
	Area Denial	4	4	4	0.75	0.50	0.50	0.19	2	8	2	4.00	2	2	4	2.67	1.0	2	0.50	0.50	0.5
	People in Open (TIC)	3	2	2	0.75	0.50	0.50	0.19	1	8	2	3.67	8	2	4	4.67	1.0	4	0.50	0.50	1.0
Radiological	Area Denial	4	2	3	1.00	0.50	0.00	0.50	2	6	4	4.00	1	2	4	2.33	2.3	2	0.50	0.00	1.0
	Economy	5	2	3	0.50	0.25	0.50	0.19	2	6	4	4.00	1	2	4	2.33	0.9	2	0.25	0.50	0.8
EMP	HANE																			
DE	Jamming Military Assets	2	4	3	0.50	0.00	0.75	0.13	2	8	2	4.00	6	4	4	4.67	0.7	1	0.00	0.75	0.3
	Blinding ISR																			
	Ground-based ASAT																			
HE	Conventional, e.g., mines, LEO	7	8	8	0.50	0.25	0.00	0.38	4	8	8	6.67	8	8	8	8.00	4.3	2	0.25	0.00	1.5
	Conventional Campaign, e.g., IEDs	6	8	8	1.00	0.50	0.00	0.50	6	8	8	7.33	8	6	4	6.00	5.3	4	0.50	0.00	2.0
	Single Attack with long economic tail	4	8	6	0.50	0.25	0.00	0.38	2	8	8	6.00	8	8	8	8.00	3.8	3	0.25	0.00	2.3
Cyber	Disrupt civilian infrastructure	9	8	8	0.75	0.00	0.00	0.75	4	8	6	6.00	8	6	8	7.33	8.0	4	0.00	0.00	4.0
	Military Networks	2	8	4	0.75	0.00	0.25	0.56	2	8	4	4.67	8	4	8	6.67	4.3	2	0.00	0.25	1.5

Not applicable | Poor | Fair | Good | Excellent

Part III

Nuclear Proliferation: A Special Case

Chapter 10. A Core Emerging Challenge

The previous three chapters examined eight technology areas available to potential adversaries and assessed the implications of attacks using weapons derived from these technologies. As in previous assessments by the DSB, one particular weapon stands in a class by itself in terms of its potential for damage, disruption, and devastation—the nuclear weapon. The importance of nuclear weapons, both in terms of the consequences of their use as well as attractiveness to some potential adversaries, motivated an in-depth look, as part of this study, at the matter of nuclear proliferation in the emerging military landscape.

The U.S. nuclear security environment is multifaceted and encompasses the problems posed by (1) nuclear relations among the major nuclear powers (Russia, China, Britain, France, and the United States), (2) new nuclear weapon states, and (3) non-state actors seeking nuclear weapons. This study focused on only one of these three factors, new nuclear weapon states, and not on the larger problem set. But as appropriate and necessary, it has explored the overlaps among these three problems.

Methodology

Two primary questions guided the assessment of the nuclear proliferation landscape. First, will nuclear weapons be embraced by enemies as their premier asymmetric capability? Second, will nuclear weapons endow a new tier of states with peer-like capabilities to limit U.S. freedom of action? To derive those answers, the following methodology was employed:

1. Looking ahead two decades, how might nuclear proliferation proceed?
2. What would be the consequences for the United States and what will U.S. leaders want to do?
3. What military capabilities and capacities should the Department of Defense create to underwrite these ambitions?
4. Are the needed capabilities coming together? What more needs to be done?
5. Is there anything more that can be done now that might make a substantial difference in preventing proliferation?

It is important to explain the relationship of this fifth item to the remainder of this study. This study, as a whole, looks ahead two decades to the year 2027 and explores how capable our future adversaries might be and what strategies they might pursue. The proliferation problem is explored within that time horizon—how proliferation might unfold between now and then, and its implications for needed military capabilities and capacities in 2027. The primary focus of this assessment is not on how to manage the proliferation problem today in a way that helps to prevent future proliferation. But it does reveal some useful insights into this topic, which will be addressed in response to question number five.

Forecasting the Future of Proliferation

What kind of nuclear proliferation problem will the United States face in 2027? Many people in the defense community already have a clearly defined answer to this question: a rapid breakdown of nuclear order with a doubling or trebling of the number of nuclear-armed states in the next decade or two. In the judgment of this study, this answer is wrong. It is also misleading, as it points to the wrong set of implications for military planning and capability development. In our judgment, the nuclear future cannot be predicted reliably. Some "outcomes" in 2027 are more plausible than others, but none can be predicted with high certainty. Military planning and capability development must account for this uncertainty.

The widespread conviction that the nation is headed toward a more anarchic global nuclear environment derives from the following two hypotheses. First, proliferation is inevitable—and "history proves it." This way of thinking results from the steady addition of new nuclear-armed states over the last few decades, as represented in Figure 3-1.

The second hypothesis is that global nuclear order now stands at a tipping point, to be followed shortly by a cascade of new nuclear proliferation. The argument runs as follows.

- The nuclear tests by India and Pakistan in 1998 signaled the renewal of nuclear competition among states of long-standing proliferation concern.

Figure 3-1. New Nuclear Weapon States, by Year

- North Korea's nuclear test in 2006 has reignited debates in Japan and South Korea, which will lead inevitably to their acquisition of nuclear weapons, with Taiwan certain to follow suit at some later time.
- Iran's progress toward nuclear weapons is triggering renewed interest among its neighbors in nuclear weapons and nuclear energy. Egypt, Turkey, and Saudi Arabia will have to follow suit; the latter may seek an extended nuclear guarantee from Pakistan rather than develop its own weapons (as suggested by the dotted line connectors in Figure 3-2). These choices will generate second-order effects among other states in the region, including possibly the rekindling of nuclear weapons ambitions in Iraq and Libya.
- There will be spillover effects from Northeast and Southwest Asia into neighboring regions and more generally. Brazil will follow Japan's nuclearization to signal its role as a major power, and others in Latin America will be compelled to follow. Nuclear competition in the Middle East will reignite the nuclear ambitions of Ukraine and Kazakhstan, among others. Ultimately, the threat to Europe will become so severe as to re-open debates there about independent nuclear deterrents.
- Further, the growth in the number of nuclear-armed states will be accompanied by a growth in the potential for non-state actors to acquire nuclear weapons or weapons-usable materials.

By this logic, as many as 20 or 30 new nuclear-armed states would exist in a decade or two, as represented in Figure 3-2.

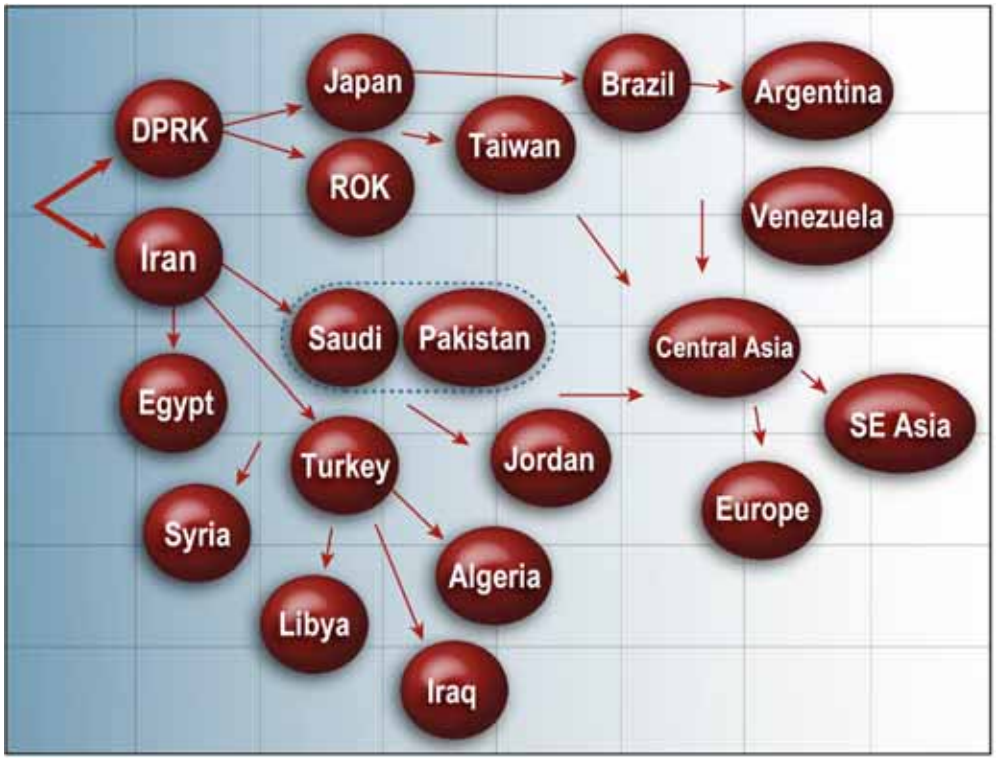


Figure 3-2. A Potential Nuclear Proliferation Cascade

What implications follow from these hypotheses? One is simply to throw in the towel on proliferation prevention. If it is inevitable, goes the argument, accept it as inevitable, don't misuse scarce political and fiscal capital for nonproliferation, and get on with needed military and other preparations. The other implication is to prepare militarily for the worst of all possible worlds. "Hunker down," by aggressively building a military posture that insulates America from an anarchic world while also creating new capabilities to dole out occasional punishment to nuclear-arming enemies.

These two hypotheses fit well with the tendency in the military planning community towards focusing on the worst-case. But that does not make them valid. From our perspective, there are obvious reasons to quarrel with each. It is difficult to square the prediction of inevitability with the fact that the number of nuclear-armed states is lower than it was when the Cold War ended roughly two

decades ago (Pakistan and North Korea have been added to the list of nuclear-armed states whereas Ukraine, Belarus, Kazakhstan, and South Africa have all abandoned nuclear weapons). It is difficult to square the prediction of an imminent cascade with the fact that acquiring nuclear weapons capabilities is time-consuming and difficult—sufficiently so that many states that have sought nuclear weapons have opted not to go the distance.

Accordingly, this study sought an alternative way of thinking about the future of nuclear proliferation. We, too, began with an assumption: that historical experience can inform an understanding of future possibilities. Indeed, we have projected some alternative futures as an extension of trend lines from historical experience, seeking combinations of trends that seem to span the plausible problem space. To understand historical experience for this purpose, the experience of proliferators, actual and potential, in creating technical capabilities associated with nuclear weapons production was mapped. This effort does not encompass every step in the evolution of their nuclear ambitions, plans, programs, capabilities, or strategies. Rather, it focuses on only those key steps that had a substantial impact on the development of the potential for weapons production, whether by increasing that potential or holding it steady or even decreasing it. The main gradients in capability are defined as follows:

- **Nil weapons potential**. Countries within this category do only limited nuclear research. They have no other access to fissile materials. Their domestic base for science and engineering is constrained by developmental factors, and they have accepted safeguards obligations.
- **Modest weapons potential**. Countries within this category have a substantial nuclear power industry. They also have a latent capability for weapons design and engineering in their national science and technology base. They have also accepted safeguards obligations.
- **High weapons potential**. Countries within this category have brought together some but not all of what they need for serial weapons production. Either they have a uranium enrichment capability or a robust scientific and engineering capability for weapons design and production. In addition, they have not fully implemented the Additional Protocol to the Nuclear Non-Proliferation Treaty, which provides for a high level of safeguards protection against illicit diversion of weapons materials and technologies.
- **Potential for serial production**. Countries within this category possess all three of the attributes: a fuel cycle allowing them direct access to fissile materials, the scientific research and engineering capacity to competitively

design and develop nuclear weapons, and rejection of the restrictions of the Nuclear Non-Proliferation Treaty and the safeguards system.

Figure 3-3 re-tells the story of the four nonproliferation failures of recent decades. It depicts the steady growth in weapons production capability. To illustrate the methodology, take the case of North Korea (yellow line):

- **1965**. First research reactor went critical. In subsequent years North Korea gained a working knowledge with key technologies and processes.
- **1987**. Weapons potential significantly increased as the Yongbyon reactor went on-line. In subsequent years, North Korea accumulated spent fuel rods, which it then removed for reprocessing as it also constructed the reprocessing plant.
- **1995**. Potential again significantly increased when (as alleged) North Korea began its secret uranium enrichment program and in subsequent years enriched uranium while further developing the plutonium pathway.
- **2006**. Nuclear test signaled production of a functioning device.

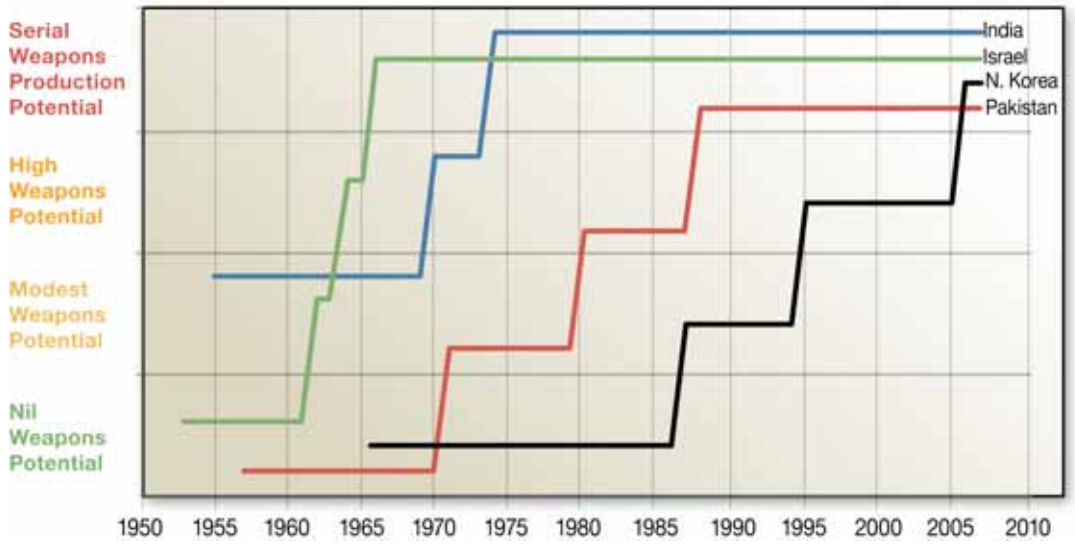


Figure 3-3. Four Nonproliferation Failures

There were many other developments in North Korea's nuclear program, strategy, and ambitions. But these few steps highlight the pathway from an original ambition to the potential for serial production.[1]

In contrast, Figure 3-4 tells the story of four rollback successes. One country, South Africa, moved steadily up and then down the capabilities ladder. Three others acquired nuclear weapons as the Soviet Union dissolved and they too chose to abandon those weapons as well as some of the associated capabilities.

Figure 3-5 illustrates the proliferation dynamics that unfold within regions, in this case Asia. One or two states might well lead a region that otherwise had not suffered proliferation to proliferate far more widely. On the other hand, one or two states might well lead a region that had suffered no proliferation to remain that way despite new pressures. Note that this figure does not include China, as the major nuclear powers are a not a focus of this work.

On a global scale, Figure 3-6 displays the complex, messy story of nuclear proliferation history. It drives home a simple point: that history is much more complex and rich than the simple linear progression that informs the proposition that proliferation is inevitable.

Two other figures (Figures 3-7 and 3-8) illuminate the fact that twice before in nuclear history the world has faced the possibility of a significant cascade of nuclear proliferation, first in the 1960s and then again in the 1970s/1980s. The first potential wave attenuated with the conclusion and entry into force of the Nuclear Non-Proliferation Treaty, as many states with nuclear ambitions set them aside in favor of security guarantees extended by the United States, latent capabilities, and reliance on the nonproliferation norm. The second potential wave attenuated more slowly but culminated in nuclear rollback by the four states in the early 1990s, as noted above.

1. Detailed support for each of the steps up or down the timelines in this work is available in Alexis Blanc, *Nuclear Proliferation: An Historical Overview* (Alexandria, Va.: Institute for Defense Analyses, 2007).

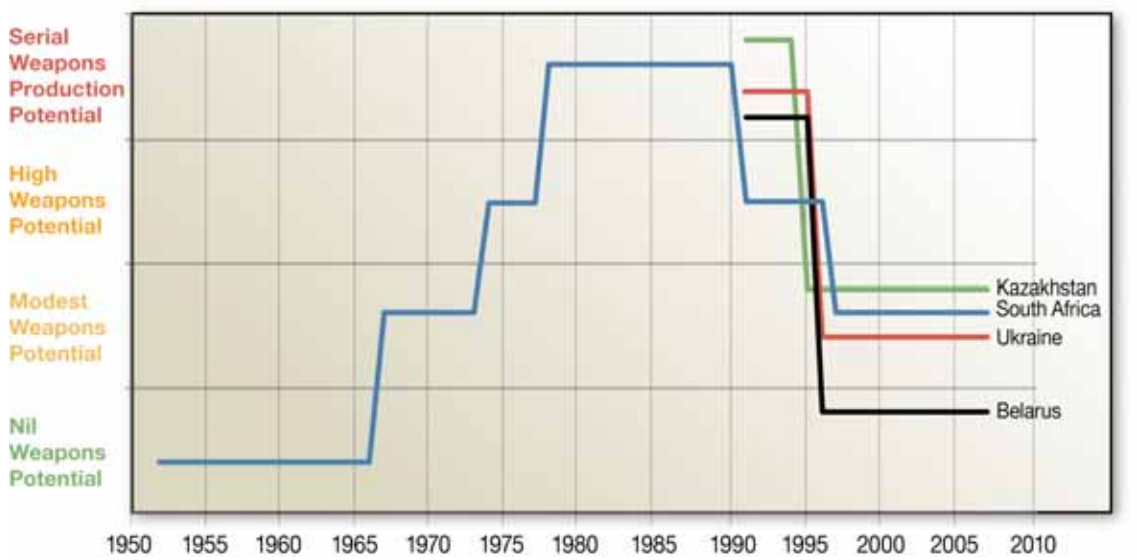


Figure 3-4. Four Rollback Successes

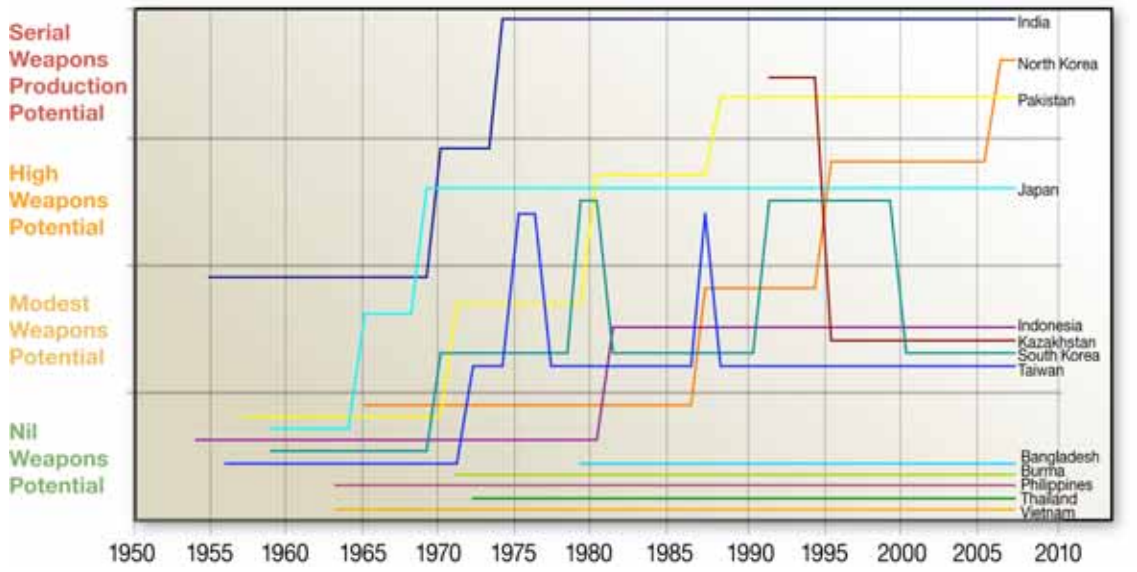


Figure 3-5. The History of Nuclear Proliferation in Asia

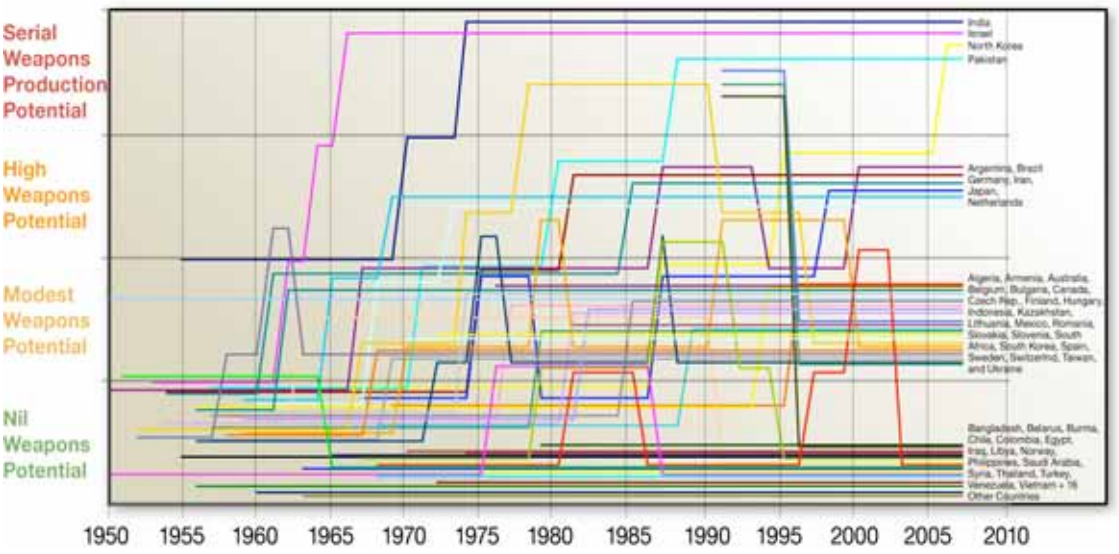


Figure 3-6. Nuclear Proliferation History in All its Complexity

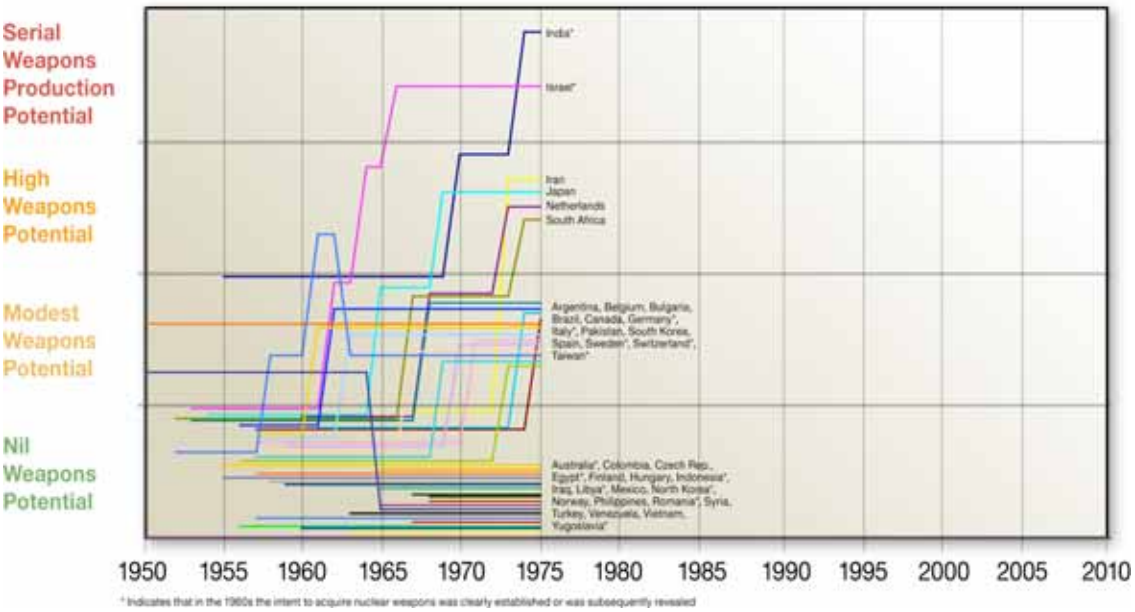


Figure 3-7. The First Potential Proliferation Cascade: 1960s

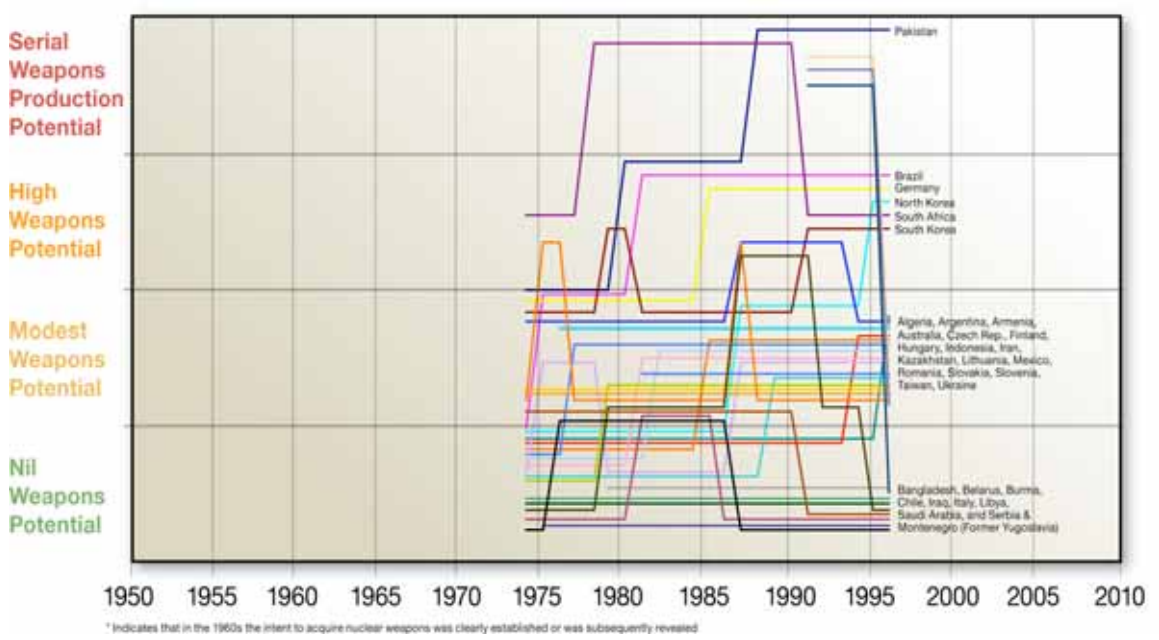


Figure 3-8. The Second Potential Cascade: 1970/80s

What insights follow from this survey of historical proliferation experience?

First, this survey reinforces the assessment that proliferation is not inevitable. The states that have acquired nuclear weapons are a small fraction of those who set out to do so. It has been possible to roll back some proliferators. Others have opted to hold steady with a level of capability short of weapons production. The historical peak of nuclear seekers was 20. In the period since the 1960s, the ratio of prevention wins to losses is 18 to 5.

Second, there have been at least two potential cascades in nuclear history. These erupted as waves, driven by a mix of primary drivers and secondary reactions. The world appears to be at a third potential tipping point. But success in diminishing the proliferation pressures of prior potential cascades suggests that the collapse of international nuclear order may not be inevitable or imminent.

Third, the decision points along any single country's nuclear "pathway" are numerous. Our research identified more than 300 major decisions by over 50 states in this time period. These are opportunities for influence. How best to use the current opportunities is the subject of a later chapter.

Fourth, proliferation typically takes a long time. Although some states have sought shortcuts to nuclear weapons, all have had to develop some degree of indigenous capability, usually substantial. This proved time-consuming and technically difficult. The challenges of indigenous development of fissile material are well illustrated in Table 3-1. It is also important to note that the most likely countries to seek nuclear weapons in the next 20 years are developing countries, many of which have not developed the kind of scientific, research, and engineering infrastructures that will allow them to rapidly accumulate capabilities indigenously.

Similarly extended timelines are also typical on the development and engineering side. Weapons design, with or without foreign help, typically takes less time than production of fissile material. But production of the designs and their subsequent weaponization has typically required approximately 15 years.

This way of thinking about the nuclear past suggests that hyper-proliferation anarchy in the 20-year future is less likely than some in the defense community believe. Indeed, in this study it led to a different set of conjectures. Almost anything is possible in a 20-year timeframe, but not everything is equally likely. North Korea's acquisition of nuclear weapons is unlikely to readily lead to a broader proliferation of nuclear weapons in East Asia. Those proliferation risks are long-standing, and states there have made a series of choices to manage those risks with some reliance on U.S. security guarantees and some reliance on latent weapons potential. Iran's nuclear acquisition may have more immediate and far-reaching consequences for the Middle East. Its neighbors may renew their quests for nuclear deterrents of their own, but unless shortcuts are available to them, the development of a viable nuclear weapons production infrastructure is decades away for them. Moreover, allies and friends of the United States in that region may see U.S. guarantees as a preferable option for meeting the challenges of a proliferating Middle East than trying to develop nuclear weapons of their own, competitively and in increasing isolation.

Other regions of the world seem unlikely to fall into renewed nuclear competition unless there is a substantial breakdown of the nonproliferation regime and other institutions of international security. In the 20-year timeframe, a doubling of the number of nuclear-armed states from today's total of nine would require that some countries with advanced infrastructures in Europe and East Asia opt for nuclear weapons, which seems highly unlikely in this timeframe.

Table 3-1. Timelines to Fissile Material Production

Technology	# of Countries Interested in Technology	# of Countries with Successful Production Programs*	Average Time to Pilot Plant** (in years)	Average Time to Production*** (in years)
Gaseous Diffusion enrichment	6	5	-	6
Centrifuge enrichment	18	7	8	14
Electromagnetic isotope separation	11	1	2	3
Chemical isotope separation	3	-	6	11
Aerodynamic isotope separation	3	1	7	18
Laser enrichment	14	-	-	-
Graphite–moderated production reactor	6	6	1	2-11
Heavy-water moderated reactors	12	5	1	2-6
Research Reactor	14	3	-	4-5
Reprocessing	19	13	6	10

Source: Pacific Northwest National Laboratories, *Nuclear Proliferation Technology Trend Analysis*, September 2005.
Qualifiers: * more than gram quantities of material produced
** technological capability demonstrated
*** significant quantities of material produced

To be sure, there is the ever-present possibility of shortcuts. In an era marked by rising concern about networks like that of A.Q. Khan and evidence of North Korean "off-shore" nuclear activities, it would seem that those possibilities are multiplying. But historically, few of the states seeking shortcuts have found them (or found them trustworthy). Moreover, states seeking to develop indigenous capabilities with selective use of shortcuts have had to make numerous decisions along the way about what level of capability to create, and these decision points have been targets of opportunity for influence.

How might the trends from the past combine and re-combine to create new patterns in the future?

Looking ahead to 2027, this study has defined two theoretically possible but not realistically plausible "outcomes." One would be a world in which all of the states with serial weapons production capabilities abandon their nuclear weapons and drop below the cross-over point from weapons potential to weapons production, as depicted on the time-line charts. This world would be one of nuclear disarmament and, in the view of this study, it is not possible between now and 2027. But this view does not rule out the possibility that one or more nuclear weapon states might roll back their capabilities.

The other notionally possible but not plausible future is hyper-proliferation. In this world all of the states with weapons potential, even if presently nil or, indeed, non-existent, accelerate their climb up the capabilities curve and cross the red line from weapons potential to weapons production.

Four alternative "outcomes" are more plausible in this two-decade timeframe, as described in Figure 3-9:

Alternative Future 1. Under this alternative, no new states have crossed the line to weapons production, but more states have latent weapons potential, and those states with weapons potential are developing increasingly robust breakout capabilities. Any rollback successes would likely fall into this category as well. There would be growing risks associated with the acceleration of technology diffusion and the larger and more diverse market in materials, technologies, and expertise. Non-state and sub-state actors could find more opportunities to advance their interests in such a world. States seeking shortcuts on the developmental pathway might also find increasing opportunities here. This alternative is referred to as "more latency."

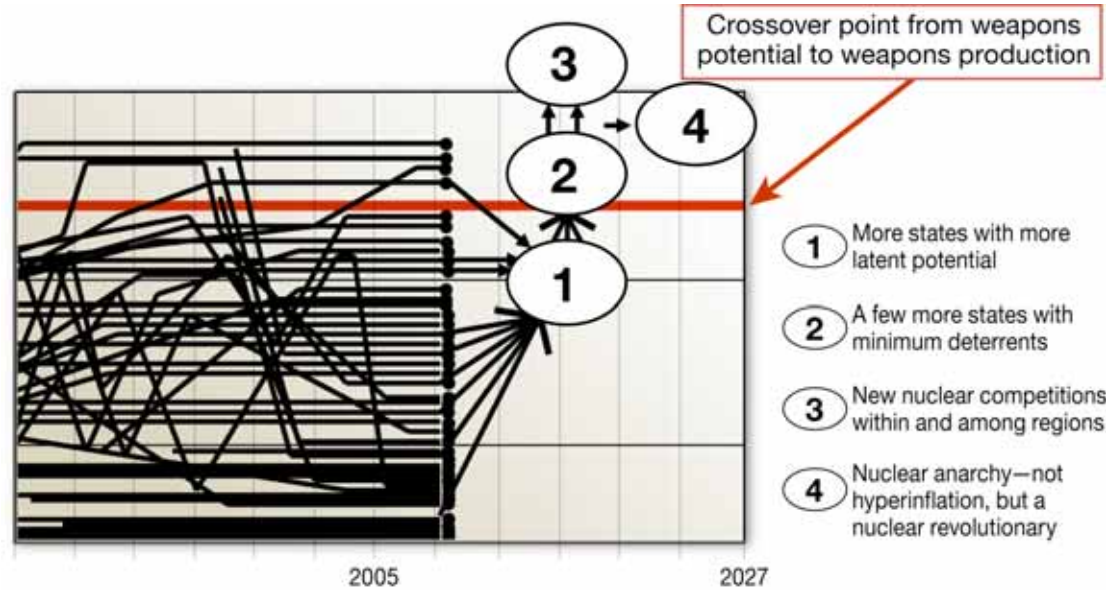


Figure 3-9. Alternative Nuclear Futures

Alternative Future 2. Alternative two would include all the challenges noted in alternative 1. In addition, a small number of states would have crossed the line into weapons production. But the defining feature of this world would be that those states are motivated primarily by a desire to possess a minimum deterrent that they safeguard for defensive purposes. This alternative is referred to as "more minimum deterrents."

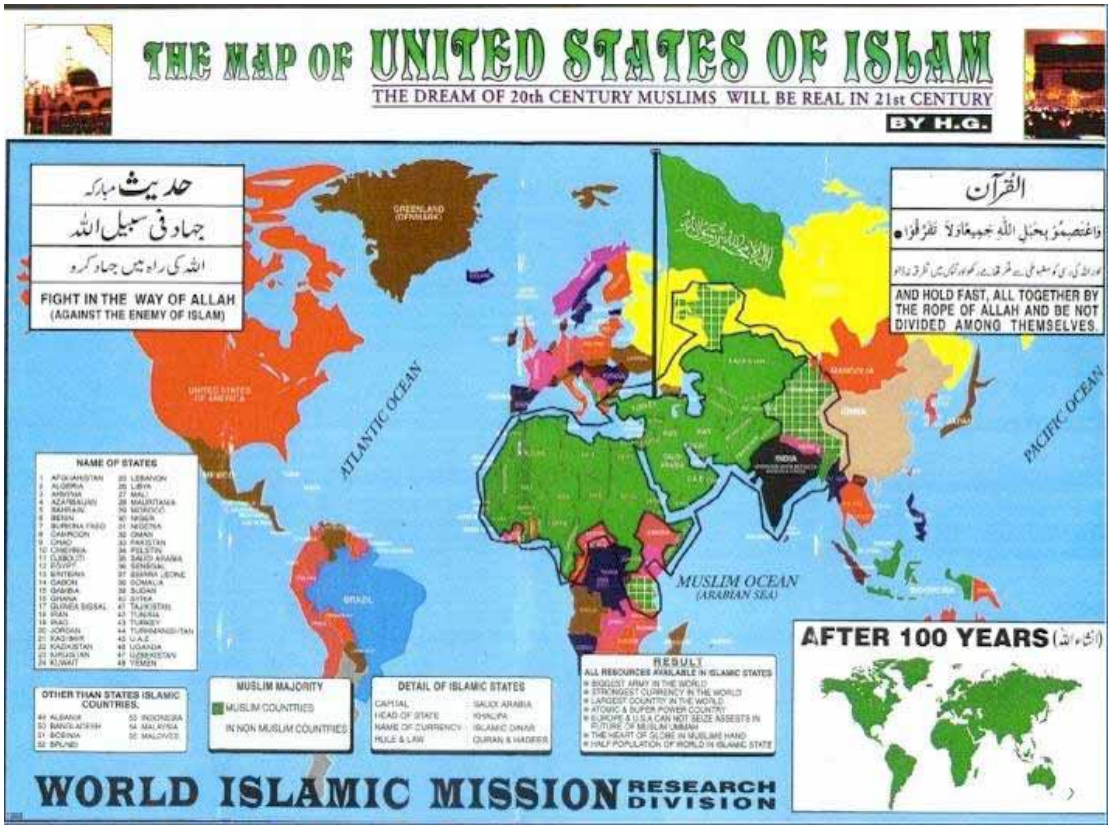
Alternative Future 3. In addition, to the challenges of the first two alternatives, this future would include some number of states that are competing for nuclear advantage. That competition might occur between neighbors and within specific regions. It might spill over across regions, particularly as long-range delivery systems are deployed. It might also include competition directly with the United States. It is possible to imagine various forms of competition: for supremacy, for parity, to seize opportunities before a nuclear counter-balancer emerges, to extend deterrence to counter U.S. regional influence, or to ensure effective retaliatory capabilities in light of improvements in an adversary's ability to strike first (and absorb a counter-strike with missile defenses). It is possible to conceive of new nuclear competitors as seeking to develop capabilities up to (and beyond) certain specific thresholds. These thresholds are defined as follows:

- First operational weapon: signals a state's emergence as a nuclear power.
- Minimum defensive capability: the level sufficient to expect one weapon to survive to a high-value target (this threshold would be much higher against countries with preemptive and defensive capabilities).
- Minimum offensive capability: above plus enough in reserve to induce retaliation restraint by the attacked party (proliferator may believe that it could win a limited war for limited stakes with such a force).
- Existential threat: above plus enough to pose an existential threat to its enemy (threshold a function of size and capabilities of enemy). If numbers sufficient, may be willing to hand some off to others.
- Parity in numbers: above plus numbers comparable to enemy (threshold again a function of enemy—very high if United States or Russia).
- Numerical and/or technical superiority: of limited additional operational value to proliferator so long as enemy poses existential threat.

This alternative future is called "new nuclear competitions."

Alternative Future 4. This alternative "outcome" could erupt out of any of the three futures described above. In this future, a new revolutionary power emerges that is willing to employ and share nuclear weapons in service of its cause. The quintessential expression of this problem would be the emergence of a nuclear-armed Caliphate guided by the philosophy of Osama bin Laden and fellow revolutionaries. In this scenario, the Caliphate is suddenly restored over the holy sites in Arabia, a nuclear umbrella is unfurled, and the new entity expands its attacks against its near and far enemies, but this time with nuclear weapons, whether held in reserve or actually employed. It is also possible that some radical regimes might seek to affiliate themselves with a radical nuclear-armed Caliphate and pursue a form of coalition warfare against their near and far enemies under a larger nuclear umbrella. This vision is cogently conveyed in Figure 3-10, from a radical Islamist website.

One of the text boxes in Figure 3-10 describes the military attributes of a "United States of Islam" in 2030, including the "strongest army in the world, strongest currency in the world, largest country in the world, and atomic and superpower country." Note that the lower right-hand box in this figure depicts a vision of the world 100 years from now, in which the total world population has been subsumed into a single Islamic "state."



Source: http://strangemaps.wordpress.com/2007/11/01/194-the-united-states-of-islam/

Figure 3-10. An Illustration of the Potential for a Revolutionary Nuclear-Armed "Peer"

This fourth alternative future is referred to as "nuclear anarchy." The members of this study believe that this alternative future has not so far captured the attention of U.S. defense planners but that it should be a central focus of policy development. The possible sudden emergence of a nuclear-armed state committed to revolutionary purposes and drawing on the sympathies of large numbers of anti-American and anti-Western peoples could well bring the return of the kind of peer adversarial competition that has not had to concern the United States for the last two decades.

The purpose of elaborating these alternative futures is not to predict a specific proliferation outcome in 2027. Rather, it is to define a spectrum of plausible outcomes so that it is possible to explore what military capabilities will be needed. Before turning to that specific question, we offer observations on how the proliferation problem will intersect with the non-state and major power nuclear problems.

It is difficult to conceive of a plausible proliferation outcome in 2027 that does not involve an intensification of the challenges associated with non-state actors seeking access to nuclear weapons, materials, technologies, and expertise. Those actors will encounter a larger and more diverse network of suppliers, which will probably afford them new opportunities to divert, steal, or bribe their way to desired capabilities. They may also find common cause with radical regimes that are willing to use them as conduits for unconventional employment of nuclear weapons.

With regard to the connection between proliferation and major power nuclear relations, it seems likely that the United States will want to focus strategic resources on proliferation and not on Russia or China if it is not absolutely necessary to do so. But proliferation will drive changes in the strategic military postures of all three, and that will make this difficult. Managing the potential instabilities in the strategic offense/defense relationships of the three will be a central challenge of sustaining global nuclear order in an era of heightened proliferation risk. Just because something can be unstable does not mean that it necessarily will be. Maybe the nation will get lucky or, better yet, find the necessary wisdom and will.

Proliferation's Implications

What implications will proliferation have for the United States? What will U.S. leaders want to do in response, and to shape the security environment? Without answers to these questions, it is impossible to know what military operational challenges might confront the United States in these alternative futures.

The possible implications of proliferation over the next two decades can be expressed as follows. Further nuclear proliferation could:

- Raise the costs to the United States and its allies and friends of U.S. intervention on their behalf, reducing its freedom of maneuver and intensifying political debate about what burdens it should bear.
- Expose the United States and its allies and friends to attempted coercion by new nuclear states and/or coalitions of states.
- Expose all states to the risks associated with access by non-state actors to weapons, materials, technologies, and expertise—not least through direct transfer from states.

- Expose all states to the possibility for more rapid breakout through sharing arrangements among states.
- Generate new demands for U.S. security guarantees.
- Generate new concerns about the nuclear vulnerability of the homeland.
- Bring to a head the growing debate about the competence of the United States to understand and safeguard the interests of its allies and friends around the world.
- Bring a loss of U.S. credibility whenever a U.S. ally or friend goes nuclear. A collapse of the nuclear nonproliferation regime would deal a particular blow to U.S. credibility, as this was a particularly American project.
- Expose all states to the risks of economic, environmental, social, and political impacts of regional nuclear wars.
- Create new demands on international security institutions to sustain the peace, redress noncompliance with international treaty commitments, punish nuclear aggressors, and intervene to try to stop regional nuclear wars.

In fact, most of these costs and risks seem to be a function not just of the proliferation threat, but also what is done about it. It is possible to reduce those costs and risks in various ways—and in a cumulative way—that can make a substantial difference—a point that will be discussed in the following chapter.

Another way to explore the possible implications of proliferation is to explore how U.S. leaders will want to act to confront proliferation challenges and shape the security environment. It is useful to distinguish between what U.S. leaders will want to do, won't want to do, and may have to do.

U.S. leaders will want to contain and deter nuclear aggressors, counter their attempts at nuclear-backed coercion, and punish those who act aggressively with nuclear weapons. They will want to assure friends and allies that they need not meet the new proliferation challenges with their own nuclear weapons and to also dissuade potential adversaries from seeking to compete with the United States by nuclear means. They will want to secure loose nuclear weapons in weak states and to suppress illicit nuclear networks of all kinds. They will want to buy more time vis-à-vis the next proliferators and to use it to good effect. They will also want to manage major power relations in a way that keeps Russia, China,

and others aligned with the United States in meeting the challenges of a more proliferated world.

U.S. leaders will not want to appease proliferators or acquiesce to the actions of a revolutionary Caliphate to attempt to unseat "apostate regimes." They will not want to stand by idly while allies distance themselves from the United States because of the perception that it might be unreliable in a nuclear crisis. They will not want to be constrained in their exercise of U.S. power and influence. And they will not want to pay a high economic or political price to inhibit further proliferation.

Despite these preferences, U.S. leaders may have to do some of the following. They may have to act rapidly as a nuclear-armed state collapses to secure its arsenal and stockpiles of fissile material. They may have to conduct a preventive war if revolutionary forces appear poised to gain control of a nuclear-armed state. They may have to defeat nuclear-armed enemies on battlefields where it is believed that nuclear weapons can be used locally without risking strategic retaliation (something U.S. leaders would likely prefer to do by non-nuclear means, if possible). They may have to try to boost the willingness and ability of new nuclear states to maintain their nuclear capabilities according to high safety and security standards. They may have to provide technical assistance to them toward that end—or facilitate/condone such action by others. They may have to acquiesce to extended deterrence roles in the Middle East and perhaps elsewhere by other states. They may even have to accommodate some of the demands of proliferators.

What military capabilities are needed to underwrite these intentions? This topic will be addressed in the following chapter.

Chapter 11. Needed Military Capabilities in a More Proliferated World

The four alternative futures described in the previous chapter were used in this study to define what military capabilities will be needed in a more proliferated world. For each alternative, two contingencies were elaborated in detail—with a characterization of U.S. interests and objectives, top-level concepts of operations, and needed capabilities and capacities (a distinction elaborated in the 2006 Quadrennial Defense Review [QDR]). One contingency focused on crisis response and the other on shaping the security environment. The complete list follows:

- **Alternative Future #1**, marked by more latency:
  - Crisis contingency: suppress a newly discovered illicit proliferation pathway.
  - Shaping contingency: inhibit nuclear defections by non-nuclear states, principally from among U.S. allies and friends but also more generally.
- **Alternative Future #2**, marked by the emergence of more minimum deterrents:
  - Crisis contingency: secure an arsenal of weapons and materials in a failing state.
  - Shaping contingency: dissuade development of more potent capabilities by those who have crossed the minimum deterrent threshold.
- **Alternative Future #3**, marked by the eruption of new forms of nuclear competition within and among the regions and also with the United States:
  - Crisis contingency: conduct stabilization and reconstruction as a part of terminating a regional nuclear war to which the United States was not a direct party.
  - Shaping contingency: extend nuclear deterrence to new security partners in regions of rising proliferation concern.

- **Alternative Future #4**, marked by the emergence of a revolutionary nuclear power or powers and near anarchy:
  - Crisis contingency: neutralize an expansive revolutionary state armed with nuclear weapons.
  - Contingency: contain a coalition of states hostile to the United States and protected by the nuclear umbrella of a revolutionary state.

The selection of contingencies is meant to be illustrative, not exhaustive. Other crises are imaginable and it is conceivable that some of the crises associated with a particular future might also occur in a different future. "Shaping" will remain an imperative in each future, whatever specific form it might take. The objective of this modest effort in capabilities-based planning was to span the problem space so as to characterize broadly and comprehensively the capabilities that will be needed.

For each contingency, the specified Blue concept of operation was used as a basis for deriving a list of needed capabilities and capacities.[2] Some were unique to a specific contingency but most cut across many contingencies. These are catalogued and summarized as follows.

Needed Military Capabilities

The United States needs three basic types of capabilities.

- **First, it needs a joint force** able to execute the missions associated with combating nuclear proliferation (as specified in the *National Military Strategy to Combat Weapons of Mass Destruction*).[3]
- **Second, it needs a strategic posture able to meet the demands of assurance, dissuasion, deterrence, and defeat** (including explicitly extended deterrence, all as elaborated in the *2002 Nuclear Posture Review*).[4]

---

2 Details of the eight contingencies are contained in Appendix III-A.

3. *National Military Strategy to Combat Weapons of Mass Destruction*, Chairman of the Joint Chiefs of Staff, Washington, D.C., February 13, 2006.

4. *Nuclear Posture Review Report*, U.S. Department of Defense, January 9, 2002, (submitted t Congress December 31, 2001) classified report.

- **Third, it needs a capacity to integrate all of the tools of national power** in support of peacetime and war-time objectives. Each of these is described briefly below, followed by a more detailed discussion.

Joint Force Capability: Interdiction

In most of the contingencies, high value was attached to the ability to effectively locate and either seize or destroy nuclear materials and weapons in transit. Generally, this was important to dissuade and deter further nuclear proliferation involving both states and non-states, especially in the shaping contingencies. In particular, the contingencies demonstrated specific needs for interdiction to disrupt smuggling routes globally, halt the flight of nuclear weapons from a failed or defeated state, and stop nuclear weapons in the approaches to the U.S. homeland.

Joint Force Capability: Elimination

The contingencies also demonstrated the need for nuclear elimination capabilities to find, secure, and render safe nuclear weapons and/or materials and/or the programs that produced them. These capabilities include site control, exploitation, disablement, dismantlement, and material disposition against both state and non-states. In the first alternative future of "more latency," this capability is primarily aimed at dissuading nuclear defections or other proliferation by demonstrating U.S. capability to eliminate nuclear weapons and materials when necessary. In addition to this shaping function, the capability also serves specific purposes in other alternative futures. Each of the crisis contingencies for the other alternative futures (capturing "loose nukes" from a failing state, intervening in a regional nuclear war, and reacting to nuclear aggression by a revolutionary power) require responsive and robust nuclear elimination capabilities.

Joint Force Capability: Passive Defense

In two of the contingencies crafted for this study, U.S. military forces were compelled to operate in regional environments contaminated with radioactive material. One contingency was associated with efforts to terminate a regional nuclear war and to participate in the stabilization and reconstruction efforts to follow. This effort could well involve operations in areas contaminated by nuclear attack prior to the arrival of U.S. forces. The other contingency involved the potential for direct attack on U.S. forces by a revolutionary state willing to

employ nuclear weapons and calculating that it could use nuclear weapons in ways that would fall beneath the U.S. retaliatory threshold. Such a case could involve military operations against an enemy trying to use nuclear weapons to cripple single points of failure in a U.S. war plan or to cripple U.S. morale—or the political will of its regional allies. Passive defenses are also relevant to the shaping contingencies in the sense that they convey a capability and willingness to operate effectively in nuclear environments and to surge protection of allies. Accordingly, the joint force must be capable of sustaining stabilization operations in a nuclear contaminated theater and sustaining battlefield operations under very limited attack. To do so requires passive defense effective against nuclear effects.

Joint Force Capabilities for Consequence Management

The circumstances that could lead U.S. forces to need to operate in a contaminated environment also create a need for those forces to be able to help allies, friends, and others subjected to nuclear attack prepare for and cope with those attacks. The associated humanitarian problem could be of daunting proportions. This study focused on foreign consequence management and did not address the separate, but related, and important issues associated with domestic consequence management.

Joint Force Capability: Attribution

The ability to quickly, accurately, and credibly identify and attribute responsibility for an unclaimed nuclear explosion is critical for the types of nuclear futures envisioned in this study. Such an explosion might take place on the high seas, on the territory of a friend or ally, or on U.S. territory. It might take place with no warning on a slow day, in the heat of an escalating crisis with U.S. government agencies already on high alert, or during an on-going war. In all circumstances, it is imperative that the president quickly have the facts at hand in order to select courses of action, to reassure the American public, and to engage diplomatically with allies and partners.

"Quickly," in this study is defined as 24 to 48 hours—a difficult stretch goal. It is highly likely that the president would also want to take a technical case to the United Nations Security Council within a few days. The linchpin is to be able to attribute responsibility. Presumably, the intelligence community would have ready for the president all relevant evidence from U.S. and partner sources. The point of origin may be easy to trace quickly, *e.g.,* a nuclear weapon delivered by a ballistic

missile on a known trajectory. But the focus here is on the unclaimed nuclear explosion for which there is scant intelligence other than that to be acquired from nuclear forensics. The focus thus is twofold: the ability of the U.S. forensics community to provide the president with the needed information, and the ability of corroborating international evidence to lend credibility to U.S. claims.

Joint Force Capability: Intelligence

In all of the alternative futures examined in this study, the demands for high-quality nuclear intelligence would be high. Both the *National Strategy to Combat WMD* and the *National Military Strategy to Combat WMD* rightly describe intelligence as a critical enabler of effective implementation. Indeed, comprehensive, technically accurate, in-depth intelligence on foreign nuclear weapons programs and activities is essential to mission success across the entire combating WMD mission space.

Strategic Posture Capability: Non-Nuclear Strike

The crisis contingencies illustrate the need to be able to destroy nuclear weapons being readied for use in a regional nuclear conflict, being transferred to a proxy actor, or being deployed as a breakout capability by a new revolutionary regime. The shaping contingencies also illustrated the value of being able to do these things in terms of influencing the decisions of others to accept U.S. protection as opposed to creating their own strategic strike capabilities.

Strategic Posture Capability: Active Defenses

Both the crisis and shaping contingencies illuminate the value of being able to protect the United States, its military forces, and its allies and friends from attack with nuclear-tipped ballistic and cruise missiles. Being seen as able to negate the value of threats from nuclear missile-armed states should be very helpful in inducing their restraint in confrontation with the United States and/or a U.S. ally.

Strategic Posture Capability: C4ISR

The contingencies all illustrate the value of a reasonably complete and up-to-date intelligence picture of foreign nuclear weapons activities; command, control, communication, and computer capabilities to coordinate complex high-speed operations; and surveillance and reconnaissance capabilities to find and track nuclear weapons and materials originating from known or likely related sites. They also suggest the value of effective information assurance.

Strategic Posture Capability: Nuclear Deterrence

The proliferation contingencies elaborate various values for the U.S. nuclear force in both crisis response and shaping. In the crisis contingencies, the U.S. nuclear force is important when persuading new nuclear competitors not to threaten or conduct attacks on the United States, its allies and friends, and its military forces. Think of this as central deterrence and extended deterrence. In the shaping contingencies, the U.S. nuclear force is important to persuade challengers that they cannot gain strategic equivalency (dissuasion), to assure allies that they need not abandon the security relationship with the United States and seek nuclear deterrents of their own (assurance), and to contain a hostile coalition through the threat of punishment. The shaping contingencies also illustrate ways in which responsible U.S. stewardship of the nuclear enterprise sets a standard for surety (security and safety) to which others should be held. In short, the contingencies illustrate various ways the United States can strategically apply its nuclear weapons enterprise (nuclear forces and supporting infrastructure) to influence the nuclear proliferation environment worldwide for the greatest net benefit to U.S. and global security. Four priorities stand out:

First, the United States needs a nuclear force that its allies, friends, enemies, and potential adversaries see as viable for purposes of deterrence, both central and extended. A credible deterrent is essential for persuading U.S. allies and friends that they need not translate their weapons potential into an independent nuclear force. It is essential also for persuading enemies and potential adversaries that there would be no net gain in their security or prestige through the acquisition of nuclear weapons because they could not hope to prevail in a crisis or war in which they threaten or employ nuclear weapons.

Second, the U.S. nuclear weapons enterprise must perform nuclear surety (safety and security) at the highest possible level. After all, in a more proliferated world the United States will want to hold all states, including especially the new ones, to these highest possible standards. To do that, it must set that best practices standard. Its own best practices are a function of assumptions about the threat and human performance factors and of cost.

Third, the nuclear weapons enterprise must be able to responsively field nuclear forces under changing conditions. The absence of such a capability works against the objectives of dissuading potential competitors and assuring allies and friends seeking viable extended deterrence. A responsive infrastructure also enables the United States to reduce reliance on a large stockpile of warheads as a reserve force and to reduce the need for testing weapons as part of the long-

term stewardship effort, which help to reinforce the responsible stewardship objective noted above.

Fourth, the enterprise must be (and be seen to be) well aligned with U.S. international treaty commitments, especially to the Nuclear Non-Proliferation Treaty. The contingencies illuminate the various ways in which the United States can employ the treaty commitments of others, international norms, and international processes to isolate and pressure problem states, and to assure and encourage those states that prefer non-nuclear futures. Accordingly, the United States must not be seen as disdainful of its own treaty commitments, including those to Article VI of the Nuclear Non-Proliferation Treaty.

Strategic Posture Capacity: Flexible Infrastructure

The contingencies associated with dissuasion and containment point to the value of being able to rapidly produce new strategic capabilities in response to geopolitical change, technology surprise, and new mission requirements. The nuclear element has already been discussed above.

National Capacity: Integration

The DIME (diplomatic, information, military, and economic) construct is intended to bring home a larger point to the defense community: diplomatic, informational, military, and economic tools of national power must be integrated to support national objectives in the security environment. This concept is as true in dealing with the proliferation challenges of the future as with other problems in that environment. The contingencies vividly illustrate the need for such integration. All of the shaping contingencies illuminate the ways in which U.S. objectives cannot be achieved by relying on military means alone and, similarly, the numerous contributions of the U.S. military to efforts for which other governmental entities have the lead. Even in the crisis contingencies, the successful implementation of Blue concepts of operation typically requires the effective integration of a broad range of interagency partners. Without such integration, the military will be called upon to do things that it is ill-equipped to do alone, such as stabilization and reconstruction after a regional nuclear war. Such integration is also essential for all of the Phase Zero activities associated with proliferation prevention, assurance, and extended deterrence.

These needed capabilities and capacities are summarized as follows:

The joint force must be able to perform the following missions effectively:

- **interdiction** to locate and seize nuclear materials and weapons in transit
- **elimination** to eliminate weapons captured from terrorists or collapsing or defeated states and the programs that produced them
- **passive defense** to allow sustained operations in a nuclear contaminated. environment, scaled on high-end to very limited enemy use
- **consequence management** to prepare and protect civilian populations in affected areas
- **attribution** to quickly provide a national assessment to the president following an unclaimed nuclear explosion, and an international technical assessment to UN Security Council shortly thereafter
- **intelligence** as an enabler to provide timely access by the president, Secretary of Defense, and combatant commanders to comprehensive, technically informed, and actionable nuclear intelligence to support crisis action, network suppression, and longer-term planning

The strategic posture must be able to meet the demands of assurance, dissuasion, deterrence, and defeat with capabilities to:

- hold at risk enemy nuclear assets and other high-value targets by non-nuclear means
- defeat enemy preemptive or retaliatory strikes with active df
- and track mobile systems, coordinate complex high-speed operations, and provide prompt situational awareness
- deter nuclear attack on the U.S. homeland and extend deterrence to allies and friends that they deem credible by nuclear and other means
- demonstrate high standards of responsible nuclear ownership and advocate for international standards
- respond to geopolitical change, technological surprise, and new mission requirements with new capabilities from the existing infrastructure

A capacity to integrate the tools of national power in service of U.S. nonproliferation and counterproliferation objectives is an essential adjunct to the other military capabilities and capacities.

It is useful to think of these needed capabilities and capacities as tools in the military toolkit. Any individual contingency may call for the use of only a few of those tools. Only the most demanding would call for the use of most or all of them. If the future could be known with certainty, the United States could emphasize the development of only a subset of tools identified here. But the future is not sufficiently predictable, as previously argued. Thus, the nation must develop the broad military toolkit envisioned here if it is going to be able to do what leaders are likely to want to do or have to do in the proliferation futures envisioned.

This list of needed capabilities and capacities derives from the study's assessment of the requirements of success in military-operational contingencies in a more proliferated world. Many of these contingencies could materialize well before the outer time limit of this study: 2027. Of course, the opposite is also true: they may not materialize between now and then, or ever. National strategy and guidance already put a high value on the ability to employ military instruments proactively to confront nuclear proliferators and nuclear challengers. Most, if not all, of the needed capabilities identified above are in fact currently needed, with the stipulation that over time the needed capability is likely to become more robust.

This approach to defining needed capabilities and capacities does not address two issues: (1) the sweeping changes to the U.S. foreign base posture that might be driven by the need to contain a revolutionary, nuclear-armed Caliphate, or (2) the kinds of force structure adaptations that would be necessary to support the defense of allies and friends and the projection of power in the face of nuclear threats from a revolutionary power. These could be sweeping.

Assessing Current Capabilities

During the course of this study, the time and expertise were not available to conduct a detailed review of the status of current capabilities across this portfolio of 13 needed capabilities. But charged with the task of identifying current capability gaps, a top-level comparison was conducted of current capabilities and future needs in select areas. Overall, three propositions emerged:

First, the current capabilities of the joint force to perform the nuclear-related missions of the combating WMD strategy are not robust. Indeed, they are grossly mismatched to the needs and policy priority of proliferation prevention and management. The stand-up of a few new capabilities has been accompanied by the atrophy of some older but still needed ones.

Second, the strategic posture is in transformation but remains poorly tuned to the requirements of assurance, dissuasion, and deterrence. Overall, this force must become much more capable of providing a broader range of strategic military options than is currently available with nuclear weapons.

Third, the needed integration remains a vision but not a reality. The U.S. government has not organized and mobilized for this problem in the way that it has for the counterterrorism problem.

Current Interdiction Capabilities

Despite good progress in creating the planning and execution processes for strategic interdiction, actual capabilities remain quite modest in comparison to the anticipated threat. There are several reasons for this situation. There are currently too few trained and assigned units with specialized personnel (especially special operations forces) to effectively operate against a dispersed proliferation network or multiple networks operating simultaneously. Current training and exercises are not addressing this requirement.

In addition, current detection capabilities for locating and tracking nuclear weapons and materials do not perform at the desired level against competent adversaries. The lack of detectors that can be used from a distance and are robust against countermeasures (such as masking or shielding) represents a substantial gap in needed capabilities for nuclear interdiction.

Finally, there is no global system architecture that would allow for an accountable prioritization of activities and investments. The result is an uneven and inefficient (sometimes *ad hoc*) distribution and application of interdiction capabilities. This is particularly problematic because interdiction depends on intelligence, interagency, and international capabilities in addition to those within DOD. As a result, successful interdiction is extremely difficult, especially against an adaptive adversary who will seek to exploit weaknesses. Successful interdiction also requires actionable intelligence and there are significant gaps there as well, as discussed in further detail below.

Current Elimination Capabilities

There are only limited efforts in DOD to plan, train, equip, and exercise for nuclear elimination. Although the mission exists, its requirements (for scope, simultaneity, etc.) have not been fully defined and it is not fully resourced.

Current capabilities are scaled and tailored to past problems (*e.g.,* a replay of the war to find Iraqi weapons of mass destruction). In future conflicts, U.S. forces may have to be ready to contend with a large arsenal, operating infrastructure, and substantial nuclear risks. There seems to be only limited ability to surge for larger-scale elimination missions or simultaneous missions. These capabilities are further limited by gaps in intelligence, particularly with regard to the location and disposition of adversary nuclear facilities, weapons, and/or materials.

Current Passive Defense Capabilities

The Services once had up-to-date and well-practiced concepts of operations and tactics, techniques, and procedures for operations on a nuclear contaminated battlefield. But with the end of the Cold War, the emphasis in chemical, biological, radiological, and nuclear (CBRN) training and research and development procurement has shifted in favor of chemical and biological at the expense of radiological and nuclear. This shift is reflected in the ratio of training hours, currently running at nine hours for passive defense for chemical and biological attack for every one hour of training for passive defense for nuclear or radiological attack. Although it is intended to provide comprehensive training on all weapons of mass destruction, the U.S. Army Chemical School, which is responsible for CBRN training, has deemphasized radiological and nuclear throughout its curriculum.

One result in this training gap is that very few forces are adequately trained on radiation detection. It is important to be specific about the nature of the training deficiency: it is not that officers and noncommissioned officers do not know how to operate or keep the equipment functional; rather, they do not understand the implications of different meter readings in terms of their impact on the health of the military personnel around them. Without proper understanding, all meter readings are interpreted as dangerous, which leads to poor risk assessments, a loss of combat efficiency, wasted time and effort as individuals deal with background-level radiation issues, and units maneuvering to avoid all measurable radiation "hazards," even those that are not hazardous. The notion that "all radiation is bad" also increases the risk of individual panic.

Another important gap is in available understanding of nuclear weapons effects. The number of systems vulnerable to nuclear weapons effects is growing and the understanding of vulnerabilities is declining. With DOD's increasing dependence on technology, U.S. military forces are increasingly at risk of equipment failure due to nuclear weapons effects, especially electromagnetic

pulse. DOD can only identify such vulnerabilities on the systems it tests and it does not test many systems. The Army tests mission-critical systems but the other military services test only a small subset of equipment with the majority focused on surviving space environments. Concerns about this problem were well articulated by the EMP Commission of 2004, but interim progress in creating the needed understanding has been disappointing.

There are other gaps as well. Operational guidelines for plausible contingencies have not been written. The architecture for stand-off detection of radiation remains underdeveloped.

Current Consequence Management Capabilities

DOD appears to be singularly focused on protecting its own forces and facilities and has not yet tackled the difficult subject of how to extend its capabilities and capacities to help its allies and friends cope with attacks on them. The official roles and missions associated with foreign consequence management do not seem to be developed, nor have plans been created or exercised.

Current Attribution Capabilities

Current forensics capabilities are firmly rooted in Cold War nuclear history. In the mid-1940s, the U.S. Air Force developed an ability to conduct airborne surveillance for evidence of a foreign nuclear test. Consequent to the dual needs of U.S. nuclear war planning and the monitoring requirements for a series of arms control arrangements, the United States, through the end of the Cold War, developed an elaborate global system of sensors and an operational concept for alerting and characterizing nuclear explosions. Although much of this system remains in place today, it is not aligned to the newly relevant problems of an unclaimed nuclear explosion, possibly in an urban area, possibly out of the blue. Despite a decade of rising concern about the need to align forensics capabilities with a changing security environment, and an on-going effort directed from the White House level, significant problems remain. Current capabilities cannot meet desirable time lines, and bench depth is not strong, meaning that the system would fare poorly if stressed by the need to deal with more than a single incident. Further discussion of gaps and efforts to fill them can only be conducted at the classified level.

Current Combating WMD Intelligence Capabilities

In 2005, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction offered an indictment of current U.S. capabilities:

> "The Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction. This was a major intelligence failure…We simply cannot afford failures of this magnitude….We still know disturbingly little about the weapons programs and even less about the intentions of many of our most dangerous adversaries."

Current capabilities are inadequate to enable interdiction that quickly collapses smuggling routes, planning for elimination in a way that scales capabilities to likely demands, preparation of passive defense and consequence management practices suitable to enemy tactics, and rapid attribution of unclaimed nuclear detonations. The Commission flagged as a specific problem "poor analytical tradecraft—namely, the failure to do proper technical analysis informed by thorough knowledge of the relevant weapons technologies and practices."

Current Non-Nuclear Strike Capabilities

In this area, the study relied on the 2004 *Report of the Defense Science Board Task Force on the Future of Strategic Strike Capabilities* to underpin an assessment that much more progress can and should be made in fielding needed capabilities. Looking ahead by one or two decades, two key gaps stand out. One is in the ability to destroy several to a few tens of nuclear-related targets in transit. The other is in the ability to destroy or functionally disable large arrays of nuclear-related targets quickly enough to prevent them from launching ready nuclear forces, or to allow the escape of such systems to unknown locations, possibly in allied and U.S. territory.

Current Active Defense Capabilities

This study did not review current missile defense capabilities.

Current C4ISR Capabilities

The study did not review current C4ISR capabilities. These, too, were elaborated in the 2004 DSB study on strategic strike, which concluded the following: There is little real time characterization and monitoring of activities at

suspect facilities. The ability to find and track mobile nuclear-related systems is limited. C4 may not be survivable or able to support fast and complex preemptive or damage-limiting operations. Sophisticated adversaries are currently able to deny state-of-the art information assurance.

Current Nuclear Capabilities

Current capabilities seem robust for deterrence of large-scale nuclear attack on the U.S. homeland by proliferators. Indeed, this capability is likely to remain very robust so long as the United States fields a nuclear force primarily for purposes of dealing with uncertainties in relations with major nuclear powers. We assume that the United States will maintain a nuclear deterrent and that planning the main operational capabilities of that force will be informed primarily by decisions about what is necessary vis-à-vis Russia and perhaps also China. Recall that the focus of this study is on nuclear proliferation and not the nuclear problem more generally in U.S. national security strategy. Accordingly, the U.S. nuclear posture as a whole and the debate about Reliable Replacement Warhead and U.S. nuclear modernization policies and practices more generally have not been reviewed or assessed.

However, on the general topic of the future of the U.S. nuclear deterrent, two basic observations are offered. First, within the timeline of this study (between now and 2027), a plan for modernizing warheads and delivery systems must be put in place and, in fact, be well underway. Obviously the debate about how to modernize the warheads has already begun. The debate about how to modernize delivery systems has not begun, but is likely to involve discussion about whether to replace the old triad of nuclear bombers and sea- and land-based nuclear missiles with successor systems (at huge expense) or to move to some other posture (with uncertain consequences). It is possible that proliferation will motivate a future debate about the necessity of re-creating a nuclear delivery force that can operate within a theater but from a medium-range distance. Second, no strategy seems to exist for accomplishing the anticipated modernization, other than a piecemeal approach that is uncertain of promising success. This casts some doubt on the assumption stated above.

The preceding analysis of needed future nuclear capabilities highlighted some specific requirements, three of which are, in the view of this study, areas of concern: the credibility of extended deterrence, best-in-class nuclear security, and responsiveness to changing conditions.

The first requirement is that the United States be able to extend deterrence that its allies and friends, as well as enemies and potential adversaries, see as credible. Unfortunately, there seems to be no evidence of detailed understanding of the thinking of allies, friends, enemies, or potential adversaries on this point. Most of the available thinking in the U.S. defense community about extended deterrence is deeply rooted in the requirements of strategic relationships constructed during the Cold War. Only sporadic efforts exist to engage in strategic dialogues with allies and friends that explore what they see as necessary and sufficient in the U.S. military posture for purposes of their security and assurance in the new era. When it comes to enemies and potential adversaries, what is evident is a set of propositions about their theories of victory and their confidence that the United States will be self-deterred so as to render moot its extended nuclear guarantees—propositions that have not been tested against available evidence. Moreover, there is concern about the possibility that U.S. policymakers may unwittingly erode the credibility of extended nuclear deterrence when they express doubts about the viability of deterrence or the need for new and different nuclear forces.

The second requirement is for best-in-class nuclear security. While a detailed review of this subject was not undertaken as a part of this study, its members share the impression of many expert advisory groups that more can be done to achieve a uniformly high level of risk management performance across the enterprise. A key challenge is how to promote the adoption of best practices by others. Enhancing norms for responsible nuclear ownership is possible to the extent that more robust nuclear surety measures can be implemented domestically and internationally with sufficient transparency to provide confidence internationally in their efficacy. But there are serious security concerns about, and appropriate limitations on, the export of U.S. nuclear surety approaches and methods. However, these decrease with greater generality and with applications to material in non-weapon configurations (whereas they increase with greater technical specificity regarding fielded nuclear weapons).

The third requirement is for responsiveness to changing conditions. The U.S. nuclear weapons enterprise is today widely perceived to be fundamentally deficient for this purpose. This study did not undertake a systematic review of the weapons complex or its capacities for responsiveness and thus is not in a position to validate or refute the perceived deficiencies. It can attest to the lack of national consensus on future directions for the enterprise and expects that

some needed capabilities will not be available over the next two decades without some fundamental choices about future directions.[5]

Current Infrastructure Capacities

Current infrastructure capacities are far from robust. This problem is broader than the nuclear enterprise alone. Expertise is aging out in various sectors of the defense research and development community. Some of the relevant defense industrial base is fading, as, for example, for the production of ballistic missiles. Defense industrial base sustainment has been the focus of various DOD studies, including some by the Defense Science Board, but there appears to be no systematic effort to implement a viable long-term strategy for preserving core needed capabilities and capacities.

Current Integration Capacity

There are many examples of the lack of needed integration. In the joint requirements process, concepts for Phase Zero remain underdeveloped for the purposes of proliferation prevention, assurance, and dissuasion. Tailored country campaigns have not so far developed despite repeated recommendations. Little effort has been made to understand and articulate how the three pillars of the national strategy to combat WMD (counterproliferation, nonproliferation, and consequence management) can and should be integrated to produce effects that are complementary and synergistic. Even less effort has been made to build a viable political consensus on the objectives of national nuclear strategy or the means to achieve those objectives. The latest reorganization of the Office of the Secretary of Defense has eliminated capacity to lead analytical effort and sharply curtailed ability to engage effectively outside DOD on these issues. These are all examples of long-standing roadblocks to integration that have not been considered.

A striking condition is the contrast between the capacity for integration created for countering terrorism and the capacity for integration so far in place for countering proliferation. The United States government seems seized with the counter-terror challenge, and has created an aggressive integration effort, led from the highest levels, that writes strategy and implementation plans,

---

5 See *Report of the Joint Defense Science Board/Threat Reduction Advisory Committee Task Force on the Nuclear Weapons Effect National Enterprise*, forthcoming.

coordinates execution, assesses performance, and redirects resources. This process has also helped guide the flow of dramatic new levels of resources for operations and for capability and capacity development. It is difficult to find any such parallel activity on the "counter proliferation" side of "the nexus." The interagency process is weak. The highest level is not consistently involved. Implementation plans are created on a more or less *ad hoc* basis. Very few new resources have flowed. Indeed, some core defense capabilities and capacities for dealing with nuclear issues and proliferation have been thinned out as emphasis has shifted to "the long war."

Current Capabilities in Summary

The following summarizes, at the unclassified level, key gaps identified during the course of this study in the needed military capabilities and capacities to execute combating nuclear proliferation missions:

- **Interdiction:** no global system architecture, too few specialized and trained personnel, detection systems do not enable desired actions
- **Elimination:** not able to surge for larger-scale challenges
- **Passive defense:** too little training, no operational-level training, no stand-off detection architecture, growing systems vulnerabilities to nuclear weapons effects
- **Consequence management:** DOD's current sole focus is installation protection
- **Attribution:** national assessment takes weeks, databases inadequate, forensics capabilities not robust
- **Intelligence:** collection, analysis, integration with technical expertise all remain inadequate, as reflected in incomplete implementation of WMD Commission recommendations

In the ability of the strategic posture to meet the demands of assurance, dissuasion, deterrence, and defeat, key gaps:

- **Non-nuclear kinetic strike:** unable to conduct prompt strike from long range or achieve desired effects
- **Active defense:** theater protection of allies and friends, homeland protection from larger forces

- **C4ISR:** across the board weaknesses in finding and tracking mobile systems, coordinating complex high-speed operations, providing prompt situational awareness—plus C4 survivability
- **Nuclear strike:** an understanding of what the requirements of extended deterrence are and might become
- **Infrastructure:** aging out of expertise, erosion of nuclear weapons complex capacity, fading of relevant defense industrial base

In the capacity to integrate tools of national power, the key gap is that the U.S. government is not organized and mobilized for this problem the way it has for the counterterrorism problem, despite abundant high-level guidance.

The Challenges of Closing Capability Gaps

It is useful to distinguish between bottom-up and top-down processes for creating desired capabilities (and capacities). The bottom-up process is driven by the separate activities of the military services, combat support agencies, technology providers, and others to work the issues "in their lane." This process can be highly effective in generating new capabilities when the motivation to do so is widely shared and the resources are available. Absent shared motivation and resources, the results are typically piecemeal, incremental, and ultimately inadequate against an adversary that has been more purposeful. The top-down process is driven by the leadership. This process can be highly effective if leadership stays on message, provides strategic management of implementation activities, and directs the needed resources to the problem. The focus of this section is on the top-down process. There is a lot of activity to report from the bottom-up perspective on each of the 13 capability areas, but, so far at least, the results appear piecemeal, incremental, and inadequate for closing gaps against a skillful adversary willing and able to create, share, or use nuclear weapons.

The top-down effort to create the needed capabilities identified above and to address shortfalls in current capabilities is reflected in the following top-level guidance:

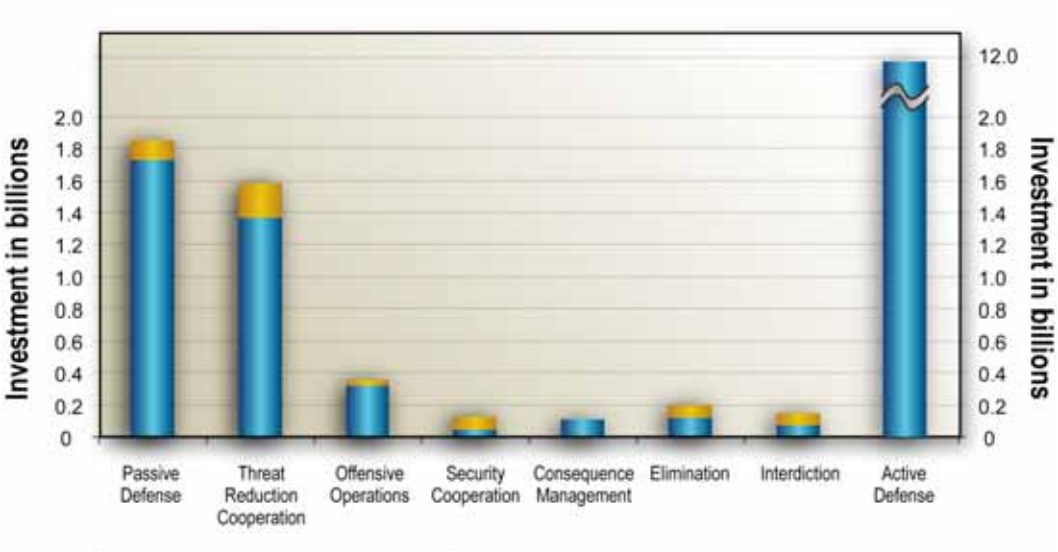
- 2002 Quadrennial Defense Review (QDR), which emphasized the framework of assure, dissuade, deter, defeat.
- 2002 Nuclear Posture Review, which elaborated the New Triad concept and the value of reducing reliance on nuclear weapons by increasing reliance on other means.

- 2005 National Military Strategy to Combat Weapons of Mass Destruction, which specified the eight mission areas.
- The 2006 QDR, which sought to transform enterprise management through the adoption of the joint capability portfolios. The 2006 QDR specified two such portfolios relevant to proliferation: combating WMD and New Triad/global deterrence. It also promised to "greatly expand" these specific capabilities. That QDR also highlighted the urgent need to enhance the capacity of DOD partners, including those in the interagency process and those abroad.

This top-down effort has not had much of an impact on the bottom-up process. Many new top-down processes have been created, but so far very little new capability has reached the force. Why is this so? Two main answers stand out.

First, the overall level of effort to create needed capabilities remains far too low to generate major capability increases. The current level of effort to develop needed capabilities and capacities for a more proliferated nuclear world underscores the point that DOD's priorities are elsewhere. Figure 3-11 utilizes the eight-mission construct of the national strategy to combat WMD to depict an approximate and unofficial basis for the allocation of funding across the missions and within them for the nuclear problem. The overall impression gained is an investment effort that is too small and ill-balanced to generate major capability increases, even as those are sought in the domains of missile defense and chemical and biological defense. (Note that the column for offensive operations does not include the funding for the nuclear weapons complex.)

Figure 3-12 illustrates funding for strategic forces over the last decade. The nearly flat line on investments incorporates the major increase for missile defense, which suggests how much funding has shrunk on other strategic systems over the last decade. (The $70 billion scale accords with the high point of spending during the Cold War.) This figure also reveals the fact that DOD spends far more on sustaining the current force than on investing for the future force. This level of effort seems unpromising in terms of developing the needed new non-nuclear capabilities in addition to whatever replaces the triad of nuclear forces inherited from the Cold War.



Note: Nuclear (yellow) versus chemical and biological (blue) (distinction not relevant for active defense and for some other generic capabilities). Dollar totals encompass research and development, procurement, and operations and maintenance. Dollar figures are approximate and have not been officially validated; there is some overlap among categories.

Figure 3-11. Approximate Investment Patterns in the Eight Missions of the National Strategy to Combat WMD, Fiscal Year 2008

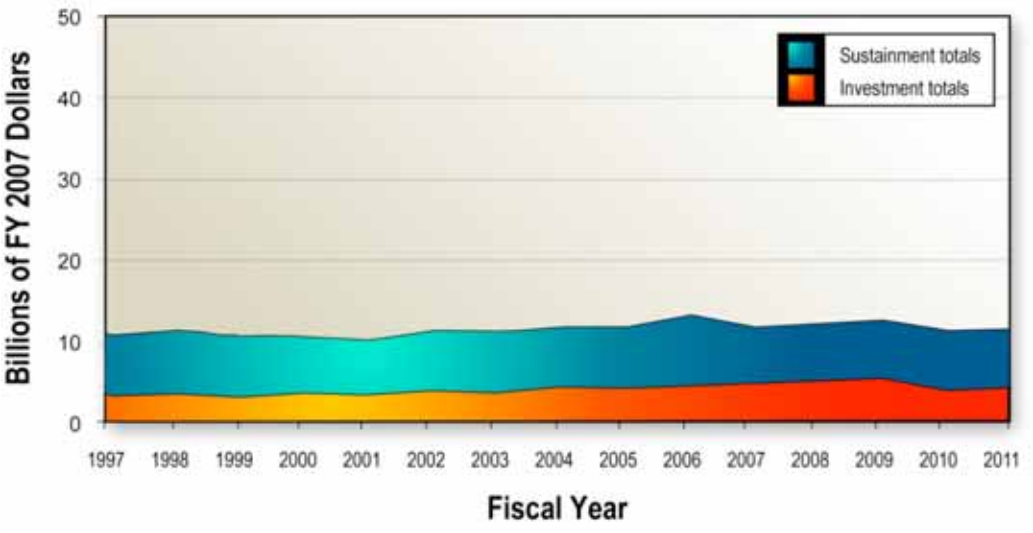


Figure 3-12. Funding for Strategic Systems

Neither time nor expertise was available during the course of this study to attach even approximate dollar figures to many of the needed new capabilities, so there is no attempt here to specify what level of investment would be "right" or where the biggest and quickest pay-offs in capability development might be. Moreover, some of the most important capability improvements can come in the operational realm and not in technology or procurement of new systems. But no evidence was uncovered to suggest that others have answers to these questions. Of note, most of the new program starts in this business over the last decade have come as a result of moving funds around within a small pool of money being spent on chemical, biological, and nuclear problems.

In sum, one plausible explanation for the continued existence of numerous capability gaps is that there has been no ramp up of investment consistent with the ramp up of very high-level political commitment to "greatly expand capabilities." The other essential factor is that the department lacks the institutional capacity it needs to sustain innovation and capability development for a more proliferated future.

Indeed, at a time when the leadership wants to "greatly expand capabilities," the department has been shedding capacities. The military services have steadily downgraded nuclear expertise. The Joint Staff has pared back and spread over a larger portfolio the relevant staff expertise. In acquisitions, the Office of the Secretary of Defense has not aligned itself with the objectives of national guidance for combating WMD. In terms of policy, recent reorganizations have eliminated focus and analytical support and seriously eroded the capacity to participate in needed interagency activities.

A simple illustration of this disinvestment in needed capability follows. In the 1980s, there were a number of nuclear-weapon-related analysis organizations within OSD and the military services that collectively provided a robust analytical capability. With the end of the Cold War, that capability was steadily reduced. By 2000, it was limited essentially to a small cell of analysts within the Office of the Assistant Secretary of Defense for International Security Policy (ASD/ISP) called the Studies and Analysis Group (SAG). This group provided computer programming, operational study support, maintained sensitive databases, and provided other related technical support. Its work advanced the development of a capabilities-based New Triad and evaluated emerging challenges, ranging from terrorists to nuclear-armed peer competitors.

The group's products were used directly by the ASD/ISP to brief the Secretary of Defense, enabled the ASD's staff to interact with the Joint Staff, and helped enable civilian oversight of planning activities at U.S. Strategic Command. In 2007, the group was disbanded. Today there is no analytic capability in OSD to support nuclear policy development, evaluate the progress in achieving nuclear policy goals, determine stockpile compositions, support arms reduction negotiations, issue guidance on DOD plans and programs, and recommend integration strategies to address future threats to the United States and its allies and friends.

At the same time, some institutional capacities have atrophied, and departmental leadership has promised to create some new capacities—but has not so far done so. The 2006 QDR included the promise to move to a joint capability portfolio management approach allowing more horizontal management across capability "stovepipes" within each portfolio; only four of the dozen or so portfolios identified by the QDR were given new horizontal management structures, and neither combating WMD nor New Triad/global deterrence is among them. Capabilities-based planning was created in order to deal with just this kind of problem; so far at least, capabilities-based planning has not proven to be effective for dealing with challenges outside the "defeat" problem space (that is, with assurance, dissuasion, and deterrence). Improved nuclear intelligence outputs continue to require much improved collaborations between the intelligence and military communities. The 2006 QDR praised the virtues of partnership capacities, both interagency and international, and committed DOD to rapid capacity development; so far at least, these efforts seem to have generated new activities on only a very small sub-set of the 13 capability areas.

In each of these areas, the problem seems to be that there is just enough effort underway to create the impression that enough effort is underway. To drive home this point, consider the case of WMD intelligence. Capability gaps are unmistakable. There is a lot of bottom-up activity to improve intelligence performance. There is also a lot of top-down activity. Processes are being improved. More information is being collected. But this critical enabler still fails to enable much of the needed activity. Why is this so?

To create better WMD intelligence, top-down efforts have led to two significant experiments: the National Counterproliferation Center (NCPC) under the auspices of the Director of National Intelligence and the U.S. Strategic Command Center for Combating WMD (SCC-WMD). The latter is the equivalent of a joint forces functional component command and is co-located

with DTRA. One of the primary functions of the SCC-WMD is to develop and maintain global situational awareness of foreign nuclear weapons programs and activities as a way to support the planning and operational requirements of the regional combatant commands. Obviously, this demands a fusion of all available information, ranging from open-source to the most classified intelligence available to the United States. For nuclear weapons programs and activities, it is critical that the situational awareness be technically informed, drawing upon the technical information available at DTRA and through DTRA's network of partnerships with the wider technical communities. To support the work of the SCC-WMD, DTRA has created a Combating Weapons of Mass Destruction Enterprise (one of the four associate directorships in the agency) and draws upon the resources of the entire agency. One of the major DTRA campaigns—situational awareness—is focused specifically on this mission requirement, and a number of the studies done by DTRA's Advanced Systems and Concepts Office are in support of the SCC-WMD's situational awareness needs. These efforts promise to enhance the understanding of combatant commanders of the known WMD challenges in their areas of responsibility—understanding that should help motivate and focus further capability improvements.

But there is also the problem of the unknown. Much of what military operators and planners need to know is not currently known—as the WMD Commission attests. How much of what is unknown might be unknowable is an open question. This brings us to the second experiment—the NCPC. From DOD's perspective, this experiment is at least as important as the SCC-WMD experiment. The NCPC is intended to make two primary contributions to the military's need for improved understanding of foreign nuclear activities. First, it identifies gaps in current knowledge and helps put in place strategies for filling those gaps. Second, it seeks to understand and help characterize the over-the-horizon nuclear proliferation threat, *i.e.*, the potential next proliferators and proliferators after next. Who are they? Why would they make this choice? How would they go about it? This work draws heavily on cross-disciplinary subject matter experts who work largely in the open-source and gray-literature communities.

Gaining "deep knowledge" on these questions promises to be extremely difficult. The problem set is growing more complex, with a growing number of countries of proliferation interest. The problem is growing more difficult, as more countries learn from the denial and deception practices of current and past proliferators. Deep knowledge also requires an interdisciplinary approach, combining regional and cultural with operational and technical expertise. Efforts to create and accumulate such deep knowledge have been undermined by the steady

erosion of investment in studies and analytical ability over the last two decades—this despite the valuable efforts of OSD Net Assessment and DTRA's Advanced Systems and Concepts Office to fill some of the gaps.

A strong and effective partnership is needed between these two experiments. Its virtues are often praised by the leaders of these two institutions and a positive workshop relationship is in the making. But what is the current result of this top-down effort? The following observations are offered:

First, the military has not been as effective as it might be in getting the intelligence community focused on its needs. The reasons are numerous. It doesn't know what to ask for, in part because it doesn't know what it can get. It often establishes special cells to work specific issues that do not effectively enlist intelligence community expertise. It has not learned intelligence community processes well enough to know what inputs can help ensure desired outputs. It focuses very heavily on tactical operations with too little interest in strategic topics, where there are unrealized opportunities to help drive intelligence collection and analysis. On proliferation specifically, military experts collaborating with the intelligence community seem to believe that proliferation ought to be easy to understand, explain, and predict.

Second, the intelligence community has not focused adequately on national military needs. To be sure, there is a lot of on-going activity associated with providing timely intelligence information to the Secretary of Defense and combatant commanders. The community participates in joint cells focused on specific issues and hard targets, provides technically informed sources-and-methods intelligence as needed, and advises on capability needs for collection, data fusion, and exploitation as they relate to the tactical intelligence picture. But the community does not well understand military needs beyond the immediately military tactical ones. It does not understand the military's need to create operational plans across all of the defined operational phases. It has little appreciation of the strategic picture that many highly experienced military planners bring to the proliferation subject. As a result, intelligence collection and analysis that might be focused on more strategic questions is not.

These are of course gross generalizations and there are exceptions to each of them. But the general pattern is clear: the experiments have not yet created the partnership that will create the needed intelligence. Although success it not yet in hand, the two experiments can succeed and their success will be mutually reinforcing. In the view of this study, it is possible for DOD to respond effectively

to intelligence community desires for more effective partnership, by strengthening the expertise it brings to the partnership. The two would benefit from a joint commitment to work long-term issues and address capability shortfalls associated with the need for situational awareness and information dominance. A strategic picture of the global proliferation problem is not out of the question and would be highly valuable for the amplification of military situational awareness. More effective partnership on WMD interdiction issues is also possible; currently there is too much fragmentation and not enough high-level DOD engagement.

This case study well illustrates the gap between process and result—between top-down initiatives to make new things happen and their effective implementation that creates the needed result. The important progress in standing up these experiments ought to be much praised. The need for continued progress to accomplish stated goals ought not to be forgotten.

Chapter 12. Toward More Effective Proliferation Prevention

Separate and apart from exploring the military operational requirements of life in a more nuclear-crowded future, this study addressed the question of whether more can be done to enhance proliferation prevention now. Much is already being done, with a particular focus on the problems posed by North Korea and Iran. The historical work conducted during the course of this study as a way to identify trends into the future proved rich in insight about the opportunities for rolling back the intentions and capabilities of potential proliferators. As argued earlier, along each state's proliferation "pathway" are numerous key decisions about developing capabilities and/or adhering to international treaty commitments, and each of these decision points is a target of opportunity that can be worked to persuade potential proliferators not to further develop capabilities or buy time.

Historical experience illustrates the prominent U.S. role in inducing restraint by potential proliferators. Working in partnership with others, and sometimes alone, it can impose economic, political, and security costs on those states, via sanctions, coalitions, and alliances. It can extend deterrence to allies to help reduce the perceived need for indigenous nuclear forces. It can lend its power to the effort to build regional security systems that help to ameliorate the perceived need for nuclear deterrents. It can offer leadership in strengthening international norms against proliferation, and advocating for (and demonstrating) the highest standards of responsible nuclear ownership. Experience also illustrates that this role is most promising when U.S. engagement is sustained and proactive. Episodic engagement has worked poorly. Equally important has been the ability to innovate policy approaches to tailor existing policy tools and create new ones to meet new challenges.

Perhaps the greatest success in attenuating proliferation pressures was in the 1960s, a time when many states in the developed and developing worlds were beginning to explore nuclear weapons options and to put programs in place. The escalating arms race between East and West provided the main context for nuclear thinking for most countries, especially in the developed "First World." China's nuclear test in 1964 was a key potential tipping point, as it might have driven other countries in Asia and elsewhere in the "Third World" to pursue nuclear weapons. The potential cascade of proliferation that might have followed was met with a

mix of guarantees from the United States, both formal and informal; sanctions against recalcitrant states; and a codification of restraint in the form of the Nuclear Non-Proliferation Treaty. The result was that only a handful of the 20–30 states that started down that path ended up with nuclear weapons.

The next potential tipping point came a decade after China's test in the mid-1970s, with India's "peaceful nuclear explosion" in 1974 and U.S. withdrawal from Vietnam in 1975, which raised fundamental questions for many U.S. friends and allies in East Asia about the credibility of U.S. security guarantees. In response to this new wave of proliferation risk, the United States effectively exploited international proliferation concerns to enforce a much higher level of discipline in the trade of sensitive materials and technologies. It also took steps to reinforce the credibility of its guarantees in the eyes of a few particularly worried allies. The result again was that a wave of potential proliferation in the developing world crested and receded without the addition of anything more than 1-2 new devoted seekers of nuclear weapons. Indeed, it culminated with the decision by four states to abandon nuclear weapons: South Africa, Ukraine, Belarus, and Kazakhstan.

This short survey does not exhaust the relevant nuclear history. It does illustrate the potential for proliferation prevention even when facing a potential tipping point, as well as the value of sustained engagement and policy innovation by the United States. Over time, prevention (and rollback) has been enabled by two main policy tools: the nonproliferation regime and deterrence. In the 1960s, the treaty regime was created to formalize the restraint that most countries in the First, Second, and Third Worlds chose as consistent with their interests in this period; extended deterrence played a critical role in meeting the security needs of many. In the 1970s and 1980s, the treaty regime was used to induce further restraint in tailored strategies targeted on problem countries. A shadow was cast over extended deterrence by U.S. withdrawal from Vietnam and the United States took many steps in this period to reassure its allies of its continuing commitments to them. In the 1990s, the nonproliferation regime was the foundation for Cooperative Threat Reduction and for tailored strategies *vis-à-vis* a handful of noncompliant states; doubts arose about the credibility of extended deterrence in the face of rogue states armed with nuclear-tipped missiles and again steps were taken to erase those doubts. In the current decade, the treaty regime has shown itself useful for all of the previous purposes, though still not efficacious in dealing with the problems of willful noncompliance (though to be clear, this is not a task for which it was created). Efforts to adapt deterrence to the challenges of dissuasion have preceded an emerging array of doubts about the credibility of U.S. guarantees and about U.S. competence to safeguard the

interests of its allies and friends. Despite well-founded frustrations with the nonproliferation regime, it remains an essential foundation for cooperative action to enforce norms. Despite repeated concerns about the viability of U.S. extended deterrence, it remains essential for preventing proliferation by the many U.S. allies and friends among the next tier of potential proliferators.

This leads to an important recommendation:

RECOMMENDATION: DEPARTMENT OF DEFENSE

With the Office of the Under Secretary of Defense for Policy in the lead, the Department of Defense should develop tailored approaches to proliferation prevention that span the full problem space and work to energize an interagency process on these issues.

- Working with the geographic combatant commands, country campaign plans should be composed that address the full range of potential problems in each area of responsibility:
  - allies and friends
  - enemies and potential adversaries
  - linchpin countries whose choices will affect many
  - potential secondary reactions
- Ensure participation in composing and executing those plans of needed interagency partners:
  - Partners include the Departments of State, Energy, Commerce, and Treasury, as well as the intelligence community.
  - This interagency partnership would work best if it is coordinated at the top, implying that the optimal solution would be a plan crafted and led at the National Security Council that DOD supports. Less preferable would be a DOD plan that has coordinated interagency inputs.
- Integrate these country campaign plans into planning for Theater Security Cooperation and Concept of Operations Plan (CONPLAN) 8099 Phase Zero.
- Execute, assess, and adapt as required by the planning cycles for the Theater Security Cooperation and CONPLAN processes.

To underwrite the execution of these plans over the medium- and long-term, it will be necessary also for the Department to develop the capabilities and capacities noted above. Deterrence cannot be extended without forces in being. Assurance derives in part from an ally's understanding that the United States has available to it viable means to deal with the challenges of aggressive neighbors. Dissuasion requires that potential adversaries understand that the military advantages they seek through the creation of new, and in this case nuclear, capabilities will not be won because the United States will not stand idly and allow the military tables to be turned.

Additional Recommendations

The following recommendations, organized by key actor, grew out of the analysis conducted and described in this and the preceding chapter. They direct specific actions that key leaders need to take to affect the type of change described and lay the foundation for developing the needed military capabilities and capacities identified.

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS

1. Follow through on 2006 QDR commitment to implement more horizontal management approach to joint capability portfolios. Formally designate portfolio managers for the New Triad and Combating WMD portfolios. Endow them with the institutional resources (principally analytical support and political top cover) to create roadmaps and assess progress in implementation.
2. In the Combating WMD portfolio, initial investments in interdiction, detection, and forensic capabilities need to be followed with step-function increase; ramp-up passive nuclear defense and consequence management. Supplement funding to DTRA for specified purposes.
3. In the New Triad portfolio, reprioritize so that investments match the accelerating threat. Also, establish the analytical capability to study options for nuclear force modernization/transformation in a plausible range of future planning assumptions.
4. Stand up a nuclear analytical group to support senior OSD leadership on nuclear posture and broader related issues.

5. Advocate with DOD leadership to integrate technical improvements into a larger process of capability and capacity development encompassing both material and non-material solutions.
6. Formulate a strategic plan for DTRA, including roles, missions, and capacities.

DEFENSE THREAT REDUCTION AGENCY

1. Lead DOD efforts to understand the problem and solution spaces. DTRA needs to be more than a gap filler job-shop.
2. Advocate with OSD for designation of the capability portfolio managers.
3. Ramp up to assist OSD with the analytical questions associated with development and implementation of portfolio roadmaps.
4. Define metrics to measure progress and balance effort across modalities and combating WMD pillars (nonproliferation, counterproliferation, consequence management).
5. Secure funding for more robust and faster-paced development of capabilities for nuclear counterproliferation:
   - For interdiction, seek funding for advanced stand-off detector work at $100 million.
   - For attribution, seek funding for ownership of technical robustness of forensics capabilities at $25 million. Key tasks: (1) identify current capability limitations of collection and analysis systems; (2) execute red-team assessment of countermeasures to technical forensics.
   - Redress severe atrophy in nuclear weapons effects enterprise. (Scale of effort appropriate to expectation of need to sustain operations under very limited attack—eliminate enemy cheap shots.)
6. Expand collaborative activities with the NCPC. Accelerate over-the-horizon work. Assist NCPC to develop more strategic approaches to WMD intelligence. Commit to completing one for each combatant command area of responsibility in two years.

U.S. Strategic Command Center for Combating WMD

1. Assess the center's roles and missions beyond elimination and interdiction in light of the full combating WMD mission space. Better map the gaps and seams with the New Triad/tailored deterrence missions as they bear on the capacity to prepare for future proliferation challenges.
2. Lead U.S. Strategic Command efforts to support the regional combatant commands in developing effective execution plans for the Combating WMD CONPLAN 8099. Where regional commands face existing nuclear threats, will require effective coordination with other Strategic Command mission areas. Include consequence management as a next priority.
3. To reap targets of rollback opportunity, develop Phase Zero 8099 implementation plans that integrate proliferation prevention and response requirements into Theater Security Cooperation Plans.
4. Advocate with the military services to budget to fill capability and capacity gaps identified by combatant commanders.
5. Support Joint Forces Command experimentation so that it adequately maps the problem/solution space. Integrate technical and operational solutions.
6. Support Defense Intelligence Agency (DIA) efforts to meet intelligence requirements of 8099.
7. Experiment with a single combatant command operational plan to explore the implications of intelligence gaps that cannot be filled. Assess how operations at all phases will be influenced. Identify ways to work around unavailable information that might be needed in concepts of operations and tactics, techniques, and procedures.

Office of the Under Secretary of Defense for Policy

1. Through regional bureaus and in partnership with combatant commanders and the State Department, develop tailored regional strategies that support national combating WMD guidance. These regional strategies should include plans focused on specific countries of interest and tailored for the unique challenges of assurance, dissuasion, or deterrence associated with each. Such plans should:

- Identify the conditions of success for U.S. policy within each country.
- Identify the sources of influence within each country and the best means to target each. In most countries, there are multiple constituent groups whose views must be understood and responded to in a tailored fashion.
- Direct the integrated employment of all instruments of U.S. national power—economic, political, and military—so that "carrots and sticks" can be orchestrated to achieve U.S. objectives.
- Direct the integrated employment of partner capacities, whether those of other major powers influential in regions of proliferation concern or of international institutions of various kinds, including both U.S. alliances such as NATO and other entities as appropriate.
- Define metrics of success and monitor performance of the plan with the support of intelligence inputs.

2. Advocate with the State Department and the White House for creation of a comprehensive national plan that integrates DOD efforts into broader U.S. strategy.
3. Utilize the new Force Employment Guidance to complete the development of guidance for combating WMD and global deterrence. Fully elaborate the Phase Zero shaping requirements.
4. In parallel with work on tailoring deterrence, undertake work on tailoring assurance. This will require new dialogues with allies and partners. Focus on linchpin countries in specific areas of responsibility and on strategic communications with them.
5. Fix the problems generated by the recent reorganization:
   - re-create a focal point at a senior level
   - re-assign personnel to enable effective OSD participation in relevant departmental, interagency, and international activities, including especially analytical ones
6. Advocate with the OSD leadership for more effective efforts to create and deepen bipartisan support of the deterrent:
   - Secretary of Defense should enhance the effort to develop a core of interested, informed, engaged members of Congress on a bipartisan basis.

- Deputy Secretary of Defense should prepare for the next Nuclear Posture Review so that its release can become a major step in consensus building.
- The Under Secretary of Defense for Policy and U.S. Strategic Command should develop a strategy for applying deterrence capabilities to produce desired nonproliferation outcomes.

JOINT STAFF

1. Address the underperformance of capabilities-based planning for the proliferation problem:
   - ensure that analytical front end adequately maps problem space:
     - Defense planning scenarios need to reflect plausible spectrum
     - Joint Integrating Concept for Combating WMD needs to reflect full nuclear counterproliferation challenges
     - Joint Operating Concept for Shaping needs to address dissuasion and assurance
   - create a Functional Capability Board with the range of interest to address proliferation concerns (The present system, which relegates all counterproliferation decisions to the Force Protection Board, is inadequate.)
2. Sustain an adequate base of joint staff expertise:
   - The number and seniority of J-5 staff with combating WMD responsibility has declined steadily in recent years.
   - J-8 needs to be staffed at a level enabling it to deal with its expanding portfolio (from chem.-bio defense to combating WMD).
3. Complete draft Joint Pub 3-12.1 (Joint Tactics, Techniques, and Procedures for Theater Nuclear Planning) and oversee implementation by the military services.

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

1. Continue to build the partnership between DOD elements (*e.g.*, DIA, SCC-WMD) and the NCPC by helping to:
   - Augment the pace of future risk assessments in the NCPC "over-the-horizon" portfolio, identify cross-cutting lessons and needs, and formulate strategic questions of the kind to which DOD needs answers.
   - Develop models of the nuclear status of each country of proliferation concern that map out internal decision-making milestones and external indicators, and exploit these models to shape motivation, intent, and capability.
   - Develop country-specific proliferation "watch" capabilities that:
     - drive intelligence collection to extend to information on political-military leadership intentions; use doctrine, regional security perceptions, and support the development of collection sources and methods where needed
     - develop a methodology for using such information to trigger U.S. actions that help shape the decisions of potential proliferators
     - guide the intelligence analysis process to close key gaps in the understanding of a proliferator's strategic behavior (For example, what would it take to understand a proliferator's "theory of victory" in nuclear conflict with the United States?)
     - understand and disseminate information on sensitivity of outcomes given insufficiencies in the available information
2. Invest to meet the requirements of the Intelligence Campaign Plan supporting CONPLAN 8099 (Combating WMD).
3. With Strategic Command and combatant command planners, identify the consequences of information/intelligence that will probably never be known. Pick a single plan, exercise with intelligence denied, and share the lessons with all commands. Ideally, such work would be linked conceptually with an NCPC gap analysis that has clarified what can be known, might be known, and won't be known.

Final Observations

This discussion of nuclear proliferation closes with the two questions posed at the beginning of Chapter 10: Will nuclear weapons be embraced by enemies as their premier asymmetric capability? Will nuclear weapons endow a new tier of states with peer-like capabilities to limit U.S. freedom of maneuver? To a significant degree, the answers to these questions are up to the United States.

Consider the possibility that the United States fails to create the capabilities for life in a more proliferated world. What would be the implications? The answer can be framed in terms of what U.S. leaders will want to do, won't want to do, and might have to do:

- If gaps are not filled, U.S. leaders may not be able to do what they will want in a more proliferated world. They may not be able to contain or deter nuclear aggressors, counter their attempts at coercion, or teach the right lessons. They may not be able to suppress networks or capture "loose nukes." Or the nation may pay a higher than needed price for doing these things because leaders failed to create the needed options.
- If the gaps are not filled, U.S. leaders may have to do things they don't want to do. They might have to appease proliferators, acquiesce to their acts of aggression, tolerate the nuclear defections of friends and allies, and suffer the costs to credibility and standing.
- And they may have to go to war against nuclear-armed enemies but then back down—or escalate in ways that would not otherwise be necessary, and that would have large consequences for the nature of the peace to follow.

Alternatively, what might be if needed capabilities are created in timely fashion? Nuclear weapons are unlikely to be embraced by enemies as their premier asymmetric capability. The United States is unlikely to find itself hemmed in by a new tier of states endowed with peer-like capabilities to limit U.S. freedom of maneuver.

The contrast between these two very different outcomes is stark. The consequences of a *laissez faire* approach to gap-filling are significant. More deliberate action is necessary.

Appendix III-A. Proliferation Contingencies 2027

This appendix provides detail on the eight contingencies analyzed in the nuclear proliferation chapters of this report:

1. Suppress a newly discovered illicit proliferation pathway
2. Inhibit allied nuclear defections
3. Capture loose nukes from a failing state
4. Dissuade proliferator development of more potent capabilities
5. Intervene to terminate a regional nuclear war
6. Extend nuclear deterrence to new security partners
7. React to nuclear-backed aggression by a revolutionary, expansive power
8. Contain a hostile coalition

The odd-numbered contingencies are crisis-driven; the even-numbered ones are contingencies associated with efforts to shape the security environment. These are linked sequentially to the four alternative futures, as described in the body of the report.

Contingency 1. Crisis: Suppress a newly discovered illicit proliferation pathway

Essential Features

- The number of states with small arsenals for defensive purposes has grown by a modest number.
- The number of states with latent capabilities continues to grow.
- Uneven capacities among new states to control nuclear components and potential suppliers of unauthorized material or components exist.
- There is an increased number of radical or autocratic regimes in regions with new or latent nuclear powers.

- Radical terrorist organizations increase their dominance in regional ungoverned territories and accelerate their drive to the stated goal of obtaining nuclear capability.
- Pervasive insecurity among regional non-nuclear states spurs desire for rapid nuclear development.
- Transnational criminal and black market activity of all types has increased.

Flashpoints leading to crisis contingency:

- Intelligence indicators of rapid buildup of nuclear infrastructure in one or more non-nuclear states or terrorist operations area in ungoverned space.
- Intercept of partial shipment of dual-use components with utility in nuclear material processing or weapons development.

  AND/OR
- Unknown quantities of fissile material unaccounted for by one or multiple nuclear custodians.
- Electronic intercepts of internet plans for design of sophisticated nuclear weapon and identification of specific components required (*i.e.*, "a shopping list").

U.S. Objectives

U.S. leaders would want to:

- Identify the source and destination of illicit materials:
  - establish proper control of nuclear or dual-use materials at the source
  - dismantle or destroy nascent infrastructure at unsanctioned locations
  - locate and secure loose fissile material
- Identify potential pathways and intermediaries:
  - eliminate transportation and shipment routes between the source and potential destinations
  - disrupt and destroy illicit financial, transportation, and supplier network activity
  - uncover and eliminate unwitting cooperation by legitimate enterprises
- Gain international cooperation to close down networks, and establish increased controls.

What they would not want to do:

- Allow unauthorized transfer of nuclear materials or components to non-nuclear actors.
- Allow unsanctioned movement of fissile material outside of originator's borders.
- Go it alone.
- Unilaterally use force without international cooperation, especially against a sovereign territory, unless there was the imminent threat of nuclear or radiological weapon use.
- Allow continued progress toward nuclear weapon capacity while establishing "proof" to the international community.
- Take action that would suppress uncovering key nodes of the network (i.e. allow it to go more underground).
- Spark creation of alternate pathways or new markets.
- Waste limited resources on black markets with no connection to nuclear trade.
- Pay a high economic or political cost to inhibit further proliferation.

Losing would mean:

- Failure of the nonproliferation regime.
- Pervasive insecurity in international environment:
  - tightening security and closing borders by major economic nations, resulting in decline of worldwide trade
  - increased nuclear competition
  - increased risk of miscalculation among nuclear actors
- Increased opportunities for nuclear terrorism:
  - higher potential for nuclear or radiological weapons use with no/little warning

Blue Concept of Operation

Political strategies:

- Short term:
  - Build an international consensus against suppliers and recipients.
  - Build an international task force to track and destroy this network by:
    - emphasizing information sharing and development of a common operating picture
    - coming to an agreement for rapid engagement by member parties best suited for specific action or activity with limited consultation of other member parties
  - Encourage immediate and complete accounting of nuclear materials by nuclear states.
- Long term:
  - Create an international environment hostile to trade in nuclear by:
    - gaining renewed (and universal) international cooperation and commitment to eliminate illicit networks
    - invigorating the Proliferation Security Initiative
    - increasing information sharing among law enforcement, intelligence, and financial agencies
    - developing international strategic communication aimed at black marketers (message: “you can’t get away with it”)
    - cooperating to track and disrupt financial flows
  - Renew the international commitment to a revamped nonproliferation regime by:
    - reorienting its focus toward security of nuclear systems and material, border controls, and cooperation to stop illicit movement and transfer
    - creating incentives for complete and accurate accounting by nuclear states

        - revamping the oversight role of the International Atomic Energy Agency and provide increased capabilities for oversight through international consortia

    - Promote dialogue among regional actors aimed at building confidence by creating mutual understandings of the sources of instability in their unfolding nuclear relationships and by adopting mechanisms to manage those instabilities.

Military strategies:

- Short term:
    - Stop the flow of nuclear material and components by:
        - increasing intelligence monitoring in key regions or transit areas
        - working with international intelligence and law enforcement agencies to develop a common operational picture of illicit activities
        - deploying military forces (especially special operations forces) to key locations and prepare for interdiction operations
        - considering a blockade at source or destination ports
    - Develop an information operations campaign to intercept and disrupt electronic transmissions, spoof communications, and electronically isolate network nodes.
- Long term:
    - Focus security cooperation on building partner capacities and interoperability to detect and disrupt illicit nuclear flows.
    - Develop niche capabilities in key areas for intelligence monitorint, interdiction, nuclear detection, and disablement.

Needed Capabilities and Capacities

Capabilities

- A strategic toolkit that is regionally deployed and includes intelligence, surveillance, and reconnaissance; nuclear detection; special operations forces; interdiction; and information operations.

Capacities

- Intelligence, surveillance, and reconnaisance to continually track and monitor material movement.
- Information sharing with allies, partners, and international agencies.
- Nuclear "rapid deployment force":
  - rapid deployment of interdiction and SOF capabilities to disrupt known movement of materials (within 24 hours)
  - force able to dismantle nuclear infrastructure and secure loose materials with little notice

Contingency 2. Shaping: Inhibit allied nuclear defections

Essential Features

- Few, if any, additional states possess nuclear weapons.
- States that possess nuclear weapons have generally refrained from wielding them to directly threaten during periods of increased tensions:
  - more defensive/self-protective nuclear postures during crises
  - elevated alerts with short employment times are rare
  - significant international efforts to de-escalate and defuse crises
- Many more states have significant indigenous latent capabilities and capacities to quickly develop, field, and mature nuclear weapons arsenals:
  - nuclear power production enterprise with closed fuel cycle
  - diverse, mature nuclear R&D programs with military participation
  - access to significant stockpiles of weapons-usable nuclear material
    - indigenous
    - shared pool among regional energy partners
  - sustained investment in conventional military modernization

- Some states and non-state entities in persistent competition with strong (nuclear or non-nuclear) powers have established security partnerships with states that are very near or over the nuclear weapons threshold.
- Nuclear surety (safety, security, use control, reliability) approaches, practices, and levels of assurance for weapons and weapons-usable material vary significantly among states.
- Sophisticated dual-use technologies, military delivery vehicles, nuclear weapons knowledge, and smuggling pathways have diffused worldwide. Nuclear weapons-usable material is the last significant hurdle remaining to nuclear weapons capabilities for criminal and terrorist enterprises.

U.S. Objectives

U.S. leaders would want to:

- Diminish the relevance globally of nuclear weapons as instruments of national power.
- Resolve persistent strategic tensions in regions that could drive state decisions to cross nuclear weapons thresholds.
- Strengthen international normative behavior for control, transparency of control, and surety of nuclear weapons, components, and usable material.
- Assure allies and friends with latent capabilities of U.S. commitment to conduct in the region that:
  - reinforces reliability of U.S. security guarantees
  - is supportive of and responsive to their security interests
- Assure competitors with latent nuclear weapons capabilities that transparent non-possession best serves their security interests.
- Dissuade everyone with latent capabilities from:
  - increasing opacity of weapons-sensitive nuclear activities
  - taking steps toward more incipient weapons capabilities
- Dissuade potential adversaries from perceiving that nuclear weapons possession could mitigate their security risks.
- Deny the ability of non-state entities to acquire or sustain pursuit of nuclear weapons-usable capabilities.

- Deter states with nuclear weapons or weapons-capable material from contributing, either knowingly or through sloppy nuclear surety, to illegitimate transfers of nuclear weapons, components, or usable material.
- Foster responsible use of nuclear power production to increase energy security and combat global climate change.

U.S. leaders would NOT want to:

- Be dissuaded from knowledge or uncertainty of competitors' nuclear weapons capabilities from following through on security commitments.
- Be perceived as impotent in slowing/stabilizing movement toward incipient nuclear weapons capabilities.
- Drive latent nuclear capability toward/across acquisition threshold as an unintended consequence of U.S. foreign relations policies and conduct.
- Be unable to garner international consensus/support for dissuasive pressures against incipient nuclear weapon acquisition.
- Be unable to detect or correctly interpret indicators of:
  - latent state capabilities moving toward/across weapon threshold
  - preparations for criminal or terrorist theft or control of nuclear weapons, components, or material
  - loss of legitimate control of nuclear weapons, components, or material
- Be perceived as having less-than-exquisite intelligence on matters of nuclear proliferation and control.

U.S. leaders might HAVE to:

- Cede U.S. self-interests in a region (*e.g.,* spread of democracy, containment of competitors' influence, military presence, etc.) for the sake of reducing nuclear tensions or gaining concessions from competitors.
- Expose intelligence sources/methods/capabilities to establish incipient capabilities/activities forensically to garner international opposition.
- Forcibly remove/destroy keystone threshold crossing capabilities of states operating outside international norms of acceptable behavior.

- Accept greater transparency of the state of the U.S. nuclear weapons enterprise in exchange of reciprocal measures.

Losing would mean:

- More states with nuclear weapons.
- Greater challenges in reducing/containing the number of nuclear states.
- Increased complexity and uncertainties in managing nuclear national security risks.
- Weakening of international nonproliferation frameworks.

Blue Concept of Operations

Political strategies:

- Promote dialogue and formal agreements among regional actors aimed at resolving sources of strategic tensions through cooperative solutions for mutual benefit.
- Strengthen international norms and sanctions against pursuit of nuclear weapons capabilities.
- Foster adoption of robust nuclear material surety "best business practices" with high degree of transparency.
- Foster adoption of/conversion to more intrinsically resistant nuclear power generation enterprises.
- Champion engagement in international agreements/ frameworks for:
  - nuclear material control and transparency
  - nuclear arms diminishment
- Be prepared to offer substantive concessions in U.S. military posture (nuclear and conventional power projection into the region) in exchange for commensurate measures.
- Strengthen U.S. commitment to extend non-nuclear deterrence and defenses to non-nuclear allies.
  - enable extended deterrence ratchet to nuclear strike capabilities, while suppressing nuclear facets in policies and strategic communications

- Exercise restraint in exercising military power against non-nuclear competitors to achieve strategic objectives (to de-motivate nuclear acquisition urges).

Military strategies:

- Establish regional cooperative security exchanges, with metrics, for gauging progress and adaptive feedback mechanisms for:
  - proliferation prevention
  - tension resolution
- Advocate a reduction in numbers and alert levels of nuclear forces.
- Establish the capacity to strengthen extended non-nuclear deterrence to partners through shared defensive and strike resources.
- Demonstrate the willingness and capabilities to increase transparency of nuclear posture and enterprise activities.
- Increase intelligence monitoring/surveillance for illicit nuclear networks.
- Establish the perception of exquisite capabilities to hold at risk any nuclear enterprise activities outside the bounds of international normative behaviors.

Needed Military Capabilities and Capacities

Capabilities:

- Insert special operation forces for forensic intelligence collection, keystone capability elimination.
- Robust extended non-nuclear deterrence infrastructure, planning, operations, and training toolkits.

Capacities:

- Resources to surge extended deterrence capabilities at the request of extended deterrence partners.

Contingency 3. Crisis: Capture loose nukes from a failing state

Essential Features

- The number of states with small arsenals for defensive purposes has grown by a modest number.
- The nuclear relationships between and among new regional nuclear actors have not become intensely competitive.
- None of those actors has developed the ambition to compete with the U.S. to create a relationship of assured mutual vulnerability.
- The number of states with latent capabilities continues to grow, increasing the risk of rapid breakout and rapid deterioration of the regional security environment.
- Non-state actors see more targets of opportunity to purchase or steal a nuclear weapon or some key components.

Flashpoint leading to crisis contingency:

- Internal instability in a nuclear state
- Potential or actual loss of positive control of warheads

U.S. Objectives

U.S. leaders would want to:

- Set conditions so that positive control over weapons is maintained, despite instability.
- If positive control by responsible party is no longer certain, then locate, secure and render safe or destroy the weapons or set conditions so that a responsible party quickly establishes or re-establishes positive control over the weapons.
- Prevent weapons in employable form from falling into hands of terrorists or other hostile party that might detonate the weapons or transfer them outside the country in question.

- Eliminate residual nuclear capability of state or ensure safeguards under responsible and accountable central authority.
- Set conditions for status quo or new central authority to maintain order.

What they would not want to do:

- Allow a deteriorating situation to lead to the central authority's loss of positive control or a responsible nuclear regime to be toppled.
- Allow weapons to "leak" out of the country in question.
- Allow horizontal escalation, *i.e.,* attacks on external parties that widen the crisis.
- Allow weapons to be used against U.S. interests.
- Return weapons to an unstable regime (or even to a stable one).
- Respond slowly to events.

Theory of victory:

- Nuclear weapons are eliminated or placed under positive control of responsible party.
- Terrorist or other groups hostile to U.S. interests do not have a nuclear capability.
- The long-term threat of loss of positive control of nuclear weapons is reduced.
- Conditions are set for stabilization within the country.

Losing would mean that:

- Some nuclear weapons end up outside the positive control of a responsible/accountable/deterrable authority, and could be used or brandished against U.S. interests or to disrupt international peace and security.

Blue Concepts of Operation

Political:

- Oppose violent extremist parties.
- Aid the responsible party within a state with reasonable prospects of maintaining or establishing positive control over weapons.
- Limit horizontal escalation or intervention by any third party.
- Reassure neighboring countries through deployment of missile defense.

Military:

- Clandestinely preposition ISR, explosive ordnance disposal, and render safe equipment to speed operations in extremis.
- Clandestinely locate and tag nuclear weapons prior to crisis.
- Assist responsible party to maintain/restore stability and positive control over weapons.
- Interdict weapons and prevent transit out of country.
- Conduct wide area surveillance.
- Detect fissile material.
- Locate, characterize, and track weapons and/or delivery systems.
- Locate, detain, and interrogate key personnel.
- Find and render safe weapons.
- Secure key installations, weapons, and areas.
- Provide overwatch for key government and military installations and assets.
- Conduct elimination of nuclear capabilities or remove weapons from country.
- Conduct foreign internal defense/counter-insurgency under limited nuclear threat.

Needed Capabilities and Capacities

Capabilities:

- Missile defenses for reassurance of regional states and defense of U.S. military presence in theater.
- Penetrating/survivable, high-volume, long-range precision strike.
- Prompt global strike.
- Non-lethal weapons for securing large sites with minimum footprint.
- Network entry and attack.
- Wide area ISR, including fissile material detection, persistent synthetic aperture radar ground surveillance with change detection.
- Rapid forcible entry to secure key airfields and installations.
- Explosive ordnance disposal team(s) and equipment.
- Render safe special operations forces and equipment.
- Special operations forces for foreign internal defense.
- In-theater render-safe pre-positioned fly-away packages.
- Special airlift for insertion and extraction at range.
- Site exploitation and security.
- Shielding against electromagnetic pulse.

Capacities:

- Penetrating/survivable, high-volume, long-range strike.
- Tier I render safe/national mission force.
- In-theater pre-positioned stocks (U.S.-based and clandestine).
- Airborne ISR assets for wide area surveillance.
- Network monitoring and attack.
- Sufficient deployable missile defenses.
- Forces and materiel for WMD elimination and site security 24/7.

Contingency 4. Shaping: Dissuade proliferator development of more potent capabilities

Essential Features

- The number of states with small arsenals for defensive purposes has grown by a modest number.
- The nuclear relationships between and among new regional nuclear actors have not become intensely competitive.
- None of those actors has developed the ambition to compete with the United States to create a relationship of assured mutual vulnerability.
- The number of states with latent capabilities continues to grow, increasing the risk of rapid breakout and rapid deterioration of the regional security environment.
- Non-state actors see more targets of opportunity to purchase or steal a nuclear weapon or some key components.

Flashpoint leading to crisis contingency:

- Not relevant for shaping contingencies—in this contingency, none of the new possessors is on the brink of political collapse.

U.S. Objectives

U.S. leaders would want to:

- Dampen incipient pressures that might lead to an intensification of competition among new regional nuclear actors.
- Assure friends and allies that they need not meet new proliferation challenges with nuclear weapons of their own.
- Suppress illicit networks of all kinds.
- Buy more time *vis-à-vis* the next proliferators—and use it well.

What they would not want to do:

- Stand by idly while allies distance themselves from the United States because of the perception that others are losing faith in the credibility of the U.S. deterrent.
- Pay a high economic or political cost to inhibit further proliferation.

Losing would mean that:

- Regional security environments become much more competitive, as sketched out in the alternative future "new nuclear competitions."
- A loss of U.S. credibility and a loss of confidence in the United States as a security guarantor, with the result that friends and allies seek nuclear capabilities of their own as part of a distancing strategy from the United States.

Blue Concept of Operations

Political strategies:

- To induce regional actors to formalize self-accepted restraint in the further development of their nuclear weapons capabilities, as for example with agreements that constrain or prevent weapons testing, fissile material protection, weaponization, deployment, etc.
- To promote dialogue among regional actors aimed at building confidence by creating mutual understandings of the sources of instability in their unfolding nuclear relationships and by adopting mechanisms to manage those instabilities.
- To offer (or reiterate) positive and negative security guarantees where applicable.
- To safeguard against the possibility that other major international actors might exploit this contingency to counter-balance U.S. influence by maintaining a regular dialogue with Moscow, Beijing, and others on the issues at stake in regions of potential nuclear competition.

Military strategies:

- To compose U.S. strategic capabilities, such that no proliferator might come to believe that a relationship of assured mutual vulnerability can be created with the United States.
- Where a U.S. friend or ally ("partner") is a potential victim of a neighbor's potential development of more potent nuclear capabilities, to extend improved protection to that partner. Protection could encompass:
  - missile and other defenses, and/or
  - locally or regionally deployed strike capabilities, and/or
  - new basing arrangements for U.S. conventional forces

Needed Capabilities and Capacities

Capabilities:

- A strategic toolkit that is regionally deployed—missile defenses, strike systems (including possibly nuclear, depending on circumstance), and ISR deployed with allies.

Capacities:

- To surge additional strategic power into the region and to an ally in the event of a sudden disruption to the regional military balance.
- A nuclear force structure large enough such that no proliferator could conceive of achieving peer status.
- A missile defense structure capable of rapidly expanding, such that no proliferator could conceive of creating a balance of mutual vulnerability.

Contingency 5. Crisis: Intervene to terminate a regional nuclear war

Essential Features

- A handful of nuclear-armed states have moved beyond possession of minimum deterrents in an effort to gain nuclear war-fighting advantage over a neighbor and/or an outside intervening state.
- In at least one global sub-region, this has brought an intensification of competition for advantage and a series of political-military crises generated by leaders seeking to exploit the benefits of shifts in the military balance.
- The United States and some other major international actors continue to desire to play a role in managing significant international instabilities and threats to the peace.

Flashpoint leading to contingency:

- A crisis gets out of hand and escalates into nuclear employment by at least one state with the potential of more to come from one or both (or more).

U.S. Objectives

U.S. leaders would want to:

- Terminate the conflict at the earliest possible time.
- Prevent the further use of nuclear weapons.
- Where such use cannot physically be prevented, disincentivize such use by establishing that further attacks would generate international retaliation.
- Ensure that effective control is maintained at all times by the warring states of their nuclear arsenals and that there is no successful exploitation of crisis deployments by non-state actors seeking to acquire nuclear weapons.
- Punish a state (or, where possible in a discriminate manner, just its leaders) that has made use of nuclear weapons for purposes of aggression in order to teach a right lesson for the larger international community.

What they would not want to do:

- Stand by idly while the slaughter continues.
- Stand by idly as a nuclear aggressor consolidates a victory.
- Punish a state or its leaders who have used nuclear weapons for purposes of defense.
- Legitimize the use of nuclear weapons in any way.

Losing would mean that:

- The guarantors of international stability would be seen as impotent in the face of nuclear aggression.
- By-stander states would conclude that they need to significantly increase their reliance on nuclear weapons of their own because they have become legitimized as “conventional” tools of military power.

Blue Concept of Operations

Political strategies:

- Build consensus within the international community and especially with Moscow (and perhaps also Beijing and others) around the key elements of a strategy for rapidly terminating crisis.
- Build a similar consensus around the key elements of a strategy for achieving an effective settlement of the factors that precipitated crisis.

Military strategies:

- Visibly prepare to project strategic military power that lends credibility to conduct counterforce attack operations if necessary.
- Extend the protection of conventional forces to the party against which aggression has been committed.
- Ready a strong international response to the humanitarian and other problems associated with a localized nuclear war.

Needed Capabilities and Capacities

Capabilities:

- A strategic toolkit with:
  - exquisite local ISR
  - prompt non-nuclear strike
  - render safe
- A conventional force:
  - capable of limited operations in a contaminate environment
  - capable of render safe operations in a state with a moderately sized force

Capacities:

- To surge additional strategic power into the region—missile defense, close-in strike.
- To surge a conventional power projection force that stabilizes one or two countries in partnership with other stabilizers.

Contingency 6. Shaping: Extend nuclear deterrence to new security partners

Essential Features

- More states possess indigenous nuclear weapon development/production capabilities, and most of these are working to diversify and enlarge their nuclear arsenals in order to wield them more effectively.
- Some competitors (state and non-state) that are not known to possess nuclear weapons are improving their abilities to quickly acquire and utilize them by:
  - advancing indigenous capabilities to develop, produce, and field (states only), or
  - strengthening relationships with supportive factions within states that possess indigenous capabilities, and
  - increasing the ambiguity of their nuclear postures and confounding intelligence collection and assessment
- States in other regions have enhanced their latent indigenous capabilities, increasing concerns for spillover proliferation cascades.
- Nuclear weapons frequently play more prominent roles in geopolitical competitions for more actors (sub-state, trans-state, state, coalitions, and alliances) in a few regions, to:
  - exert influence over regional competitors
  - influence policies of major powers (United States, India, China, Russia, European Union, etc..) that impinge upon core regional strategic interests
  - deter or limit U.S. military power projection within the region
- Security partnerships/coalitions among nuclear weapons possessors and non-possessors seek to contain U.S. influence in the region.
- Extended nuclear deterrence is more prominent and varied:
  - offered by nuclear states to regional partners in direct competition with U.S. offerings
  - extended by allies independent of the United States to their partners in volatile regions

  - concerns with extension by anonymous proxy in support of coalition interests
- The potential for nuclear proliferation shortcuts is much higher, due to:
  - more potential source terms, both complicit and unwilling
  - diversity, unevenness of nuclear security practices and policies
  - complexity of potential pathways
  - more potential receptors with technical and operational sophistication
- International concerns for nuclear instabilities, cascading proliferation, and employment are at historic highs, having overtaken global warming and food production in priority.
- The wielding of nuclear weapons as a source of power and influence has not yet crossed the threshold of employment to produce nuclear detonations.

U.S. Objectives

U.S. leaders would want to:

- Prevent/defuse crises that could escalate nuclear employment potential.
- Establish international norms of responsible nuclear weapon ownership for: crisis management, surety (security, safety, use control) of nuclear weapons and material, transparency.
- Prevent further (horizontal) nuclear proliferation.
- Limit/reduce diversity and size of existing arsenals (dissuade further vertical proliferation, motivate rollback).

U.S. leaders would NOT want to:

- Go to nuclear war as an unintended consequence of U.S. or a partner's actions.
- Be compelled to cede major geopolitical position by a nuclear-armed competitor.
- Engage in nuclear signaling/brinksmanship without well-understood vocabularies for strategic communications.

- Be perceived as impotent to effectively dissuade/prevent:
  - vertical development of hostile competitors' nuclear weapons capabilities
  - further nuclear threshold crossing of friends and non-competitors
- Lose a security partner to a competitor's extended nuclear deterrence.

U.S. leaders might HAVE to:

- Be prepared to fight with non-nuclear means against a nuclear-armed adversary.
- Threaten U.S. nuclear engagement in a regional conflict to dissuade it from escalating to nuclear.
- Sacrifice U.S. nuclear capabilities/features or OCONUS military power projection posture in order to gain commensurate concessions in others' nuclear postures.
- Accept higher risks in some facets of nuclear national security to reduce risks in higher priority facets. (balanced risk management).
- Cede extended nuclear deterrence in a region to non-competitor states.

Losing would mean:

- Greatly increased risks and expectations of:
  - nuclear weapons employed in volatile regions
  - non-state nuclear weapon possession and use
- Broader recognition and acceptance of the legitimacy and effectiveness of nuclear weapons as tools of power and influence.
- Significant erosion of international norms and decorum in wielding nuclear weapons (actual, inferred, and threatened possession) for power and influence.
- Formation and strengthening of coalition(s) involving nuclear weapon possessors in strategic opposition to U.S. and allied interests (regional and global).
- Weakening of relative U.S. ability to exert power and influence affairs globally.

Blue Concept of Operations

Political strategies:

- To promote dialogue among regional competitors and their strategic partners to:
  - resolve sources of tensions that could potentially escalate to confrontation
  - establish crisis management and strategic communications protocols
- To induce regional nuclear competitors to participate in internationally binding treaties/conventions to:
  - resolve sources of tensions that could escalate to nuclear crises
  - verifiably limit/reduce nuclear arsenal growth and development
  - increase transparency of nuclear weapon readiness/alert postures
  - prohibit provocative behaviors that could escalate nuclear crises
- To foster the adoption of and contribute nuclear weapons and material surety "best business practices" and toolkits for possessors of nuclear weapons capabilities.
- To be prepared to offer substantive rollback of U.S. nuclear weapons capabilities/posture in exchange for commensurate measures among regional nuclear states.
- De-emphasize nuclear strike as the primary method of extended deterrence.
- Rely more explicitly on intertwining strategic interests and deploying non-nuclear strike and defensive resources as the primary instruments of extended deterrence.

Military strategies:

- To beef up non-nuclear strike and defensive resource sharing with partners (nuclear and non-nuclear) at risk from nuclear competitors.
- To "surge" extended deterrence to partners during escalating tensions as crisis management tool.
- To demonstrate U.S. capabilities and willingness to:
  - support nuclear posture transparency and crisis management regimes

- fight and win with non-nuclear means against nuclear-armed opponents
- engage in and decisively win asymmetric nuclear warfare, making the most effective use of the available arsenal, no matter what its specific features are

Needed Military Capabilities and Capacities

- OCONUS deployed/sharable non-nuclear strike and defense toolkits, and associated training, exercise, and support for extending deterrence by non-nuclear means.
- Rapidly deployable toolkits for "surging" nuclear components to extended deterrence partners that "plug-and-play" into general extended deterrent frameworks, *e.g.:*
  - transparent nuclear C3 overlay onto regional combat support network
  - "self-certifying" nuclear weapons for general purpose delivery vehicles
- Toolkit and operational proficiency to greatly increase U.S. capacity to absorb and recover from nuclear detonations, and strategic communications to convey this capacity.
- Forensic intelligence tools to rapidly establish culpability and roles in any ambiguously sourced nuclear detonation, and strategic communications to convey these capabilities.
- Technical capabilities and capacities to "tune" size and readiness posture of U.S. nuclear forces and stockpiles as geopolitical strategic conditions change.
- Nuclear force deployment and targeting planning contingencies to establish confidence, limits, and methods of U.S. nuclear deterrence for alternative force sizes/compositions. (Provide widest envelope of options for nuclear arms control negotiators.)

Contingency 7. Crisis: React to nuclear-backed aggression by a revolutionary, expansive power

Essential Features

- Saudi Arabia is taken over by al Qaeda, proclaiming the beginning of a new caliphate.
- Saudi missile and air forces are quickly armed with a modest number of nuclear weapons obtained from a prearranged unknown source.
- With this nuclear deterrent as protection, the expansive nuclear caliphate (ENC) threatens virulent terrorist campaigns to topple and incorporate the states of the Islamic world.
- This aggressive, nuclear-armed, ideologically radical state—initially controlling 25 percent of global oil production and reserves—poses a fundamental challenge to world order.
- Near-nuclear anarchy threatens from multiple sources: the unknown source of the ENC nuclear weapons may supply others, the ENC will embark on its own nuclear weapons program, and it will likely deploy these weapons to any additional states it comes to control.
- Other regional states may see these developments as requiring them to have nuclear forces.

U.S. Objectives

U.S. leaders would want to:

- Quickly intervene to overthrow the revolutionary government of Arabia before it can consolidate its political control.
- Destroy or disable ENC-ready nuclear forces before they could possibly be used.
- Prevent ENC nuclear weapons and materials from being smuggled or otherwise moved out of the country.
- Find, render safe, destroy or dismantle, and remove all components of any other ENC nuclear programs and activities that may exist.
- Prepare for and implement whatever consequence management actions would be suitable in the event of nuclear detonations or contamination.

U.S. leaders would not want to:

- Leave its allies and friends to fend for themselves against such a dangerous and aggressive enemy—especially as allies and friends seem likely to start crash efforts to acquire nuclear weapons.
- See nuclear weapons apparently confirmed as an effective shield for aggression against interests the U.S. had previously protected.
- Compromise the U.S. role and influence that has come with having been willing to pay high prices to protect allies and friends.
- Take preemptive/preventative actions that result in highly destructive nuclear strikes against U.S. or other forces or states.

Failing to successfully snuff out the ENC in its earliest days could mean:

- A difficult campaign to contain the ENC that could last for decades and would require creating and maintaining a cohesive defensive alliance until the ENC has been defeated or had lost its zeal for expansion.
- A race between the U.S. and allied efforts to create the New Triad and the other necessary capabilities to effectively neutralize ENC nuclear strike capabilities versus ENC efforts to establish nuclear forces that can ensure at least a few nuclear detonations on every allied state.
- Crash programs by threatened regional states to buy or create their own independent nuclear forces

Blue Concept of Operations

Political strategies:

- Project for allies, friends, and others the implications if the ENC is able to establish itself, and seek the broad support for immediate intervention.
- Assure U.S. regional allies and friends that they have the protection of U.S. nuclear deterrent forces, as well that of U.S. defenses and other conventional forces and capabilities.
- Jointly plan and prepare for the intervention:
  - managing the consequences for areas that suffer nuclear attacks and contamination
  - political stabilization of the liberated areas and the immediate support and restoration of their societies

Military strategies:

- Ensure that assembly, support, and operations of forces within the theater do not provide rich targets for ENC nuclear attacks.
- Employ information operations to conceal warning of when and if the attack on the ENC is actually coming.
- Prepare forces to seal the borders of the ENC and allow only thoroughly inspected and necessary cargoes to pass. Intercept and, if necessary, destroy vehicles attempting to avoid inspection.
- Attack and destroy the air and missile delivery systems and the key infrastructure that are known or suspected to be made part of ENC-ready nuclear force capabilities.
- Intervene with ground forces and overthrow the regime.
- Find and eliminate all nuclear weapons related facilities, weapons, and materials.
- Support stabilization and humanitarian aid.

Needed Capabilities and Capacities

- New Triad capabilities to protect U.S. forces and allied forces and populations from nuclear attacks and their worst consequences in order to keep the risks of the intervention tolerable.
- Supporting capabilities to seal within the ENC all nuclear weapons and materials until they can be captured and destroyed.
- Broad-area survivable surveillance systems allowing effective tracking for quick destruction of identified or likely ENC nuclear weapons and materials in transit.
- An intelligence picture of ENC nuclear capabilities that is sufficiently well developed and up-to-date to support attack and destruction of all its ready to launch nuclear weapons.
- Up-to-date training for U.S. and coalition forces on how to operate with maximum safety in the presence of nuclear contamination and other nuclear effects.
- Capabilities to find, recognize, and sanitize an entire state's nuclear weapons related activities within at most a few months.
- Safe, secure, and responsive nuclear forces that provide the deterrent efficacy that is available in this and other plausible contingencies.

Some Key Features of the Contingency Scenario

- If the U.S. and its allies do not have access to substantial amounts of high quality New Triad and supporting capabilities required by this kind of contingency, they could be forced to engage in an expensive and dangerous containment campaign that could last for decades.
- Limiting reactive nuclear proliferation by the many states who would feel threatened by the appearance of such a nuclear-armed challenger would be a major challenge for the U.S. and could lead to strong pressures on the U.S. to provide extended nuclear deterrence to a large number of states. Other nuclear states may have to be involved in providing nuclear security guarantees.
- The United States would need the acquiescence, if not the active support, of Russia, China, and NATO to carry out either early intervention against the ENC or the long containment campaign to follow.
- The highly aggressive nature of the ENC and its threat to the majority of global oil production and reserves seems likely to guarantee exceptionally broad international support for intervening and, if necessary, containing the ENC.

Contingency 8. Shaping: Contain a hostile coalition

Essential Features

- Proliferation in the Middle East has coincided with some partial al Qaeda success in casting out "apostate regimes," but not full progress in restoring a unified caliphate.
- Many of the successor regimes are hostile to the United States and its role in the region and enjoy broad popular support to aggressively confront the U.S. presence while they also attack the residual moderate governments the United States seeks to protect.
- Those regimes sometimes find it useful to cooperate to project power and other times are divided by non-identical interests.

U.S. Objectives

U.S. leaders would want to:

- Frustrate their efforts to continue revolutionary activities against moderate governments that they oppose.

- Continue economic activity with those in the region remaining engaged in the globalized economy. This would include energy access wherever possible.
- Protect against and punish attacks on U.S. forces in the region and other forms of U.S. presence—political, economic, and cultural.
- Exploit differences of interest among the coalition to frustrate their efforts to find consensus.
- Challenge their efforts to extend deterrence to additional potential partners.
- Reassure the leaders of moderate states that feel threatened by this coalition that they need not resort to nuclear forces of their own to safeguard their societies.

What they would not want to do:

- Acquiesce to efforts by the leaders of the coalition to extend their revolutionary purposes.
- Stand by idly as they make war against Israel and other free societies in the region.

Losing would mean that:

- Al Qaeda would enjoy continued successes in its long war for Islamic renewal (as it sees it).
- A significant restructuring of global power, with significantly reduced freedom of maneuver for the United States and a significant loss of stature as its power and/or will are seen increasingly as unable to withstand the jidhadi WMD threat.
- Emboldened jihadi leaders more willing to run the risks associated with opening their WMD arsenals to like-minded non-state actors.

Blue Concept of Operations

Political strategies:

- Create and lead a counter-coalition of states in the region seeking protection and others outside the region willing to extend protection.
- Foster and exploit a convergence of worldview among the major powers to ensure that none "defects" to become a supporter of the coalition in a bid to counter-balance U.S. hegemonism.

Military strategies:

- Build up and supplement the military power of states in the Middle East and nearby regions seeking protection from the coalition.
- Secure the U.S. homeland from missile and unconventional attack.
- Draw a strong cordon around the coalition so that its nuclear weapons, materials, and technologies do not leak (or get sent surreptitiously) to others beyond the region.

Needed Capabilities and Capacities

Capabilities:

- Non-strategic toolkit, *i.e.*, stout conventional defense for U.S. allies in the region, including from terrorist attack (including nuclear).
- Strategic toolkit, *i.e.,* strike capabilities that integrate local and global in a continuum of escalation options.
- Protection capabilities that:
  - protect key allied capitals and capabilities.
  - fully protect the United States from coalition missile attack or significant terrorist operations so that it is free to intervene locally without fear of escalation to attack on CONUS.

Capacity

- To project power conventionally in an unfolding crisis.

Part IV

Unconventional Operational Concepts and the Homeland

Chapter 13. One Game: Defending the Homeland

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

> The Department of Defense must change its conceptual approach to homeland defense. The Department can no longer think in terms of the "home" game and the "away" game. There is only one game. … Defending the U.S. homeland—our people, property, and freedom—is our most fundamental duty. Failure is not an option.[1]

Part IV of this volume focuses on the implications to DOD of adversary attacks on the homeland, as an instrument of war, with an eye toward the particular challenges that can arise if an "away" game is in progress as well.

War on the Domestic Front

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

A series of interviews on the Chinese book *No Limit Warfare* quotes one of its authors, Senior Colonel Qiao Liang, as saying "If we were to try to use high technology to counter U.S. high technology, that would in fact land us in the U.S. trap. We could never catch up to them on that track. So for a poor and weak country to try to use high technology to counter the United States would in fact be like throwing eggs against a rock."[2]

The refusal to adopt a symmetric approach to war also goes beyond the basic issues of military strength and operational doctrine. The nations and non-state

---

1. *Strategy for Homeland Defense and Civil Support*, Department of Defense, June 2005. See also Appendix IV-B for relevant excerpts of this strategy.
2. Sha Lin, "Two Senior Colonels and No-Limit War," *Beijing Zhongguo Qingnian Bao* in Chinese, Foreign Broadcast Information Service translation, June 28, 1999.

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

Many scenarios come to mind where U.S. adversaries view an issue as threatening life and/or state, while the United States has relatively little at stake. Under those circumstances, adversaries will often attempt to influence U.S. foreign-based activities.[3] Simply put, they could execute innovative asymmetric approaches to shape U.S. national will in order to:

- Deter U.S. entry into any foreign affair of no perceived immediate national security impact or no perceived threat to national sovereignty by threatening disproportionate asymmetric damage to the United States.
- Halt U.S. entry or accelerate a withdrawal if the nation decides to employ forces in a foreign action.
- Delay any U.S. decision to act by executing a range of asymmetric approaches. Many unconventional homeland approaches, particularly information operations, will also be very difficult to trace. Since the U.S. political process requires a high degree of certainty for legislated action, the nation's response could be delayed and diffused until it is simply too late to act effectively.

Moreover, U.S. military leadership has had difficulty embracing the concept of a two-front war, with one of the fronts being the homeland battlefield. Since the end of the Indian Wars in 1891, the United States has treated warfare as an "away game." Attacks on the U.S. homeland (except by symmetric capabilities of ballistic missiles and long-range bombers) have been unthinkable due to the geographical isolation of the Americas and the strength of U.S. naval and air forces. The rise of global travel, commerce, and information flows has radically changed traditional American isolation. America's sea and air power still make conventional mass invasion unlikely, but **as military modes shift from concentrated industrial**

3. Kenneth F. McKenzie, Jr., "Where Are Our Asymmetric Vulnerabilities," *The Revenge of the Melians: Asymmetric Threats and the Next QDR*, McNair Paper 62, 2000, Institute for National Strategic Studies, National Defense University, page 3.

warfare to distributed wars among populations, domestic disruption is likely. Effects-based targeting, used with great success by U.S. forces to inflict maximum impact with minimum force, is similarly useful to aggressors seeking to distract the U.S. population; disrupt infrastructure, commerce, and government; and delay support to U.S. military forces operating abroad.

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

In light of these potential consequences, the United States should expect future asymmetric attacks to focus on manipulating its populace—by attacking either critical infrastructure targets or the populace directly. The attacks would generally be tactical, but with strategic effect. If the population internalizes the terror associated with future attacks and begins to believe they are at risk in the normal course of their daily lives, then the will of the nation could be shaped. Additionally, if the threat involves weapons of mass destruction (WMD), the resulting image of massive casualties would elevate the effect to even higher levels of fear. If terror is reinforced by successive events, the American people could come to believe that they have no control. Then the real intent of these attacks would surface. A perception could emerge that personal security would only be regained by a decision to withdraw from a distant conflict (with no clear connectivity to the United States). The result would be achieved. Figure 4-1 captures these factors.

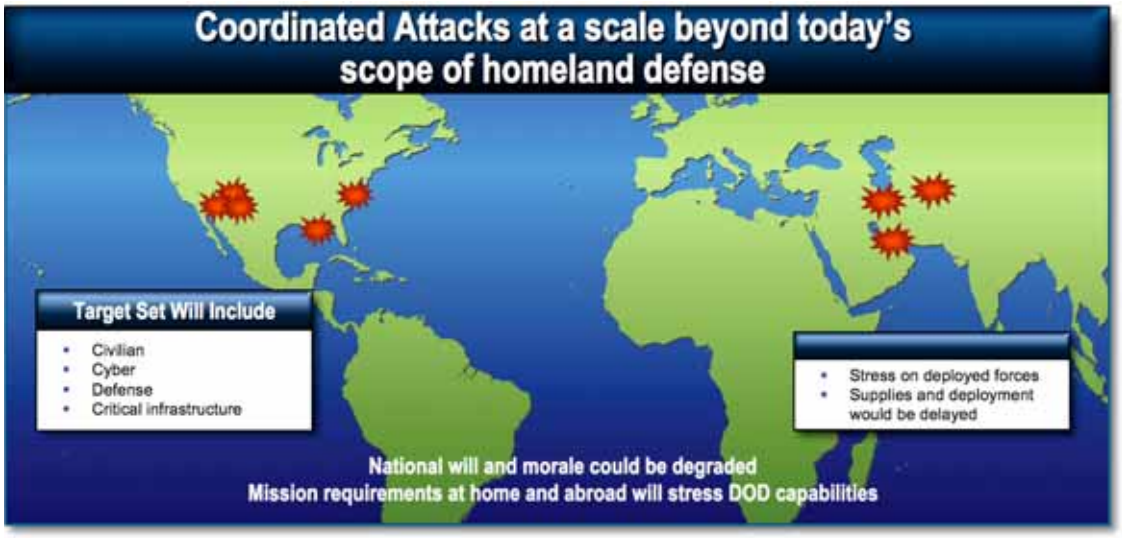


Figure 4-1. The "One Game" Approach of Future Capable Adversaries

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

Consequences of Catastrophe

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

- **failure of critical infrastructure**—lack of essential goods and services (Table 4-1)
- **insufficient professional resources to deal with multiple catastrophes**—response forces (Federal Bureau of Investigation, National Guard, DOD, DHS, police, fire, American Red Cross, and others) sized to handle only one or two crises at a time
- **national will hard to focus**—public anger manifested through misguided, vigilante-style attacks
- **impaired ability of national, state, and local governments to govern**—lack of, or confusing, communications; fractured local authority; insufficient, disorganized emergency response

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

- **Flight.** Remaining in place would prove untenable for many people for actual or perceived reasons.
- **Breakdown of mutual aid agreements.** Resource-intensive incidents are typically handled through mutual aid agreements within the National Guard, first responder, and medical communities. When under attack, however, leaders in unaffected regions might opt not to support interregional common aid agreements and to conserve their resources in case they are needed locally.
- **Breakdown of civil order.** Looting, vigilante actions, gang violence, riots, and civil disobedience would further stress first responders.
- **Failure of quarantine.** Many will be reluctant to stay confined.
- **Hoarding.** People will rush to amass excess goods to stock up after the attack.
- **"Shoot your neighbor."** As people perceive the social and civil situation deteriorating, they will escalate the force they use as a first resort to protect home and family from interlopers ("shoot first, ask questions later").
- **Rampant rumors.** Media will promulgate messages from many sources without confirmation.

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

Table 4-1. Examples of Consequences of Attacks on the Infrastructure

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

Responses will be further exacerbated because of the evolution of U.S. society. Dependence on "just-in-time" centrally managed, networked supplies of water, power, food, communications, and transportation leaves the United States extremely vulnerable to an effects-based attack. Additionally, over time, mobility of the American population has resulted in a breakdown of extended family and community-based societal structures that once provided informal local leadership and community organization and support. In twenty-first century society, many do not know their neighbors, let alone have the capability or capacity to form effective

support networks for long periods of time. Skepticism of authority makes governance in a disaster difficult, while the public nevertheless expects governmental assistance to mitigate the aftermath.

Implications for DOD

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

1. How well does DOD (and others) understand what is expected of it? How well prepared is DOD to execute across a range of homeland defense missions?
2. Given the "one game" nature of the capable adversary, can DOD have high confidence that it will be able to ensure deployment and supply in whatever set of missions it undertakes within and from the homeland?
3. Success in both the current scope of homeland security and defense, and the more stressing environment of the future, depends on teaming and integration unprecedented in recent history: across and among all levels of government; with and across the private sector; down to individual actions for preparedness. Where does the nation, and especially DOD, stand in building the "one team" needed for success?

Chapter 14. DOD Roles and Responsibilities

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

- Homeland security. "Concerted national effort to prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." DHS is the lead agency to prevent terrorist attacks within the United States. The Attorney General leads law enforcement to detect, prevent, and investigate terrorist activity with the United States.
- Homeland defense. "Protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression." DOD is responsible for homeland defense.
- Defense support to civil authorities (civil support). "DOD support for domestic emergencies and for designated law enforcement and other activities." This occurs by direction of the President or Secretary of Defense.

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

DOD: Support versus Lead

Engaging in an overseas deployment, while at the same time responding to a significant scale of attacks in the homeland, will stress DOD capabilities. The public will expect DOD to defend the homeland and DOD will be ordered to participate, regardless of the intentions of the military leadership prior to the incident—engaging in incident prevention, mitigation, and remediation through the U.S. domestic political process. Legislation and directives support this approach. Further, the 2005 National Defense Strategy clearly directs the military leadership to properly shape, size, and globally posture to: 1) defend the U.S. homeland and 2) operate in and from the forward regions.

Homeland defense currently includes a range of activities in CONUS. Often, DOD will be called on to provide support to the civil government, but its activities can also progress to a leadership role in response, and consequence management efforts if and when the scope of attack is sufficiently severe. The concept described is notionally depicted in Figure 4-2, in which the transition from a supporting role by principally DOD reserve component forces shifts to one of leadership at significant attack levels involving reserve and active duty forces.

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

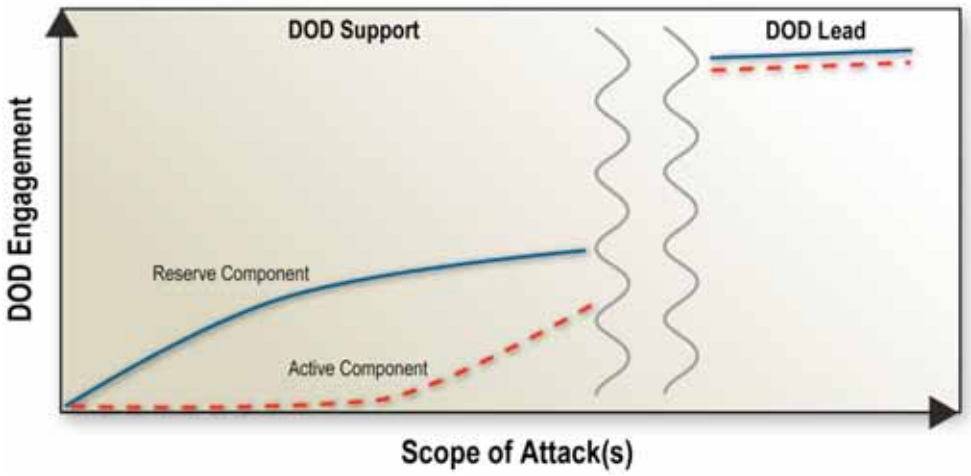


Figure 4-2. Notional Transition of DOD Forces from Support to Lead

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

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

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

Legislation and Directives

The study found nothing in legislation, directives, or other documents to prevent a more aggressive posture and engagement by DOD. On the contrary, the documents set expectations for DOD preparedness, whether as supporting agency (expected in most situations) or supported agency (shift to homeland defense). Starting with the Constitution, the federal government is to "provide

for the common defense." The Stafford Act allows for use of the military for disaster relief operations at the request of the state governor, and further defines three scales of involvement: essential assistance (up to 10 days), emergency, and major disaster.

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

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

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

- in support of natural disasters (its immediate assignment of resources in the aftermath of the 1906 San Francisco earthquake; its immediate deployment (unrequested) of a hospital ship to New Orleans after Katrina)
- to preserve public order where other options are unavailable or overwhelmed in order to carry out governmental operations
- in sudden and unexpected civil disturbances, disasters, or catastrophes when civil authorities can no longer maintain control
- to provide catastrophe relief without or before imposition of the Stafford Act, on a temporary basis
- to undertake some specific law enforcement activities

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

DOD Capabilities for Homeland Security and Defense

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

Nonetheless, DOD leadership, both civilian and military, has been slow to accept this apparently expanded scope of responsibilities because with it comes significant resource demands and financial costs that are not likely to be adequately supported. The study determined that a focus on specifics was needed in order to motivate the Department's leadership to focus on priorities. Table 4-2 offers an illustrative list of those specific roles and missions that are generally accepted as DOD responsibility and those that are not.

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

Table 4-2. DOD Responsibilities for Homeland Defense

Reasonable	Unreasonable

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

Table 4-3 provides a rough assessment of the key capabilities DOD should have in order to execute the responsibilities listed in Table 4-2. The assessment includes not only a "grade" and trend (in the far right column labeled "How Good"), but also a breakdown to better highlight progress (or lack thereof).

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

Table 4-3. Capability of DOD to Perform Expected Roles

DOD Capacities for Homeland Security and Defense

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

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

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

Table 4-4. DOD Support to Hurricane Katrina

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

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

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

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

- Fifty percent of forces in Iraq in 2006 were guardsmen.
- Thirty-three percent of the National Guard deployed in Iraq or for Katrina in September 2005.

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

The "worst case" model would be the local first responder to a specific incident, who is then activated by the state governor as a member of a National Guard unit (to respond to the same incident, another incident in the state, or under EMAC to another state), and whose unit is subsequently called to federal status to provide homeland support or to engage in military operations overseas. Figure 4-3 illustrates the dilemma. As a result, it is critical to planning at every level that the extent of "double counting" be quantified at a higher level of resolution, and its effects on planning assumptions understood.

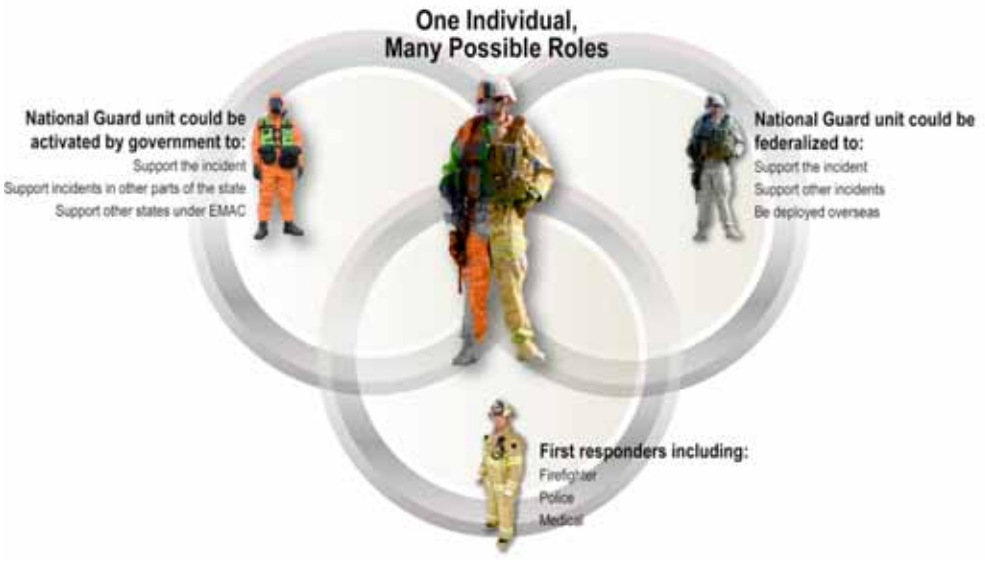


Figure 4-3. Double and Triple Counting of the Reserve Components

RECOMMENDATIONS: DOD ROLES AND RESPONSIBILITIES

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

1. **The Secretary of Defense task the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD [HD&ASA]) to revise and implement DOD policies and procedures covering homeland defense requirements.** This tasking should include the clarification of relationships, roles, and missions of all the elements (federal agencies, civilian and private sectors, state and local responders, and law enforcement) of homeland defense at a level of specificity highlighted in this chapter. Clarification of this sort would go far to eliminate the uncertainty and/or confusion about what is expected of DOD and what others can indeed expect of DOD. The scope should include contingencies where DOD assumes the lead response role in the homeland. Only those policies and procedures that lower the barriers to planning, exercising, information sharing, cooperation, and coordination across the entire homeland defense community should be approved.
2. **Service Chiefs and the National Guard Bureau assess force requirements and adjust, adapt, and/or expand force structure to meet the "one game" demands of the future.** Force structure should be built not just on the regional command war plans for overseas operations, but also on those being developed by U.S. Northern Command for homeland operations. The effort will involve the development of accurate databases to understand the civilian skills and job commitments of the reserve components in order to assess and address the "double counting" issue. It will also require close planning and coordination with the Service Secretaries across the spectrum of doctrine, organization, training, materiel, leadership and education, personnel, and facilities in order to ensure that shortfalls are addressed.

Chapter 15. Assuring Deployment and Supply

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

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

This chapter examines how well the nation is prepared to meet the simultaneous demands of fighting a war both in the homeland and abroad. The assessment is based on the resiliency of the nation's critical infrastructure and functions, DOD processes and status for ensuring resiliency, DHS processes and status for protecting the nation's critical infrastructure, DOD preparedness (supply, logistics, installations), as well as family and individual preparedness.[4]

Critical Functions and Infrastructure

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

- What military missions and functions must be assured from the homeland?
- What assets and operations are critical to that assurance?
- How do we figure that out?

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

- Who is responsible for doing what (DOD, DHS, others with key infrastructure responsibilities), and do we understand how the system expects to function under stress?
- What will be the availability of critical national assets and capabilities?
- What competing demands will be made on the military and National Guard?
- How do DOD and the nation measure its preparedness—or readiness?

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

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

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

chapter. The protection challenge for the U.S infrastructure is significant, as illustrated in Table 4-5.

Table 4-5. Size Indicators of Some Critical Infrastructure and Key Assets

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

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

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

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

DOD Approach and Progress for Assuring Defense Critical Functions

DOD is beginning to make progress in identifying what is critical through the Defense Critical Infrastructure Program (DCIP) within ASD (HD&ASA), supported by the Naval Surface Warfare Center in Dahlgren, Virginia. Together with the combatant commanders, a "mission assurance" process is being developed and implemented—a process that incorporates many of the recommendations of a prior DSB study regarding risk management and mitigation.[5] The process focuses first on identifying critical functions and capabilities, followed by identifying and assessing those few assets or facilities necessary to ensure the functions or capabilities. The process also provides guidance to assess a number of critical infrastructures "outside the fence" on

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

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

- Combatant commanders identify critical capabilities, missions, and functional networks (41 have been identified as in the most critical tier 1 category; several hundred are in the tier 2 category).
- The critical capabilities, missions, and functional networks are decomposed into defense critical assets that are assessed against threats, hazards, and vulnerabilities (risk assessment). Risk of loss is assessed and mitigation actions are proposed (protect/harden, duplicate/backup, relocate, and others).
- The Services then analyze the results and the proposed mitigation actions (N.B.: The Department is at this stage now).
- Finally a senior group (the Deputies Advisory Working Group or its equivalent) adjudicates differences and prioritizes for resource allocation.

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

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

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

The study judged that the list appeared logical, but neither complete nor consistent in the application of the tier criteria.[6] Recognizing that it is a process in its early stages, the DSB nonetheless believes that more effort must be applied to get it right and complete.

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

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

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

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

DHS Process and Status for Critical Infrastructure Protection

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

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

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

the DHS has identified 36 "Tier 1" assets and over 2,500 "Tier 2" assets.[7] These include several identified by DOD. How the tier criteria are developed and applied were not clear (to this study team, at least) nor were the processes by which the SSAs or SCCs influenced choices.

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

Information Assurance

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

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

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

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

Logistics

The DOD logistics system has shown significant improvement in its ability to produce a rapid and precise response (Figure 4-5). Examples include:

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

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

The U.S. industrial base produces the vast majority of the material required to support the Department of Defense. There are many critical commodities and items that are essential for DOD to accomplish its mission, both abroad and at home. Examples include: meals ready to eat, subsistence, medical, fuel, and spare parts for critical weapon systems. Many of these items (especially critical spare parts) are produced by sole-source companies or by companies with limited competition. Strategies have yet to be developed to assure the availability of these materials in the event of attacks on the homeland. Such a strategy should include:

- a comprehensive list of critical commodities and items, updated and (re)prioritized on a routine basis
- assessment and assurance of transportation routes required for their delivery from industry to DOD facilities
- assessment and assurance of the sources of the critical commodities and items (for example, through developing alternative sources of supply for these items by contracting for the capability, but not necessarily the actual production)

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

Each military service and the Defense Logistics Agency have either implemented or are in the process of implementing state-of-the-art commercial

logistics information technology systems. However, no organization has been given the leadership role to ensure that these systems are interoperable and secure. These new logistics IT systems remain vulnerable to attacks because, by design, they must remain accessible to the commercial industrial base. DOD needs to develop a team of experts from both within DOD and the commercial sector to address this vulnerability.

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

The weakest segment of the DOD supply chain is often described as the "last tactical mile." In the logistics context, this represents the tactical movement and distribution of material once in-theater to its actual use by the warfighter. There has not been a coordinated effort to implement a single asset visibility system for the "last tactical mile" that would track and report consumption to the DOD national provider or to the end user. ODUSD (LM&R) should coordinate this effort. Visibility of material in the "last tactical mile" must be an element of a joint logistics enterprise-wide visibility system, which uses a common data architecture, has authoritative sources of data, and is available 24 hours a day, 7 days a week.

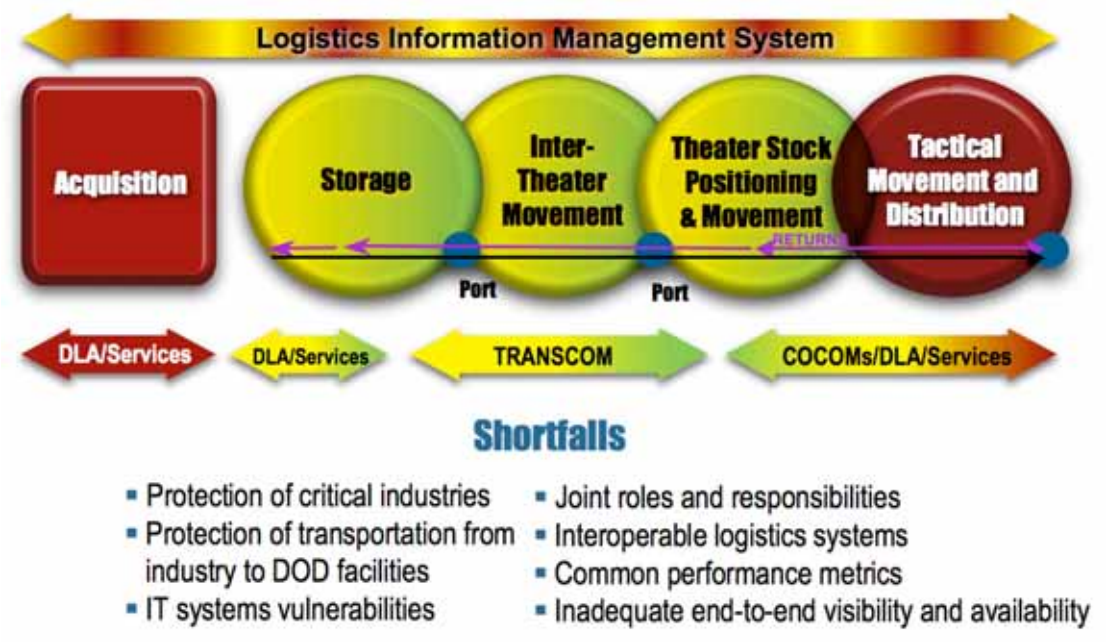


Figure 4-5. Assessment of Robustness of DOD's Supply Chain

Military Installation Protection

In addition to ensuring supplies from a robust private supply and internal distribution system, DOD must also assure the security of the forces it expects to deploy. The first step is assuring the inherent security of the installation itself. The military services each approach base security and force protection differently, but almost all of them plan on the support of local community emergency response resources in a serious incident (this being a consequence of outsourcing in this domain).[8] These civilian capabilities will not be available if the incident is an attack of a serious-enough scale. In particular, the study worries about the consequences of a WMD attack in terms of both the technical and operational shortfalls in both military and civilian communities.

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

A previous DSB task force assessed best practices for protecting U.S. military installations and recommended various approaches to enhancing security and protection of these facilities.[9] Principal findings included:

- DOD has many facilities that are vulnerable to the threats considered in the study, but a rational focus should be on protecting its critical military mission capabilities and functions (as opposed to installations and facilities).
- Interdependencies of DOD facilities upon non-DOD infrastructure are not entirely known.
- DOD, until recently, lacked policies and standards to guide installation commanders in securing, or creating contingencies around, infrastructure on which they depend.
- DOD Directive 3020.40, "Defense Critical Infrastructure Program," signed August 2005, assigns DCIP responsibilities at all levels across the department.

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

- ASD(HD&ASA)/DCIP lead efforts to characterize defense sector infrastructure dependencies, develop risk mitigation guidance, and establish uniform DCIP standards (which is now underway, as outlined previously in this chapter).
- Services develop and implement plans to mitigate risk across owned installations; provide annual update to the Deputy Secretary of Defense.
- Installation commanders develop local assessment of dependencies and implement risk mitigation plans consistent with guidance and standards.
- Commander, U.S. Northern Command develop understanding of dependencies and risk mitigation by Services in the continental United States; other combatant commanders do the same in their respective areas of responsibility.
- DOD through ASD(HD&ASA)/DCIP monitor, collect, and share examples for installation preparedness as a basis for judging risk mitigation decisions within the previously recommended risk management program.

---

9. Report of the *DSB Task Force on Critical Homeland Infrastructure Protection*, January 2007.

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

Family and Individual Preparedness

Every mission begins at home.[10]

No amount of planning, training, and exercising can totally protect against homeland attacks. The second line of defense, as discussed in the previous sections of this chapter, must be to harden government and civil organizations and critical functions against the effects of an attack and/or to assure an orderly recovery. The third line must be preparation of individuals and their families to withstand the impacts of a national catastrophe.

The study team was reminded of the many examples where individual preparedness proved pivotal in mitigating the consequences of a natural disaster, and the strong role it played in the early days of the Cold War. The effectiveness with which Florida is able to contend with hurricanes, having learned valuable lessons from Hurricane Andrew, especially when compared to Louisiana's inability to deal with Katrina, shows how state and local preparation can blunt a disaster's impact. The preparedness of the Swiss population to hunker in place during military emergencies is another good example of preparedness. More often, however, unless catastrophe is a near-term reality, most major domestic preparedness programs are likely to fail because of competing, short-term resource needs. Katrina was widely and credibly forecast for many years, yet Louisiana remained poorly prepared (Table 4-6).

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

Table 4-6. Progress Toward Preparedness

In the aftermath of Katrina, President Bush demanded that "we find out the lessons, that we learn them, and that we fix the problems, that we take every action to make sure America is safer, stronger, and better prepared." The lessons referenced were those enumerated in The *Federal Response to Hurricane Katrina Lessons Learned*, 2006. These included planning, resource management, evacuation, situational awareness, communications, and coordination. These lessons are not new; in fact they have been repeatedly observed and stated:

Hurricane Katrina, 2005

Command centers in the Department of Homeland Security (DHS) and elsewhere in the Federal government had unclear, and often overlapping, roles and responsibilities that were exposed as flawed during this disaster … This lack of coordination at the Federal headquarters-level reflected confusing organizational structures in the field. … Furthermore, the Joint Field Office (JFO) staff and other deployed Federal personnel often lacked a working knowledge of National Incident Management System (NIMS) or even a basic understanding of ICS.

The Federal Response to Hurricane Katrina Lessons Learned, 2006:52

September 11, 2001

It is a fair inference, given the differing situations in New York City and Northern Virginia, that the problems in command, control, and communications that occurred at both sites will likely recur in any emergency of similar scale. The task looking forward is to enable first responders to respond in a coordinated manner with the greatest possible awareness of the situation. …. Emergency response agencies nationwide should adopt the Incident Command System. When multiple agencies or multiple jurisdictions are involved, they should adopt a Unified Command. Both are proven frameworks for emergency response.

The 9/11 Commission Report, 2004:315,397

Oklahoma City Bombing, 1995

The Integrated Emergency Management System (IEMS) and Incident Command System (ICS) were weakened early in the event due to the immediate response of numerous local, state and Federal agencies, three separate locations of the Incident Command Post (ICP), within the first few hours, and the deployment of many Mobile Command Posts (MCPs), representing support agencies.

After Action Report: Alfred P. Murrah Federal Building Bombing, 2003:3

Hurricane Andrew, 1992

The Committee heard substantial testimony that the post-disaster response and recovery to Hurricane Andrew suffered from several problems, including:

Inadequate communication between levels of government concerning specific needs;

- Lack of full awareness of supply inventories and agency capabilities;
- Failure to have a single person in charge with a clear chain of command; and
- Inability to cut through bureaucratic red tape.

Governor's Disaster Planning and Response Review Committee Final Report, 1993:60

These shortfalls in communications are repeatedly identified in a multitude of after-action reports. Recent catastrophic events have resulted in many legislative actions and directives to address these problems:

- Homeland Security Act of 2002
- Homeland Security Presidential Directive-5 – Management Domestic Incidents
- Homeland Security Presidential Directive-7 – Critical Infrastructure Identification, Prioritization & Protection
- Homeland Security Presidential Directive-8 – National Preparedness
- Post Katrina Emergency Management Reform Act of 2006
- Intelligence Reform and Terrorism Prevention Act of 2004
- Implementing Recommendations of the 9/11 Commission Act of 2007

As evidenced by the enormous scope of the recent 9/11 legislation, it is widely perceived that little progress has been made in addressing these problems. Why don't we learn? Why are these problems a challenge to military operations?

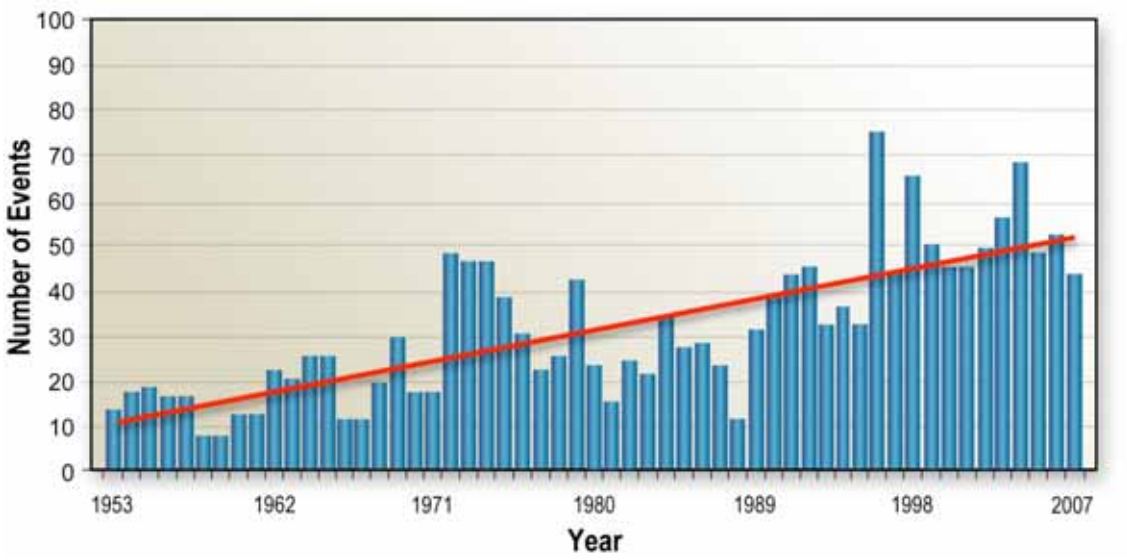
Whatever measures are taken to deal with domestic catastrophes, they all must have intrinsic value—improved efficiency, greater safety, better level of service, less cost. Government should not be the principal source of resources, but should lead in encouraging improvements, providing guidelines, and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

Resiliency

According to FEMA, there have been over 1,700 federal disaster declarations issued since 1953, with an annual average of 31 events per year. The number of events during the last decade has exceeded this average (Figure 4-6). A capable enemy could take advantage of any one of these annual events as an opportunity to launch an attack while U.S. resources are strained and leadership distracted.

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

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



Source: FEMA, August 2007; http://www.fema.gov/news/disaster_totals_annual.fema

Figure 4-6. Number of U.S. Disaster Declarations

This reality has a sobering consequence. Even in the best of worlds, with all public and private emergency response and recovery systems operating as designed, help may not be there when military members and their families desperately need it. Evidence of this has been dramatically illustrated during countless disaster relief operations. To cite one example, in January 1998, the worst ice storm in New York State's recorded history paralyzed an area in a northern region of the state the size of Vermont, affecting over 18 million acres.[11] Twenty thousand utility poles had collapsed, the power grid was out of service for weeks, fallen trees made most roads impassable, and citizens were left to survive in the sub-freezing temperatures with only the food, water, and other supplies they had on hand.

For most of them, especially those with children, the experience was a terrible ordeal. Tragically, some did not survive. But for a few, the experience was no more than an inconvenience. These were usually older people who had grown up in a time when self-reliance was an accepted way of life. They had stockpiles of water, food, fuel for woodstoves, and medicines. One elderly

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

couple replied to a rescue team that came to their home to offer assistance, "Go help somebody else, we're good here until Spring."

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

A Culture of Preparedness

Instilling and promoting a culture of preparedness can provide both physical and psychological benefits to members and their families. There is much that can be done without great expense or effort to better prepare for both natural and man-made disasters.[12] Greater hazard awareness, training, home storage, and family communication and evacuation plans can provide greater peace of mind, strengthen emotional resiliency and empower DOD families to carry on through a disaster. Preparedness also reduces the impact of a crisis and likelihood that these families will have to depend only upon the emergency relief infrastructure. Self-sufficiency also empowers members and families to help others and set an example the community can follow.

Most emergency preparedness guidelines encourage a minimum of 72 hours worth of supplies per individual for use until authorities are able to restore order and marshal emergency services.[13] However, experience has shown, and future disaster estimates (such as for a pandemic flu) indicate, that individuals should be prepared for much longer periods (two weeks to several months). Over time, individuals and families can build up their own home storage supply of food, water, medicines, and other necessary items including financial reserves and prudent debt avoidance.

Fortunately, preparedness at the individual and family level is the cheapest and perhaps most achievable of strategies to enable the nation's military

---

12. Events include such things as floods, mudslides, hurricanes, tornados, fires, severe snow or ice storms, earthquakes, volcanoes, infectious disease outbreaks, severe power and fuel outages, hazardous chemical releases, nuclear or radiological incidents, acts of terrorism and/or civil disturbance.
13. Helpful Resources: DHS Be Ready, http://www.ready.gov/; FEMA, http://www.fema.gov/areyouready/, http://www.pandemicflu.gov/plan/tab3.html; Citizens Corps, http://www.citizencorps.gov/; CDC, http://www.bt.cdc.gov/; Florida Division of Emergency Management, http://www.floridadisaster.org/bpr/family%20preparedness/ index.htm

community to continue operations during times of adversity. The idea of individual and family preparedness was reinforced by a group of noncommissioned officers (NCOs) with whom a part of the study team met: "We can't protect our country if we can't protect ourselves."

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

RECOMMENDATIONS: ASSURING DEPLOYMENT AND SUPPLY

The recommendations offered here are restricted to those that affect DOD, although there are many related items that DHS should address, as well. **The first set of recommendations is associated with ensuring deployment and supply. Toward that end, the Secretary of Defense, should direct:**

- OSD ASD (HD&ASA)/DCIP to extend the mission assurance process to the defense industrial base and recommend approaches for addressing shortfalls.
- USD (AT&L) to work with defense industrial base owners to develop and implement corrective action plans.
- OSD ASD (HD&ASA)/DCIP to develop a prioritized action plan for addressing identified risks to DOD owned assets.
- U.S. Northern Command to lead the integration and analysis of defense agency critical functions, within the framework identified by ASD (HD&ASA)/DCIP, to enhance mission assurance, and to be the principal advocate for prioritized resource needs and shortfalls.
- Service secretaries to fund actions for mission assurance in owned functions.
- USD (AT&L)/LM&R to ensure resourcing of logistics shortfalls:
  - to assure sources of supply and movement to DOD depots
  - to eliminate the last tactical mile issues
  - to make the information management system interoperable, robust, and resilient to attack, from both within and outside

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

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

- Reinforce message via NCO leadership academies, on-base medical community, Armed Forces Network, unit town-hall meetings, movie/TV celebrities, veterans' organizations, and other similar venues.
- Assure base commanders export this capability to adjacent civilian communities.

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

This message could be reinforced through NCO leadership academies, on-base medical community (pan-flu education), Armed Forces Network, unit town-hall meetings, celebrity endorsements, motivational speakers, promotional sales (at cost) via commissaries, as well as veteran and community organization involvement. DOD could also partner with other organizations such as the DHS-sponsored Citizens Corps on how best to prepare and educate members and their families.[14] According to FEMA, there are over 2,200 Citizens Corp Councils serving areas containing 75 percent of the total U.S. population.[15] Commissary stocks of long shelf-life items should also be increased. A significant collateral benefit (according to the NCOs) would be enhanced morale for members serving in assignments that separate them from their families.

---

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

Chapter 16. Building the National Team

"One Team"

The third dimension of the study's assessment of homeland defense addressed the status of the "national team" and DOD's involvement. As stated in Chapter 13, success in both homeland security and defense, whether against terrorism or more stressing peer-generated environments, demands a level of partnership and integration between and among all levels of government as well as with the private sector. In its investigation, **the study team found an almost exclusive focus in national strategy and plans on terrorist attacks**, most often a single event, even if distributed in nature (as a bio or cyber attack might be), **rather than on the more capable adversary envisioned in this study**.

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

The Homeland Security Team

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

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

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

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

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

Interagency

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

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

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

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

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

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

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

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

Federal-State-Local

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

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

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

Y2K Information Reporting and Communications

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

- common, consistent operational picture to the President and decision-makers
- owners to fix their own problems at the lowest level
- use of existing agencies and capabilities; supplement where needed
- federal assessment, assistance where national interest, life, and safety merit
- Federal Response Plan used as the model
- individual agencies required to validate data they supplied
- information content planned, templated, routinely transmitted; significant events transmitted on an exception basis
- one voice to the nation

The model for the operation of the Information Coordinating Center is captured in Figure 4-7. The interagency and intergovernmental coordination and teamwork leading up to the rollover and immediately thereafter was commendable, and could provide a valuable model for information-sharing in high alert and/or crises for today's homeland security and homeland environment.

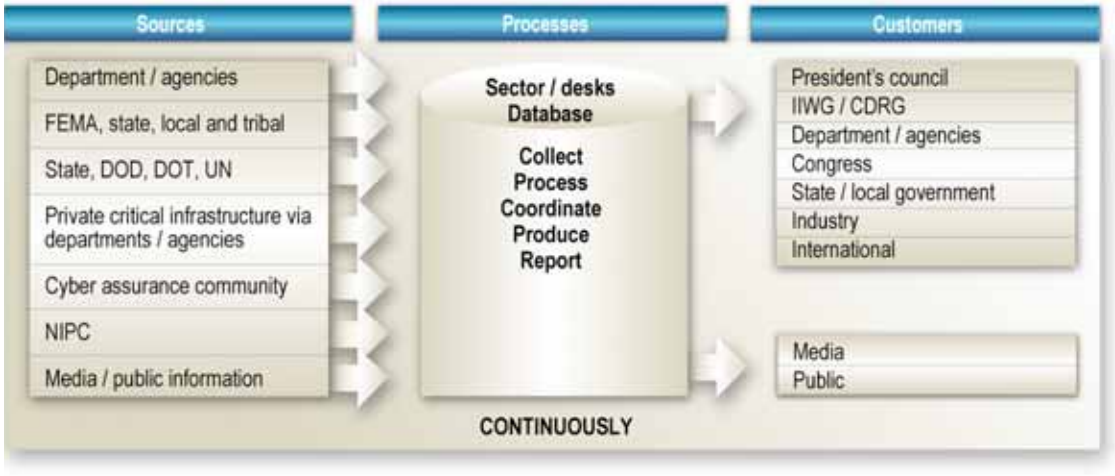


Figure 4-7. Y2K Information Flow

Response to Katrina

The failings of government at every level in the response to Hurricane Katrina have been the subject of many studies and treatises, both within and outside the government. This study turned to the experience of its members as well as outside sources to better understand specifics of the response. Clearly, state and local agencies and officials had inadequate planning and preparation to deal with the scope and scale of the event, but problems occurred at every level. The federal-state-local shortcomings, as developed independently for the Homeland Security Council, are summarized as follows:[16]

- Key decision-makers were unfamiliar with response plans.
- Federal agencies were slow to respond to the unprecedented requirements for federal support and coordination.
- Federal multi-agency coordination centers were not established in the field until after the height of the crisis.
- Critical public affairs structures were not operating at full capacity until weeks after landfall.

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

- The delayed establishment of key federal coordination mechanisms (such as a joint field office) exacerbated management problems and confusion in the field.
- The joint field office should have been fully resourced and pre-positioned prior to the event.
- Key federal, state, and local personnel, especially state National Guard leaders, should have been co-located to facilitate joint planning and decision-making.
- The military played a critical role in the response to Hurricane Katrina, but overall coordination was lacking.
- DOD's mission assignment process proved cumbersome and delayed the delivery of some resources.
- Greater operational planning is needed for specific defense support to civil authorities missions.
- Greater integration between U.S. Northern Command and the National Guard would have enhanced coordination and response.
- Equipment, personnel, and training shortfalls affected the National Guard response.
- DOD needs a greater understanding of the types of support that will be expected during a domestic disaster.
- DHS officials need greater awareness of the capabilities and authorities of DOD; conversely, key DOD personnel should be trained on the National Response Plan, the National Incident Management System, and the Incident Command System.

State and Local Intelligence Fusion Centers

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

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

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

Public-Private

As discussed previously, DHS has been tasked with significant leadership responsibilities for identifying and protecting the nation's critical infrastructure and key resources. In addition to the Government and Sector Coordinating Councils (GCCs/SCCs) it has organized to facilitate the process, DHS has established the Critical Infrastructure Partnership Advisory Council (CIPAC) to support the National Infrastructure Protection Plan (NIPP). Through CIPAC, DHS coordinates federal infrastructure protection programs with infrastructure protection activities of the private sector and state, local, territorial, and tribal governments, and facilitates interaction among the stakeholders in each sector.[17] Because CIPAC meetings are customarily closed to the public, participants can more comfortably share security-sensitive information about threats, vulnerabilities, and protective measures.

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

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

For example, DHS and other sector-specific federal government agencies (SSA) worked with SCCs to produce sector-specific plans (SSP) required by the NIPP.[18] But the experience of the sectors was dependent upon the relationship with the SSA. The information technology sector, whose SSA is the cyber security component of DHS, was very satisfied with the experience, as was the oil and natural gas sector, whose SSA is the Department of Energy. Success was attributed to strong relationships and information sharing between the private and public principals.

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

In spite of these problems, critical infrastructure owners and operators independently have taken steps to protect their assets and enhance the resiliency of their systems based upon their own risk assessments.[19] In many instances, however, they say they are not doing all they could be doing to protect their facilities and employees because of competing interests or issues.[20] For example, companies are chartered to fulfill a fiduciary responsibility to their shareholders for continuity of operations, but in some cases the activities needed for them to best protect their employees are counter to the activities to provide the best continuity of operations. Also, if they actually envisioned the kinds of scenarios contemplated in this study, it could put them on uncertain legal ground regarding risk disclosure and could result in a misperception on Wall Street that could negatively impact shareholders.

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

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

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

A related intelligence issue is the private sector's view that even when DHS intentions are good, it does not always recognize when a sector has a "need to know" due to complex interdependencies with other sectors, unfamiliarity with sector operations, and co-location of infrastructures. As an example of this problem, DHS did not notify the railroad sector of the 2006 Iraq chlorine vehicle-borne IED incidents even though the industry has cleared personnel and a DOD-cleared facility.[21] Although the attacks in Iraq involved chlorine trucks and not rail tank cars, detailed information about the Iraq attacks is very relevant because of the volume of chlorine transported by rail and because the railroad industry is in the process of designing the next-generation chlorine tank car.

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

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

telecommunications, and electric companies unaware of the potential danger to their operations.[22]

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

In the late 1990s, many sectors established Information Sharing and Analysis Centers (ISAC) at the urging of the federal government.[23] ISACs were tailored to the needs of the individual sectors. Some sectors received federal funding for their ISACs; other ISACs were self-funded. But DHS ended federal support for sector-established ISACs and established the Homeland Security Information Network (HSIN), a "one-size-fits-all" approach. The level of satisfaction with HSIN depends upon the constituencies of the SCCs. For example, where the previous ISAC was not well supported, HSIN is a step forward. However, where SCCs are safety and security standard-setting organizations for their industries, and where sectors are network industries, more robust information sharing within the sector is traditional and indeed required for safety (such as the emergency management and railroad sectors). HSIN does not measure up to their standards for timely and useful information. The panel questions whether a single system could ever meet the diverse needs of the many sectors it is attempting to support.

Leadership for the National Team

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

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

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

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

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

Plans and Exercises

There appear to be numerous doctrinal and operational plans, with embedded processes for review and revision of the plans. **But processes to ensure that the plans are practiced and capabilities measured against readiness metrics are lacking.** While there are many exercises (possibly too many), the exercises are highly scripted, unconnected to each other, and typically focus on a top-down approach (where the supporting organizations are "training aids" to the senior-level players) instead of bottom-up approach (focusing on an integrated and layered response beginning with the initial event). Even the national-level exercises have not been effective—more often broad than deep, where the real lessons get learned. They are often stopped before the more difficult issues of transfer of command, or employment of specialized assets, or unknowns (like public panic), come into play. Figure 4-8 is a compilation of the top two levels of national exercises planned for the next five years. Surprisingly, this chart represents the first time that all such exercises were captured in one place. The DSB, and the DHS program manager responsible, note the lack of connection and integration among them.

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

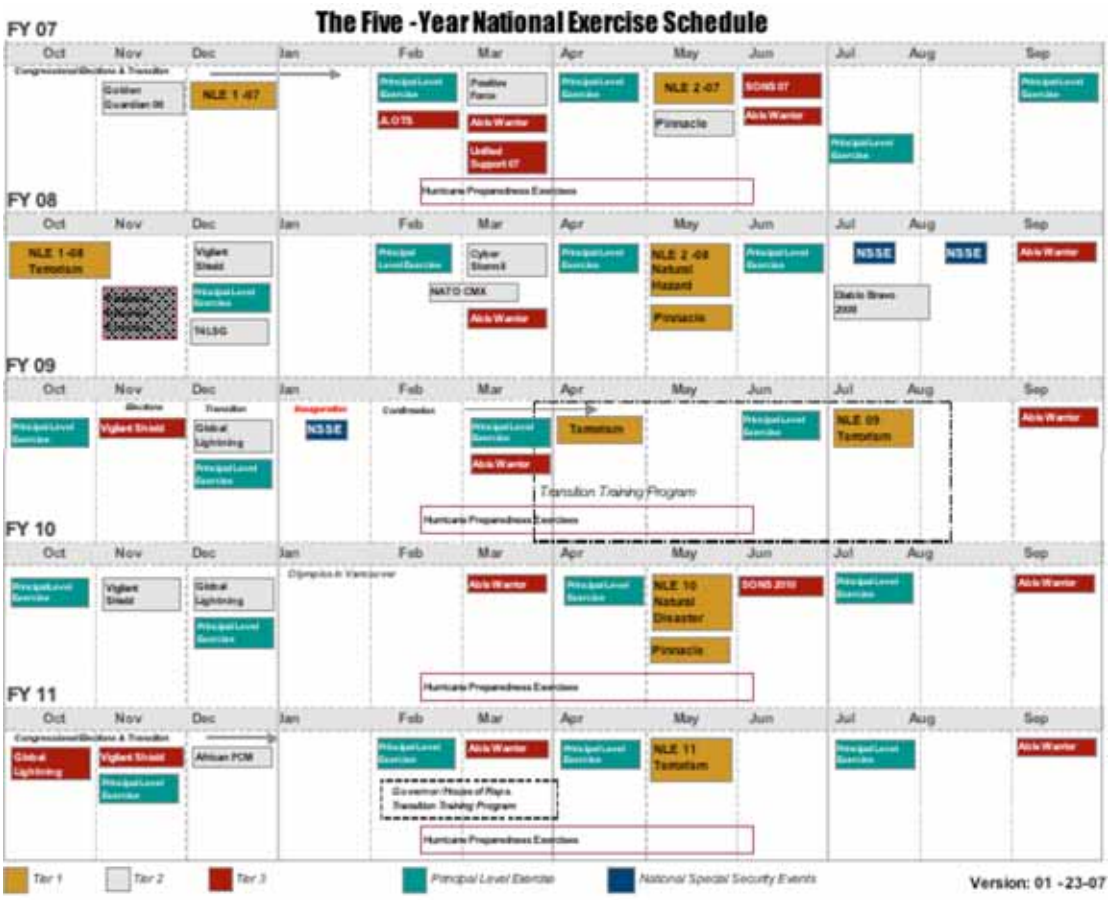


Figure 4-8. The Five Year National Exercise Schedule

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

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

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

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

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

- **The exercise must have an objective.** It must be designed to stress specific elements of the operations plan (in many homeland security and homeland defense cases, a unified operational plan) in ways that result in lessons that will improve the plan and participants' actions. Exercises are learning (not training) opportunities.
- **There must be a model for the exercise.** If the objective of the exercise is to test operations in response to a specific event, there must be a model for that response beforehand against which to evaluate the results of the exercise. This model may or may not be a computer model, but it should be easy enough to understand that anyone involved in, or reviewing, the exercise can clearly understand the exercise.

- **The exercise design should allow observation based on the model.** If the exercise is designed to produce a given result, the result should be well understood, observable, and comparable to that from the model.
- **The data obtained by early observations should be such that they can be analyzed quickly** so that the model, which is bound to be wrong in some respects, and the modeling methods can be changed prior to the next phase of the exercise.
- Exercise design and execution must provide a comprehensive, objective, and accurate **after-action reporting mechanism**, coupled with a corrective action plan and a **commitment to resource** implementation by all parties.
- Regardless of the importance of the exercise in providing answers related to new operations, **the exercise should also provide teaming opportunities for the participants** to work together with other members of the homeland security/defense team.

Why Can't We Learn?

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

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

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

The Department of Homeland Security sponsored a workshop soon after Katrina to examine why the emergency response community finds it difficult to learn certain lessons. This workshop uncovered several barriers to learning and achieving change. These findings were echoed by many responders, homeland security professionals, and private sector representatives with whom the study met. In summary, they are:[24]

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

Motivation for Change

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

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

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

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

Review and Reporting Process

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

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

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

Learning and Teaching

There are many theories on organizational learning behaviors, and most agree on four essential phases, such as those described by Kolb in Figure 4-9.

Figure 4-9. The Learning Cycle

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

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

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

Planning and Executing Exercises

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

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

Resource Constraints

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

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

Crisis Communications

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

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

RECOMMENDATIONS: BUILDING THE NATIONAL TEAM

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

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

- Promote the combination of the National Security Council/Homeland Security Council (NSC/HSC) to coordinate and integrate a national strategy and response for global asymmetric engagement.
- Request a National Intelligence Estimate on the scope of the projected threat.
  - Direct the Office of Net Assessment to conduct a capabilities-based net assessment.
- Request that DHS work with DOD to codify the transition from DOD support to DOD lead for a war at home.
- Direct the Deputy Secretary to develop a comprehensive DOD communication system and public affairs strategy for homeland defense preparedness and crisis/consequence management.
- Develop an equipment and concept of operations architecture compliant with the NIMS.
- Ensure availability of DOD communication assets compatible with civilian responder community.
- Work with DHS to develop messages, and coordinate and educate those who deliver them, appropriate to the full range of contingencies.

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

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

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

- unified management of national capabilities
- communication and information sharing across public and private boundaries
- regional planning and coordination
- interoperable and response capability shortfalls
- transition from DOD support to DOD lead scenarios

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

- train and exercise to a common set of goals and objectives
- build from the bottom up—including all relevant players
  - maximize value of involvement: make it worthwhile
  - exercise what is important at the strategic and policy level
  - exercise what is important in sufficient depth
  - provide unified management of national capabilities
- follow through with effective corrective actions both in policy and practice
- structure to identify interoperable and response capability shortfalls

- address transition from homeland security to homeland defense operations (transition from DOD support to DOD lead scenarios)
- aggressive red teaming to identify interoperable and response capability shortfalls

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

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

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

provide a powerful incentive for state and local regions to maintain interoperable and compatible equipment and concepts of operations.

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

- graduate-level, senior service DHS-sponsored "war" college developed in conjunction with the National Defense University
- an Executive Exchange Program modeled on the President's Executive Exchange Program
- recognition as credit equivalent to senior service schools and for promotion to flag officer rank and the senior executive service in DOD
- training expanded to state and local levels, and the private sector

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

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

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

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

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

Article II of Constitution

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

Stafford Act

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

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

Posse Comitatus Act

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

Homeland Security Directive #5. Management of Domestic Incidents

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

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

Homeland Security Directive #8. National Preparedness

The Department of Defense will provide to the Secretary of Homeland Security information describing the organizations and functions within the

Department of Defense that may be utilized to provide support to civil authorities during a domestic crisis.

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

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

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

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

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

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

NSPD 51, HSPD 20, National Continuity Policy

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

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

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

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

Military Support for Law Enforcement Agencies

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

DODD 5525.5 Cooperation with Civilian Law Enforcement Officials

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

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

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

- Provide information to civilian agencies and the National Narcotics Border Interdiction System (NNBIS) to facilitate access to DOD resources.
- Coordinate with the Department of Justice, the Department of Transportation (U.S. Coast Guard), and the Department of the Treasury (U.S. Customs Service) and represent DOD on interagency organizations regarding matters involving the interdiction of the flow of illegal drugs into the United States.
- Review training and operational programs to determine how and where assistance can best be provided to civilian law enforcement officials.
- Implement procedures for prompt transfer of relevant information to law enforcement agencies.
- Implement procedures for establishing local contact points in subordinate commands for purposes of coordination with Federal, state, and local civilian law enforcement officials.

DODD 3025 Military Assistance for Civil Disturbances

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

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

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

Key Definitions

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

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

aggression, or other threats as directed by the President.[25] The Department of Defense is responsible for homeland defense.

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

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

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

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

Defense Critical Infrastructure

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

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

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

Core Capability: Preparedness and protection of defense critical infrastructure

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

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

- identify infrastructure critical to the accomplishment of DOD missions, based on a mission area analysis
- assess the potential effect of a loss or degradation of critical infrastructure on DOD operations to determine specific vulnerabilities, especially from terrorist attack
- manage the risk of loss, degradation, or disruption of critical assets through remediation or mitigation efforts, such as changes in tactics, techniques, and procedures; minimizing single points of service; and creating appropriate redundancies, where feasible
- protect infrastructure at the direction of the President or the Secretary of Defense where the nature of the threat exceeds the capabilities of an asset owner and civilian law enforcement is insufficient
- enable real-time incident management operations by integrating current threat data and relevant critical infrastructure requirements

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

Core Capability: Preparedness of the Defense Industrial Base

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

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

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

Core Capability: Preparedness to protect designated national critical infrastructure

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

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

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

Part V

What We Know and Don't Know about Adversary Capabilities: Intelligence

Chapter 17. What We Know and Don't Know

This chapter offers an assessment of the Intelligence Community's posture regarding strategic topics associated with future stressing wars—threats such as those posed by weapons of mass destruction, cyber warfare, and other asymmetric threats or innovative concepts of operations that could be employed by an adversary.[78] Rather than focus solely on what the community knows, this study delved into the question of what the nation "doesn't know" in the context of future conflict. This latter question departs from typical assessments of this type and led us to consider how the community can better position itself to gain knowledge in important areas that go unaddressed today.

We conducted our assessment in three ways:

1. First, we conducted extensive discussions with many intelligence collection, analysis, and user organizations regarding their subjective evaluation of detailed aspects of Intelligence Community's knowledge of adversary threats in the following areas: strategic nuclear, chemical, radiological, directed energy, electro-magnetic pulse, biological, cyber, and high-leverage kinetic. These threats are referred to in this discussion as asymmetric threats.
2. Second, the Defense Intelligence Agency (DIA) assessed the community's knowledge of a specific set of countries and strategic threats tailored to the study's areas of emphasis.
3. Third, the Director of National Intelligence (DNI) and the Under Secretary of Defense for Intelligence (USD[I]) in the Department of Defense approved the use of an intelligence tool known as Intellipedia to conduct a community-wide "deep dive" into the state of knowledge of specific nuclear-essential elements of information associated with an Indo-Pakistan war scenario. This deep dive was formally assessed by the National Intelligence Council, which provided classified results related to the Intelligence Community posture in this area.

---

78. The Intelligence Community, established by executive order in 1981, comprises 16 organizations throughout the federal government's executive branch that play a role in the business of national intelligence: Central Intelligence Agency; National Security Agency; National Reconnaissance Office; National Geospatial-Intelligence Agency; Defense Intelligence Agency; Bureau of Intelligence and Research (Department of State); Federal Bureau of Investigation; the intelligence organizations of the four military services (Army, Navy, Air Force, and Marine Corps); Department of Homeland Security; U.S. Coast Guard; Energy Department; Department of the Treasury; and Drug Enforcement Administration.

Collectively, these three forms of assessment produced consistent conclusions about the current posture in the community.

Given an understanding of the Intelligence Community's "know/don't know" posture related to future stressing wars, this study then developed ideas of how the community can close the identified intelligence gaps. The forthcoming recommendations focus on improving foreign intelligence collection, analysis, and customer support activities; assessing counter-intelligence issues associated with future stressing wars; and developing better domestic intelligence associated with the foreign-inspired threats to the U.S homeland. The conclusions of this assessment also point to options for retiring intelligence gaps at the edges of war, lead to recommendations related to issues associated with applying net assessment and gaming to deal with intelligence uncertainties, and address methods for improving intelligence support and interaction with the Defense Threat Reduction Agency (DTRA) on threats related to weapons of mass destruction (WMD).

Know/Don't Know Posture

While much of the assessment of the community's know/don't know posture is classified, this study does concur with the sentiments of the 2005 WMD Commission, which asserted that "strategic issues" such as these should command top level focus in the Intelligence Community and, further, that the community should devote some of its best collection, analysis, and customer interactions to these topics.[79] Yet, two years later, it is still not clear that the community has internalized these observations, nor taken deliberate steps in the areas of collection, analysis, and customer support efforts to devote the necessary resources to strategic threats.

79. *Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 2005.

RECOMMENDATION: KNOW / DON'T KNOW POSTURE

To better position itself to close strategic information gaps, the intelligence community should create a set of X-treme intelligence teams.

The key issue here is to "organize for a high probability of success." Small, agile, multi-disciplinary teams should be formed from the best talent available in collection operations and would be supported by analysis, technology, security, and high levels of customer involvement. The teams would focus on strategic essential elements of information related to important strategic threats. These integrated Intelligence Community teams would be applied against a narrow range of the nation's most strategic and pressing intelligence and customer needs, operate beyond "mission managers" that currently exist within the Intelligence Community, and work closely with community assets to focus on the assigned threat. While the teams would start as prototypes to prove the concept, their approach is intended to change the nature of the intelligence game by pushing to higher and more successful levels of performance.[80]

As with X-treme sports, the team members will be hand-selected for their proven abilities, potential for extraordinary performance against difficult odds, and for thinking and actions outside the box. The team leadership, dynamics between and among the team players, their ability to know and extract support from the existing Intelligence Community, and their technical and operational skills would be unsurpassed. Team size and structure is to be determined, but it could be comprised of both full-time and part-time consulting personnel.

Countering Foreign Intelligence Threats to U.S. Military Operations

Foreign intelligence operations against the United States are now more diffuse, more aggressive, more technologically sophisticated, and potentially more successful than ever before. In particular, the use of human intelligence operations by weaker powers to achieve advantage is a classic "asymmetric strategy," which increasingly will challenge future U.S. military operations as adversaries learn from

80. The classified version of this report includes detailed description of the differentiated attributes of X-treme teams.

past successes. As the counterintelligence community learned in the lead up to Operation Iraqi Freedom, strategic operational planning to degrade foreign intelligence capabilities has long lead times to identify collection gaps and strategies to fill them, assess vulnerabilities, develop targets, exploit opportunities, and execute operations to degrade or neutralize enemy capabilities.

Given DOD's global responsibilities, activities to identify, assess, and defeat foreign intelligence activities are an ongoing defense mission, spanning peacetime to wartime. Despite this compelling requirement, the Secretary of Defense does not have central command over the forces assigned to countering foreign intelligence threats. Nor is there a full-time commander focused on defeating the foreign intelligence threats to DOD's personnel, operations, installations, and information. While service counterintelligence components provide support to the individual combatant commands to counter foreign intelligence operations within their respective areas of responsibility, the command structure is ill-suited to undertake global operations against an adversary intelligence service, which in the context of future stressing wars will have operational presence beyond the immediate theater (including within the United States).

To fix this serious problem, the Secretary of Defense should establish a new joint operational component within DOD, drawn from the service counterintelligence components and CIFA, with the standing mission of degrading foreign intelligence capabilities. This new command would enable a robust planning function focused on defeating foreign intelligence threats, and serve as the beginning of a "purple" defense counterintelligence service. It would also be responsible for developing doctrine to guide who does what globally against foreign intelligence targets (a key missing ingredient in the defense counterintelligence posture), for assigning resources, and for directing and executing operations to achieve strategic objectives.

Finally, establishing a new joint operational counterintelligence component would galvanize intelligence community support for the defense counterintelligence effort, and provide the nucleus for a serious national level strategic capability. The new command would provide a single focal point interface with the counterintelligence support element within the National Clandestine Service, as well as the Federal Bureau of Investigation (FBI) and other community resources. If DOD can deliver an integrated force capable of degrading foreign intelligence targets as part of a strategic campaign, the other departments and agencies with counterintelligence resources can—and likely will—fall in line.

Today, defense counterintelligence is a collection of disaggregated and service-driven operational programs, each with distinct doctrinal and organizational bases that are grounded in history and differences in service missions. This circumstance was true back in the late 1960s when DIA was first constituted (and was assigned the foreign intelligence part of the counterintelligence mission) and despite significant changes remains true today. The Army aligns its counterintelligence function with those of human and signals intelligence under the Assistant Chief of Staff for Intelligence; its counterintelligence officers have no criminal jurisdiction. The Air Force and the Navy, on the other hand, keep counterintelligence separate from their intelligence functions and combine its duties with criminal investigation. The Air Force component (the Office of Special Investigations) reports to the Air Force Inspector General, while the Navy Criminal Investigative Service is a separate command within the Department of the Navy. The 650th Military Group, NATO, is yet another separate operational unit.

CIFA was created in part to compensate for this disunity of command, to supply strategic direction, and to integrate defense counterintelligence programs. But simply imposing an organizational cover on a disjointed architecture doesn't make it joint. Defense counterintelligence needs a genuine Goldwater-Nichols transformation to bring strategic direction and command coherence to countering foreign intelligence threats to future military operations.

Summary of Findings

- DOD's personnel, operations, installations, and information are principal targets of foreign hostile intelligence.
- The job of defeating adversary intelligence capabilities directed against U.S. military operations is a key DOD mission.
- Despite this compelling requirement, the Secretary of Defense does not have unity of command with respect to the counterintelligence forces that are assigned to identify, assess, and defeat these threats.
- Operational intelligence on foreign intelligence activities is poor.
- Military service counterintelligence components provide support to individual combatant commanders, but the command structure is ill-suited to undertake global operations against an adversary intelligence service.

RECOMMENDATION: FOREIGN INTELLIGENCE THREATS

The Secretary of Defense should establish a joint operational component within DOD with the standing mission of detecting and degrading foreign intelligence capabilities that threaten U.S. military operations while retaining the focus of the service counterintelligence organizations.

Intelligence on Foreign-Inspired Domestic Threats

Foreign-inspired domestic threats to DOD forces, operations, resources, and critical assets within the United States remain largely unknown to U.S. intelligence and, therefore, present high order challenges to U.S. military operations in future engagements.

Dating from the Cold War, DOD has broad experience in mission-critical asset identification and protection, and has developed and employed dynamic tools for assessing installation infrastructure dependencies and vulnerabilities both inside and outside the fence. While implementation has been uneven, current defense guidance clearly assigns responsibility for anti-terrorism/force protection and for defense critical infrastructure protection, including policy lead, support duties, and command execution responsibilities for mission-critical infrastructure protection. It is a difficult (but manageable) analytic problem to identify mission-critical dependencies and vulnerabilities; it is quite another (and more difficult) problem to identify adversary plans, intentions, and capabilities to disrupt or deny these critical assets in order to enable measures to protect them.

As the National Intelligence Estimate on Terrorist Threats to the U.S. Homeland, released July 17, 2007, warned, "The ability to detect broader and more diverse terrorist plotting … will challenge current U.S defensive efforts and the tools we use to detect and disrupt plots. It will also require greater understanding of how suspect activities at the local level relate to strategic threat information and how best to identify indicators of terrorist activity in the midst of legitimate interactions."

When one extrapolates from this warning (which concerns the highest priority intelligence target receiving the most intense national intelligence effort) to the even less well-understood threats to the U.S. homeland presented by peer and near-peer actors, the implications are profound and urgent. The nation

simply does not have the intelligence it needs to protect mission-critical DOD activities at home. Moreover, DOD's requirements for intelligence support at home have not been well-defined. This deficiency may be due in part to low expectations for having those intelligence support requirements met, but is likely also due to competing DOD priorities for intelligence support.

The panel discussed, without coming to resolution, the debilitating shortcomings inherent in current national processes and capabilities dedicated to identifying and assessing foreign-inspired domestic threats. Insights into foreign presence and operations within the United States—spanning aggressive foreign intelligence collection operations, activities that might constitute "battlefield preparation" for hostile action within the continental United States, and foreign terrorist activities—are outside the traditional lanes of U.S. intelligence, which historically have been directed (and in important ways confined) to a foreign focus, outside the continental United States.

Legislative history behind the new DNI structure, including the work of the 9/11 Commission and the WMD Commission, suggests that the Office of the DNI was created in large measure to better connect foreign and domestic intelligence. Yet the weaknesses in capability persist. Intelligence on foreign-inspired domestic threats must be derived in part from contributions of independent law enforcement agencies at the federal, state, and local levels, which lack the training or established processes needed to function as intelligence producers, or the structural discipline or experience to function as a community. There is also some measure of trial and error in bringing intelligence tools and techniques into the domestic arena, as ongoing public debate weighs civil liberties concerns against public safety and national security needs. These concerns extend to DOD force protection activities at home, as recent experience with the Counterintelligence Field Activity (CIFA)/Talon database attests.

One promising note is the work of the New York Police Department (NYPD), which (consistent with the rule of law) has adopted seasoned intelligence collection and analysis practices and exported them to the streets of New York. As a recent example, Transit Police on the Number 7 train in New York observed two men videotaping infrastructure. Most of the video was of tourist interest, but two minutes of the tape included imagery of train track. The cameramen were later found to be working for Iranian intelligence. The NYPD turned the individuals over to the FBI and they were deported 10 days later. NYPD's success in such work derives in large measure from having hired a deputy police commissioner who is a retired senior CIA intelligence officer. New

Yorkers also have the painful history of September 11, 2001 as compelling motivation to work locally to ensure the security of the city and to contribute to overall national-level understanding of the threat.

The current and projected lack of intelligence on foreign-inspired domestic threats has three immediate implications for DOD. First, understand that intelligence on foreign-inspired domestic threats is poor and plan accordingly. Planners will need to take threat uncertainty into account, underscoring the renewed importance of national security emergency preparedness plans and programs to ensure enduring essential capabilities through prioritized planning for redundancy, reconstitution, and recovery.

Second, clearly articulate and prioritize intelligence support requirements at home, and reinvigorate DOD's intelligence, counterintelligence, and security programs to help meet them. The defense guidance (DODD 3929.40 August 19 2005) charges the USD(I) with responsibility for establishing policy to provide intelligence, counterintelligence, and security support to the Defense Critical Infrastructure Program (DCIP), including establishing intelligence collection policy for DCIP efforts, establishing policy for sharing and maintaining DCIP-related threat assessments, and validating DCIP intelligence collection priorities. The USD(I) should take the lead in validating and prioritizing intelligence requirements for DOD's three complementary responsibilities of force projection, defense of the homeland, and support to homeland security across the spectrum of civil support needs, and for the range of national security and emergency preparedness activities (including warning intelligence and situational awareness) necessary for their success.

These activities are broader than force protection, or base protection alone, and include people and functions on and off base, as well as privately owned elements that are often more vulnerable than a base itself. The analytic methodology employed for national security and emergency preparedness should yield a taxonomy of prioritized intelligence requirements that DOD should present to the DNI. This analytic work should also inform U.S. Northern Command's intelligence campaign plan and metrics for homeland defense contingencies.

DOD's role and focus to address improved collection and analysis of foreign-inspired domestic threats needs to be expanded, which falls to the Deputy Under Secretary of Defense for Counterintelligence and Security to execute. While the new joint operational counterintelligence component discussed elsewhere in this report has global responsibilities, its establishment and work product should also

prove an invaluable resource to DOD and nationally for the positive intelligence and operational options it may supply for identifying, assessing, and defeating foreign intelligence operations within the United States.

Finally, help develop local "intelligence" capabilities in prioritized areas. Unlike politics, it is manifestly untrue that "all intelligence is local." Instead, some intelligence is local. Indeed, the whole thrust of the intelligence critique presented herein is the need for strategic intelligence assessments. National-level intelligence is critical to DOD's ability to execute its mission in future stressing wars; but national security emergency preparedness, antiterrorism, and force protection programs are also dependent on local insights. As an additional layer of protection, DOD should prioritize its need for the kind of local threat data best collected and analyzed locally, and identify localities where adopting the NYPD model described above would likely be of particular value to DOD's mission.

Summary of Findings

- Among the most stressing challenges to U.S. military operations are threats to homeland-based forces, operations, resources, and assets.
- DOD is responsible for force protection (and dependent on critical defense infrastructure including industrial base) but does not have and cannot presently acquire sufficient understanding of the threat within the United States.
- U.S. intelligence lacks situational awareness and sophisticated understanding of foreign-inspired threats or operations within the United States.
- Without change, the current DHS, FBI, and other law enforcement organizations, along with the existing Intelligence Community entities, will not be able to provide adequate domestic intelligence to meet DOD mission needs.
- DOD has not adequately defined its intelligence requirements at home related to future stressing war scenarios.
- NYPD has adopted an approach for utilizing strong intelligence collection and analysis methodologies that may be an ideal "franchise model" across localities critical to DOD missions.

RECOMMENDATIONS: FOREIGN-INSPIRED DOMESTIC THREATS

- **The Under Secretary of Defense for Policy, working with USD (I), should ensure that DOD identifies military capabilities in localities where the NYPD model can be more aggressively applied; develop and expand that NYPD intelligence methodology—in effect, franchise the NYPD template locally via DHS and law enforcement training and grant activities.**
- **USD (I) should strengthen his role as the DOD focal point for intelligence in support of defending U.S. military homeland-based capabilities, assets, facilities, and functions.** Principle attention should be given to the following:
  - Revalidate requirements and needs.
  - Develop and update domestic intelligence campaign plans and metrics:
    - Expand the role and focus of Deputy Under Secretary of Defense for Counterintelligence and Security to address improved collection and analysis of foreign-inspired domestic threats to the DOD rear.
    - Work with the Intelligence Community, DHS, and law enforcement organizations to improve collection and analysis of threats to DOD-dependent critical infrastructure.
  - Define what additional capabilities are required.

Need for Strategic Analysis

The study reviewed the relationship between intelligence and net assessment processes, and had several interactions with the Director of Net Assessment in the Office of the Secretary of Defense, with regard to studies and analysis. The study concluded that net assessment processes of red on blue interaction, expanded to full gaming and simulations of future strategic threat issues, could be very useful in better understanding the significance of intelligence gaps, in gaming notional threats to explore the sensitivities of the intelligence uncertainties, and for making and exploring a range of informed intelligence speculations in the face of unknown threats.

Interestingly, as a bi-product of closer intelligence and net assessment cooperation and coordination, in-depth intelligence collection and analysis could also be improved, and the DOD and the intelligence community together could rediscover the full potential of net assessment disciplines to contribute to departmental preparedness and intellectual ferment for anticipating and dealing with strategic threats of the kind posed by potential peers or near-peers.

Summary of Findings

- Net assessment (blue on red interaction) has proven itself in identifying important gaps in complex and multi-dimensional military problems.
- Given the poor state of knowledge of future stressing war, net assessment and gaming and simulation techniques should be employed to identify and understand intelligence gaps, the implications of these gaps, and commensurate intelligence opportunities. Employing such tools would also sensitize the blue side to "fact-of" such intelligence gaps.

RECOMMENDATION: STRATEGIC ANALYSIS

The Office of Net Assessment, USD (I), and DNI should establish a capability to assess big complex peer problems (*e.g.* space anti-access) for net assessment and modeling of future stressing war.

Intelligence Community

With regard to the high-end threats addressed by this study, DTRA is an important customer and partner for the intelligence community. There are certain aspects of the community's relationship with DTRA that are models of great support (the Underground Facility Analysis Center [UFAC], for example), but there are also areas where the intelligence connections with DTRA leave something to be desired. The WMD Threat Research and Analysis Center (WTRAC) and U.S. Strategic Command's Combating WMD Center are two such examples.

While the recommendations in this area focus on actions for the director of DIA, there could also be implications here for the DNI to ensure that DTRA is better serviced by the Intelligence Community, and that the community is able to access and utilize the technical expertise that DTRA can bring to collection and

analysis. In particular, cooperation and collaboration on third- and fourth-generation nuclear weapons might serve as a specific starting point for building dramatically improved relationships on these strategically important topics.

Summary of Findings

- To date, collaborative efforts between DTRA and the intelligence community are insufficient to support the WTRAC and STRATCOM Center for Combating WMD.
- The UFAC is an effective model for collaboration between DTRA and the community.
- Improved collaboration between the two organizations could particularly help with challenges associated with advanced design (including third and fourth generation) nuclear weapons.

RECOMMENDATIONS: INTELLIGENCE COMMUNITY

The Director, DIA should take the lead in expanding support for activities related to WTRAC interactions around the UFAC model.

Develop a special analysis effort between DTRA and the Intelligence Community on third and fourth generation weapons.

The recommendations described herein are targeted to improve U.S. intelligence capabilities in support of future stressing wars. The challenges ahead will require broad emphasis on counterintelligence, on foreign inspired domestic threats, and on the other challenges described in this section. Many of these recommendations involve new ways of doing business, improved collaboration among community organizations, and attention from community leadership to ensure adequate resources are directed to these efforts.

Part VI

Fighting Through Asymmetric Counterforce

Chapter 18. The Asymmetric Challenge

The United States has significant plans for improving its conventional military capability, which should enable it to retain its advantage in force-on-force capability through the next several decades. Faced with this conventional U.S. advantage, potential adversaries will likely seek asymmetric methods to undermine and ultimately deter or influence U.S. military operations. Such asymmetric methods might include attacks on U.S. vulnerabilities, the use of deception to avoid a direct U.S. response, use of non-attribution, and intimidation of allies. Methods that are difficult or impossible to detect and attribute create an advantage for an adversary, who can therefore achieve an effect before retaliatory combat operations can be initiated by the United States.

Adversaries will seek to destroy a variety of capabilities to reduce U.S. combat capabilities. A combination of the following elements offers effective options to achieve this effect:

- direct attack of deployed military forces focusing on command and control; intelligence, surveillance, and reconnaissance (ISR) assets; and logistics support centers
- interruption of logistics lines of communication to interfere with support for deployed forces
- attacks against the U.S. homeland
- use of asymmetric capability to intimidate U.S. allies or neutrals into withdrawing support to the United States, thereby undermining U.S. credibility to protect its allies

Until recently, it was assumed that the U.S. homeland was a sanctuary where military forces could prepare for combat operations, and from which they could be supported. This assumption is now broadly viewed as flawed, as was discussed previously in this report. Disrupting the logistics support chain and/or attacks against the American populace or infrastructure could undermine public support for any U.S. military operation abroad and impede efforts to secure more military capability to support homeland defense. It can also undermine trust in U.S. systems.

Adversaries may seek to employ multiple asymmetric attacks that simultaneously impede or deter U.S. military operations abroad and at home. Moreover, there is a troubling risk that the United States could face an adversary with sufficient understanding of asymmetric counterforce to optimize a sequence of actions in key areas that would cripple U.S. military operations, while maintaining a non-attribution posture. Examples of combined and sequenced actions include: cyber attack against ISR system control elements to deny the United States knowledge that its satellite systems are under direct attack, substitute older imagery for current images to mislead decision makers, send false control signals to unmanned aerial vehicles (UAVs) to deny ISR coverage, and send false warnings of WMD attacks.

In addition to the examples above, there are numerous other potential combinations that planners must imagine and consider in order to prevent or counteract an adversary's attempt to undermine U.S. military capabilities at home and abroad. While the range of potential asymmetric attacks is wide, this study chose to focus its work on a small set of the most compelling challenges, which were selected based on the following criteria:

- potential for catastrophic consequences
- lack of U.S. preparedness to handle the threat (and even greater lack of preparedness among U.S. allies and friends)
- modest investment by adversary may bring dramatic consequences
- adversary attacks against deployed U.S. forces would have consequences for civilian populations, and economic and political targets at home and abroad
- non-attribution capability may make retaliation difficult
- potential to undermine international perception of U.S. power

Among the many options considered, the three most compelling challenges identified for examination in this study are:

- **Combat operations in a WMD environment.** This challenge includes the threat of, or actual use of, WMD against U.S. forces and/or an ally. Countering this threat involves protecting critical bases of operations, and projecting and sustaining forces in distant anti-access environments.
- **Countering attacks on space assets.** Critical to this challenge is gaining and maintaining space-situational awareness, conducting defensive and

offensive counter-space operations, and conducting combat operations when space capabilities are degraded.

- **Cyber warfare against information and networks.** The challenge of keeping pace with this ever-advancing threat is real. Counters include learning to operate with degraded networks and corrupted information, and developing integration applications of cyber defense, attack, and exploitation.

Many challenges were considered, but not selected, as the "most compelling." Examples include attacks on naval task forces, directed energy attacks against fighter and bomber aircraft, simultaneous attacks against multiple U.S. military installations (without alerting force protection responses), and directed energy attacks against airborne systems. Each of these attacks would indeed have a significant effect on military operations. However, it is the opinion of the members of this study that they would not have catastrophic effects of the type and scale that could be achieved through the use of WMD, attacks on U.S. space assets, or cyber attacks against U.S. information and networks.

After examining these asymmetric counterforce issues, the study concluded that the United States must invest more heavily in the development of intellectual capital, technology, and operational concepts that will, in time, enable the U.S. military to significantly counter these challenges. Serious and focused preparation in these areas can significantly reduce an adversary's ability to impact U.S. conventional military forces and, in effect, impede or deter his actions. The next three chapters detail the findings and recommendations for each of the three challenges that derive from these broad conclusions. As Part 4 of this report addressed the impact of asymmetric operational concepts on the homeland, this part of the report will focus on the impact of the United States to wage war abroad.

Chapter 19. Combat Operations in a WMD Environment

During the Cold War, the world was dominated by two superpowers. The widespread use of WMD was constrained by the balance of power between the two superpowers (mutually assured destruction) and later by various treaties. Since the fall of the Berlin Wall and the collapse of the Soviet Union, the world has been dominated by one superpower that has no apparent peer. In the 21st century, it is widely accepted that competitors—-peer, near-peer and major non-state actors—will exploit asymmetric means to win an advantage over a still strong United States. These competitors, especially non-state actors, will be far more difficult to deter using means that have worked in the past. Though deterrence is not rejected as a strategy, it is important to plan for a future in which deterrence is not effective.

This chapter explores the impact of the use of weapons of mass destruction (nuclear, radiological, chemical, and biological) on the ability of the United States to fight and win in a foreign theater of operations. Key issues addressed include the following:

- How do the WMD modalities available to adversaries challenge U.S. forces?
- What would a determined peer, near-peer, or non-state actor target—U.S. forces (deploying or deployed), allied or partner forces, local populations, or local food and water supplies, for example?
- What are the major implications for the U.S. ability to station, deploy, employ, and sustain military forces overseas in the combat theater of the future?
- What actions should the United States take to improve preparedness?

In the future, competitors will likely seek the greatest possible advantage in any action against the United States. For example, the attacks of September 11, 2001, would not have been as dramatic had the target cities been other than New York or Washington, DC. A competitor that would use WMD is not likely to be constrained by societal or moral norms, or by laws of war from using such weapons, even against heavily populated civilian areas. Indeed, they may actually achieve more of the effects they desire by creating mass civilian casualties. This

chapter omits the impact of such attacks on the homeland (as they were addressed in previous chapters) except to note that the ability to sustain the flow of forces or supplies to an overseas theater could be seriously impaired if the supporting logistics structure in the United States were attacked.

The impact of WMD attacks on civilian populations should be of particular concern to U.S. forces. The military services depend on large numbers of contractors, both U. S. and foreign, to sustain operations in a foreign theater. A civilian work force that is killed or injured by WMD is no more useful than one that has walked off the job in the face of threats to use such weapons. The resident civilian population in most anticipated theaters will not be well-protected against these threats, and may require a large commitment of U.S. forces in the wake of an attack. The nature of the help that will be needed to manage the consequences of a WMD attack will be different from that required to support displaced persons on a more conventional battlefield. These concerns, and the extraordinary impact WMD will have on the way the U.S. will fight, must be accounted for in planning for war over the next 20 years.

The same capabilities the Department of Homeland Security is trying to put in place in the wake of Hurricane Katrina will be needed by U.S. forces and partner nations overseas. That said, requirements are markedly different when preparing to fight through a WMD event. Preparedness measures to survive and recover from a WMD attack on the U.S. homeland are far below the level achieved in the early years of the Cold War when, in response to a clear and compelling threat, there was a strong and visible civil defense structure, frequent civilian training and drills, and robust training and exercises for military forces. Although it is true that the services have maintained a higher state of readiness than their civilian counterparts, U.S. forces are not ready for the WMD threats they may encounter. Nor can it be said that the U. S. government civilians and contractor work force that support deployed forces are ready to sustain operations in a theater threatened by WMD.

The *National Military Strategy to Combat Weapons of Mass Destruction* establishes the military strategic goal of ensuring that the United States and its armed forces, allies, partners, and interests are neither coerced nor attacked by enemies using WMD. If an adversary succeeds in using WMD against the United States, the strategy calls for military forces capable of minimizing the effects to continue operations in a WMD environment and assist the civil authorities of the United States and its allies and partners.

Actions can be taken before, during, and after a successful WMD attack to minimize its effects:

- Actions that can be taken **before** an attack to prevent debilitating consequences include hardening likely targets, positioning sensors to detect chemical or biological agents, inoculating prospective victims against likely biological agents, and providing protective equipment and training people to use it.
- Actions that can be taken **during** an attack and in its immediate aftermath to ameliorate consequences include detecting the attack, sounding the alarm, increasing protective posture, identifying victims, and applying first aid.
- Actions taken to clean up **after** an attack are those defined in Joint Publication 1-02 as consequence management—"actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents."

Various agencies are responsible for taking such actions, as Table 6-1 depicts. For attacks against the U.S. homeland, DHS has lead responsibility for preparations before, response during, and consequence management after an attack. DOD, under U.S. Northern Command, is charged with providing support to civil authorities in domestic emergencies, such as in the case of large-scale disasters. DOD's involvement in the Hurricane Katrina response serves as example. The displacement of the U.S. population by a WMD event may be greater in scope and scale than the Katrina experience and may be of much longer duration if a nuclear weapon is involved. Such events will overwhelm the ability of the civil emergency response structure and will require DOD support over a much longer period.

U.S. forces—active, guard, and reserve—that are called to respond to homeland emergencies will not be available to support an overseas operation. In fact, support for a WMD event in the United States may take precedence over operations abroad. Should a sizeable number of forces be required at home, it could impact the conduct of operations abroad. The number of military personnel involved in support of Hurricane Katrina was about 80,000 at the peak. One can infer a similar, or even greater, commitment of forces to a WMD event with the attendant impact on the progress of operations in an overseas contingency. It will therefore be even more important that partner nations have the capacity to support U.S. forces abroad.

Table 6-1. Responsibility for Mitigating Actions in Response to a WMD Attack

	Before	During	After
U.S. homeland	DHS	DHS	DHS/**DOD (DSCA)**
U.S. forces (in CONUS, overseas, or en route)	**DOD**	**DOD**	**DOD**
Allied or partnered forces	Partner nation	Partner nation	Partnered/host nation state is primary federal agency for foreign consequence management; **DOD may support state**
Local population	Host nation	Host nation	Host nation state is primary federal agency for foreign consequence management; **DOD may support state**

For U.S. military forces, DOD has the lead responsibility for mitigating actions before, during, and after an attack, whether the forces are in the United States or overseas. For countries participating as part of a U.S.-led coalition, the parent nation has responsibility for allied and partner forces. The host nation has responsibility for the local population and infrastructure, and the food and water supply before, during, and after a WMD attack.

Should the host nation government or partner forces find themselves overwhelmed by the consequences of a WMD attack and request assistance from the United States, the Department of State is the designated lead federal agency, and DOD may be directed by the President to support the foreign consequence management effort. Thus, it is possible that the same U.S. military capabilities, particularly the specialized capabilities organized, trained, and equipped to deal with WMD attacks, may be in demand to support civil authorities in the U.S. homeland, foreign consequence management efforts abroad, and U.S. combat forces in overseas contingency operations—all at the same time.

Critical Challenges in Fighting Through WMD

In analyzing the impacts of fighting in a WMD environment, three challenges stood out as particularly critical to the success of U.S. military operations (Table 6-2). Failure to adequately address these challenges could have debilitating effects on U.S. military operations against a WMD-armed enemy.

Table 6-2. Fighting Through WMD Poses Critical Challenges

Challenges	Potential Effects
U.S. military operations depend on others who lack protection from chemical, biological, and radiological attacks ▪ Allied and partner military forces ▪ Critical civilian personnel ▪ Host nation population	Partners who lack capacity to withstand attacks will suffer disproportionate losses, rendering them unable or unwilling to support U.S. military operations. Loss of partner support could have catastrophic effects on outcome of the conflict.
Concepts and doctrine have changed little since the Cold War ▪ "Combating WMD" is focused on weapons ▪ Emphasis on "fighting through" has diminished	Forces that are not well trained and equipped to deal with chemical, biological, and radiological attacks will suffer massive losses and may be rendered combat-ineffective. Plans not validated through realistic exercises may be ineffective in the face of WMD attacks.
U.S. forces vulnerable to small-scale nuclear attack ▪ Critical nodes ▪ EMP	Even one or two nuclear weapons could bring U.S. force deployments to a halt and cripple C4ISR.

First, U.S. forces abroad depend on host nations for bases and logistical support, and on host-nation and other civilians to deploy and sustain the force. These elements are subject to the effects of any WMD attacks directed against U.S. forces. Yet most host nations do not have the same degree of protection against such attacks, nor do they have the same capability to manage their consequences. As a result, host nations and supporting forces may be less willing to support U.S. military operations in the face of WMD threats if they could reasonably expect to suffer disproportionately, compared to U.S. military forces. Further, the civilian population in an area of operations could require support from U.S. forces in the aftermath of a WMD event. The United States can take actions to mitigate such consequences. Providing training assistance to partner countries and foreign consequence management support are key elements of strategic communication, particularly in overseas areas, because they convey U.S. concern for, and resolve to assist, friends and allies.

Second, in recent years, concepts and doctrine have not kept pace with the changing WMD environment. The "combating WMD" doctrine that has been developed to deal with the new environment appears overly focused on defeat

of the weapons themselves, giving less attention to the capabilities needed to fight a campaign against an adversary armed with and willing to use them. The demands of current operations have further reduced the time most forces have available to train for operations in a WMD environment. In short, U.S. forces may not be properly organized, trained, and equipped for fighting through the effects of WMD.

Third, although U.S. forces are better protected against chemical and biological attacks than the civilians and foreign nationals on whom they depend, nuclear attacks pose a much greater challenge to both U.S. forces and their partners. Even a single nuclear weapon could render key nodes unusable for extended periods, and EMP effects from a limited nuclear attack could blind sensors and shut down key command and control systems. U.S. forces routinely trained for operations in a WMD environment into the early 1990s—fighting through chemical, biological, and even nuclear effects.

Building Partnership Capacity

In its published guidance, the Department both *emphasizes and qualifies* its support of building partnership capacity to fight through WMD attacks. In recent years, DOD has strongly pledged to help partners prepare for such attacks. For example, the July 2000 Joint Publication 3-11, *Joint Doctrine for Operations in a NBC Environment,* states:

> All **commands are responsible for cooperative actions** in peacetime with governments, armed forces of allies, and potential multinational partners **to facilitate sustainment of operations in NBC environments** [emphasis added].
>
> The JFC [Joint Force Commander] has responsibility for ensuring that coalition and HN [host nation] weaknesses do not compromise U.S. forces or missions. It may be necessary in this regard to apply U.S. resources to support multinational partners and HNs before, during, and after NBC attacks.

The February 2006 *Quadrennial Defense Review* further emphasizes the importance of marshalling all the elements of national and international power and makes building partnership capacity central to DOD strategy. As stated in the report:

> **The Department must help partners improve their ability to perform their intended roles and missions.** This includes foreign governments trying to police themselves and govern their populations more justly and effectively…." [p. 17, emphasis added]

Finally, the March 2006 *National Military Strategy for Combating WMD* states that:

> [DOD] must assist international partners to build capacities to combat WMD effectively. … The military must strive to expand and exercise combating WMD partnerships with a goal of creating partners that can provide for themselves and assist during coalition operations.

Two other directives issued in March 2006 seem to indicate, however, that DOD has qualified its support for building partnership capacity during aspects of combating WMD. The Chairman of the Joint Chiefs of Staff Instruction 3214.01B, *Military Support to Foreign Consequence Management,* emphasizes the host nation's responsibility and generally constrains U.S. support to specific requests made through the Department of State. Further, DOD Instruction 2000.21, *Foreign Consequence Management,* states that, when requested, DOD "will support U.S. Government Foreign Consequence Management operations to the extent allowed by law and subject to the availability of appropriated funds for such purposes."

This guidance raises questions regarding whether and to what extent DOD will honor its pledge to help develop the capabilities of its allies and partners, as well as critical civilian personnel and host nation populations, to "fight through" a WMD environment.

The bottom line is that the lack of clear guidance creates a gap that has an impact on activities in support of building partnership capacity are resourced.

DOD has taken some steps toward building partnership capacity, but much more is required to fully develop this needed capability. The *Security Cooperation Guidance* describes the Secretary of Defense's priorities to build partnership capacity for the future. The contributions of partner nations through enhancement of their capacity to defeat current and emerging threats are a cornerstone of the security cooperation effort. Although priorities have been established, resources are limited for activities such as exercises, global train and equip, and the National Guard State Partnership Program. In addition to the *Security Cooperation Guidance*, the 2006 post-QDR roadmap for building partnership capacity established DOD strategic and budgetary priorities for these activities across the Department. The 2006 reorganization of the office of the Under Secretary of Defense for Policy underscored the emphasis on allies and partners by creating deputy assistant secretaries of defense for partnership strategy and coalition support.

Using authority granted under Section 1206 of the 2006 National Defense Authorization Act, DOD funded some global train and equip projects around the world during fiscal year 2006, obligating almost $100 million for programs in key target countries. Such programs include the following:

- Pakistan. Improving counterterrorism strike capabilities (~$27m)
- Indonesia. Securing strategic sea lanes against terrorists and oil disruptions (~$18m)
- Lebanon. Reducing Hezbollah's operational space (~$10m)
- Sri Lanka. Reducing ungoverned maritime spaces (~$11m)
- Gulf of Guinea (Nigeria, Sao Tome & Principe). Expand governed maritime areas (~$6.8m)
- Morocco, Algeria, Tunisia, Nigeria, Chad, and Senegal. Securing the trans-Sahara region against terrorists (~$6m)
- Yemen. Countering cross-border terrorist activity (~$5m)
- Panama and the Dominican Republic. Forward defense of the U.S. homeland (~$15m)
- Thailand: Securing strategic sea lanes (~$5m obligated before coup)[1]

These initial DOD projects have been well thought out, but modest in scale and primarily focused on counterterrorism. Combatant commanders, for example, requested resources for 67 projects for fiscal year 2007 totaling almost $800 million, $500 million more than was authorized. Moreover, the projects that were funded (such as those fiscal year 2006 projects listed above) focused on counter-terrorism rather than combating WMD. While these efforts are important, they do not address the unique challenges of combat *in* a WMD environment.

In addition to the challenge of inadequate funding, efforts also suffer from the fact that current authorities limit DOD's ability to build partners' capacity most effectively. Despite repeated DOD and Department of State requests, Congress has not made global train and equip—another name for building partnership capacity—authority permanent. Furthermore, current law (title 10, section 12310, *Duties Relating to Defense against Weapons of Mass Destruction*)

1. OUSD (Policy) briefing, undated, "Building Partnership Capacity with Section 1206."

prohibits use of National Guard WMD Civil Support Teams outside the United States. These teams are at the core of U.S. domestic WMD capabilities and their members are the subject matter experts who can most effectively train and assist U.S. partners in developing their own capabilities. In a related example, the funding for the National Guard State Partnership Program remains based on yearly supplemental appropriations. Begun in 1993, this program has established 56 partnerships between National Guard Joint Forces Headquarters and foreign countries on every continent and in every region of the world.

Overall, the factors described here create a gap in how DOD conducts building partnership capacity. Despite its strong rhetorical support, these programs are woefully under-resourced. Moreover, building partnership capacity does not address in any substantial way helping allies and partners *prepare to fight through WMD*.

To truly build partnership capacity, DOD must increase its emphasis on and expand its vision of this important set of activities. While the current effort is well meaning, it needs to grow significantly beyond its current *ad hoc* and meager funding levels. DOD must also expand its vision in this area to include preparing allies and partners to "fight through" WMD. A new vision for building partnership capacity will create opportunities to expand proven programs and establish other initiatives for key target regions and countries in the coming years.

RECOMMENDATIONS: BUILDING PARTNERSHIP CAPACITY

DOD should establish a discrete program of not less than $500 million per year to enhance partners' capacity to "fight through" WMD.

In support of this program, the Under Secretary of Defense for Policy (USD [P}) should issue appropriate guidance (including measures of effectiveness) to develop strategy, assign responsibilities, allocate resources, and provide oversight. In addition, the Chairman, Joint Chiefs of Staff, should direct that combatant commanders are given more priority to building the capacity of partner forces and nations to fight through WMD.

USD (P) should direct recurring and stable programmed funding of $18 million per year for the National Guard State Partnership program.

DOD needs to continue to work to reduce obstacles that limit its ability to conduct activities that enhance partner capacity. This restriction prevents these subject matter experts from helping train U.S. partners to fight through WMD.

Preparedness to Fight in WMD

While U.S. forces are better organized and equipped today, they are not as well trained to fight in a WMD environment as they were during the Cold War. Emphasis on operating in a WMD environment has waxed and waned over several decades. The Army's interest in the offensive application of nuclear weapons peaked during the 1950s with the "Pentomic Division" experiment, and then diminished rapidly as the Vietnam War became the Army's principal mission. When focus shifted after Vietnam back to defense of Europe, the prospect of having to fight on a dirty battlefield again caught the Army's interest, probably reaching its peak just before the collapse of the Soviet Union. Ground units and land-based air units routinely practiced operating in full protective gear for extended periods and trained to perform their wartime missions in a nuclear, biological, and chemical (NBC) environment. Soldiers and airmen who faced the Warsaw Pact *expected* to be attacked with chemicals, and thus gave serious attention to learning how to survive in such an environment.

Emphasis on chemical defense continued after the fall of the Soviet Union, particularly in the run-up to Operation Desert Storm and later Iraqi Freedom. Thinking about and training for operations in a nuclear environment dropped off sharply, however, and even chemical defense preparedness began to diminish once the WMD that was expected to be encountered in Iraq could not be located.

Today, as units cycle through training in preparation for rotations to Iraq and Afghanistan, little time is devoted to training for operations in an NBC environment. Despite the acknowledged need for plans to be visibly and successfully exercised in order to provide maximum deterrent effect on potential adversaries, most WMD war games and exercises end when the adversary uses nuclear or chemical weapons; few address the issues associated with fighting on despite their effects. Korea is an important exception: there, the proximity of a major chemical threat motivates a much higher degree of readiness.

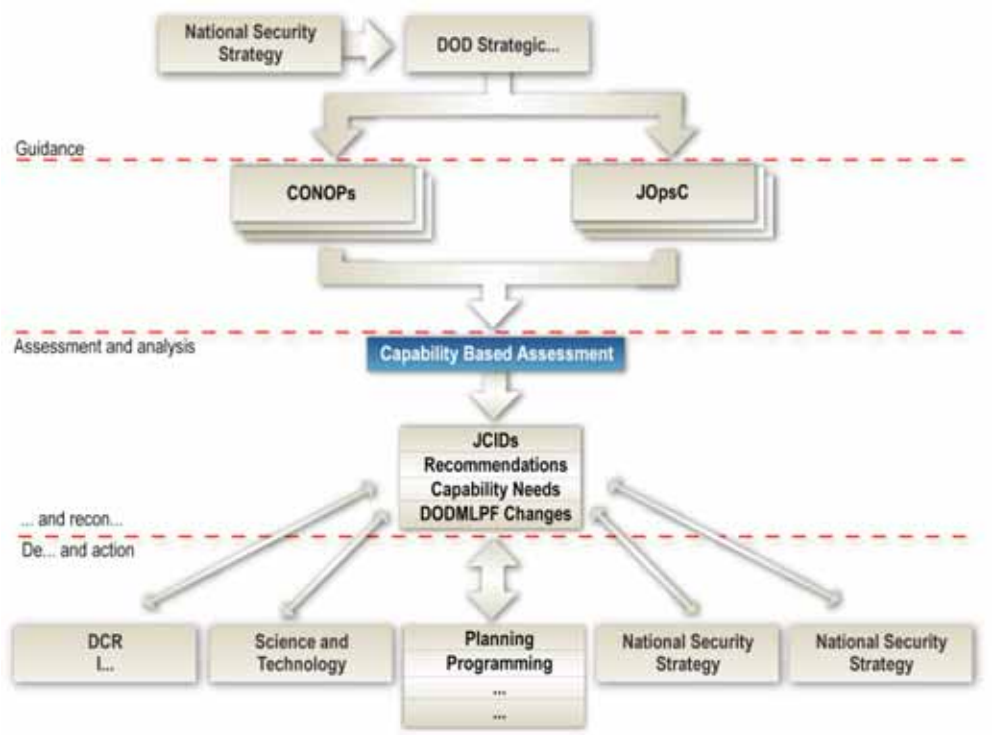
After the break-up of the Soviet Union, emphasis within DOD shifted to counter-proliferation. This term was later subsumed as part of "combating WMD," derived from the goal stated in the *National Security Strategy* of preventing enemies from threatening the United States, its allies, and friends with weapons of mass destruction. Consistent with the intent declared in the *National Security Strategy* to act preemptively, if necessary, to forestall or prevent such hostile acts, the "combating WMD" policy and doctrine, as implemented to date, appear to be focused more on defeat of the weapons themselves than on fighting a campaign against an adversary possessing and prepared to use them. The *National*

Military Strategy to Combat Weapons of Mass Destruction, published in February 2006, more clearly articulates the need to continue operations in a WMD environment after first use by the adversary, but supporting policies and doctrine lag.

The Joint Capabilities Integration and Development System (JCIDS), illustrated in Figure 6-1, uses joint concepts to identify and describe shortcomings and redundancies in warfighting capabilities, identify the timeframe in which the shortfall or redundancy exists, describe effective solutions, and identify potential approaches to resolve those shortcomings. The JCIDS process is initiated through the execution of a capabilities-based assessment, which identifies the capabilities required to successfully execute missions, the shortfalls in existing weapon systems to deliver those capabilities and the associated operational risks, and the possible solution space for the capability shortfalls. A capability-based assessment may be based on a Joint Integrating Concept (JIC) approved by the Joint Requirements Oversight Council; a concept of operations endorsed by a combatant command, Service, or defense agency; or an identified operational need.

A JIC is part of the family of future Joint Operations Concepts (JOpsC) developed from top-level strategic guidance to provide a top-down baseline for identifying future capabilities. New capability requirements must relate directly to capabilities identified through the family of future joint concepts. Therefore, the future concepts are not intended to provide immediate solutions, but rather proposed solutions that can afford careful examination over a more extended period of time. A concept of operations may indicate short-term capability needs. Concepts allow the joint community to adjust or divest current capabilities by providing the operational context needed to justify or modify current programs. The process flows from national level and strategic guidance through either a concept of operation for short-term needs or the JOpsC family of concepts, as shown in Figure 6-1.[2]

2. CJCSI 3170.01F, Joint Capabilities Integration and Development System, 1 May 07, and CJCSM 3170.01C, Operation of the Joint Capabilities Integration and Development System, 1 May 07. Both accessed 14 Aug 07 at the Joint Electronic Library website, http://www.dtic.mil/cjcs_directives/index.htm



Source: CJCSI3170.01F. Joint capabilities integration and development system, 1 May 2007, Figure A-1, page A-3

Figure 6-1. JCIDS Top-Down Capability Needs Identification Process

Assessments to determine the capabilities needed for combating WMD, or for *combat in WMD*, have been at best interim steps because the front-end conceptual basis has not been available. The Capstone Concept for Joint Operations, part of the JOpsC, highlights the WMD challenge, but offers no ideas on what do to about it. The Joint Forcible Entry Operations JIC mentions nuclear and chemical weapons only twice, as something from which to protect the force. The Major Combat Operations Joint Operating Concept addresses the challenge in much greater depth, and includes the following proposed assessment plan:

> **Operations against an adversary with weapons of mass destruction.** Future adversaries will pursue nuclear WMD to offset their inability to respond to the overmatching conventional military capability of the United States and its partners. Those future adversaries that are successful in developing a nuclear WMD capability will have a significant deterrent to US military engagement when our National interests are threatened. Furthermore, the US must consider preemptive and other actions (e.g., ISR) that may serve as triggers to use or disperse nuclear weapons and other WMD. Finally, the US must consider response courses of action in the event the adversary uses WMD and must

> consider second- and third-order effects of WMD use. National policy and guidance are undefined on how to deal with an irrational or rogue actor with limited WMD capability. This has operational implications in regard to preemption, shaping, and response. Operationally, the US and its potential coalition partners lack sufficient capability to locate, identify, track, and contain nuclear weapons and other WMD. Operational approaches to destroy, neutralize, observe or capture WMD hinge upon US ability to find and track them in hardened, deeply buried locations. Failing this, the United States and multinational forces must be prepared to project force and protect forces in a CBRN environment. A US and perhaps allied policy of preemption in light of potential triggering must be considered.
>
> **Potential Experimentation Methodology:** Craft a focused, controlled experimentation environment that promotes scenarios that challenges [sic] our ability to locate, identify, track and contain WMD and that can simulate potential capability solutions.
>
> The scenario(s) must describe an environment that will allow for analysis of the adversary's WMD capabilities, adversary's will to use WMD, possible target areas in US homeland and multinational partner nations, and US/allied responses and deterrent policies needed to respond to actions taken by the adversary.
>
> Because of its critical nature and high priority, a series of events dealing with combating WMD and solving WMD-related issues should culminate in a focused event and a senior leader review.[3]

This proposed experimentation methodology has not been implemented.

A Combating WMD JIC, authored by U.S. Strategic Command, is nearing completion. Once approved by the Joint Requirements Oversight Council, this concept will provide the basis for a formal assessment of the capabilities needed for operations in a WMD environment. Such a capabilities-based assessment should address a number of larger campaign scenarios to provide the necessary context, ranging from major combat operations as noted above to irregular warfare and military support to stabilization, stability, transition, and reconstruction operations to combating WMD in the context of homeland security operations. The current joint doctrine for operations in NBC environments points out correctly that the basic principles of operations in NBC environments apply to military operations other than war. The joint force commander and joint force

---

3. Major Combat Operations Joint Operating Concept, Version 2.0, December 2006, pp D-4 and D-5. Accessed 14 Aug 07 at the Future Joint Warfare website, http://www.dtic.mil/futurejointwarfare/joc.htm

elements must be prepared for NBC use and contamination with toxic materials at any point, including the transition from non-combat to combat environments.[4]

As noted above, future concepts like the Combating WMD JIC are intended to provide proposed solutions that can afford careful examination over a more extended period of time. Under JCIDS, short-term capability needs can be assessed based on a concept of operations to allow the joint community to adjust or divest current capabilities by providing the operational context needed to justify or modify current programs.

The recent approval of CONPLAN 8099 provides the basis for identifying near-term capability needs as geographic combatant commands develop supporting plans. The concept of operations they develop can provide the context needed to assess current capabilities.

In summary, without a set of capabilities-based assessments developed from sound strategy, sound concepts, and a range of campaign scenarios, the Department has no way of knowing whether current capabilities are adequate for operations in an NBC environment, or what new capabilities might need to be developed.

RECOMMENDATIONS: PREPAREDNESS TO FIGHT IN WMD

To improve capabilities to conduct military operations in an environment contaminated by WMD, the study makes the following recommendations:

The JROC should direct a series of capabilities-based assessments to identify capability needs and gaps for operating in a WMD environment.

These assessments should be based in the near-term on concept of operations developed by geographic combatant commanders in response to the Combating WMD CONPLAN and, in the longer term, on the Combating WMD Joint Integrating Concept, applied to a wide range of scenarios.

Joint Forces Command should conduct a series of experiments, with the support of U.S. Strategic Command's Center for Combating WMD, to

4. Joint Publication 3-11, Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments, 11 July 2000, pg. VI-2. Accessed 14 Aug 07 at the Joint Electronic Library website, http://www.dtic.mil/doctrine/doctrine.htm

explore WMD-related issues associated with operations in a WMD environment.

Chairman, Joint Chiefs of Staff should direct the combatant commands to place particular emphasis on joint and multinational exercises where "fighting through WMD" is a main objective.

Such exercises will serve to enhance deterrence and help geographic combatant commanders gain awareness of the capabilities and limitations of their own forces and of host nations and partner forces, when operating in such an environment.

Small-Scale Nuclear Attacks

The greatest threat from WMD, in terms of consequences, will come from the use of nuclear weapons. As declared in the *National Military Strategy to Combat Weapons of Mass Destruction*, the nation's military strategic goal is to ensure that the United States, its armed forces, allies, partners, and interests are neither coerced nor attacked by enemies using WMD. Deterring or disarming a determined nuclear-armed adversary is, of course, the preferred course of action. But it is necessary also to be prepared to minimize the effects of an attack and continue to operate should such an attack occur.

Given current U.S. methods of operation, forces overseas can be vulnerable to even a small-scale nuclear attack involving as few as one or two weapons. Current operations in Iraq illustrate this vulnerability. Leading up to Operation Iraqi Freedom, the United States was limited to moving personnel and equipment through the air and sea ports of debarkation in Kuwait. A second route into the theater through Turkey was anticipated but was foreclosed by the Turkish Parliament. Preparations for operations continued in Kuwait, with all forces required to move through a single port complex. Had that port complex been attacked by even an improvised nuclear device, deployment operations and the ensuing reception, staging, onward-movement, and integration would have been severely disrupted—perhaps even brought to a complete halt.

Another example of current vulnerability to the use of nuclear weapons comes from the increased use of maritime forces closer to shore. Tactics, techniques, and procedures have not evolved to address the increase in maritime operations in the littorals, where the WMD threat, particularly from nuclear weapons, is greater than that in deep water.

Hardening equipment against the nuclear threat includes protection from blast, thermal, and EMP effects. Hardening is expensive and, given pressures to cut costs, seldom receives more than cursory consideration during equipment development. Once a program has moved past the design phase, it is cost-prohibitive to redesign the equipment to meet hardening criteria. Information availability is critical for net-centric operations. The physical layout of command and control systems varies from theater to theater based on geography and availability of systems. Since a network failure could be catastrophic, vulnerability analyses of C4ISR networks is essential to identify potential points of failure.

RECOMMENDATIONS: SMALL-SCALE NUCLEAR ATTACKS

To reduce vulnerabilities to small-scale nuclear attacks, the study makes the following recommendations:

U.S. Strategic Command's Center for combating WMD should work with combatant commanders to visualize potential nuclear effects and construct plans for fighting through them. Modeling and simulation tools are available that can help with visualizing, understanding, and mitigating these effects.

DISA should develop tools for network analysis that will allow joint force commanders to assess the vulnerability of C4ISR systems to nuclear effects based on their physical locations. Analysis should identify ways to reduce critical node vulnerability, establish redundancy requirements, and identify options for degraded operations and reconstitution.

Secretary of Defense direct the Defense Threat Reduction Agency and the Defense Information Systems Agency to assess the utility of applying nuclear hardening techniques to discrete network elements using combinations of shielding, redundancy, and radiation-hardened components.

A renewed emphasis should be placed on nuclear hardening for equipment vulnerable to EMP. It will be cost-prohibitive to harden all systems, but some systems critical to network operations may warrant the extra cost. Emphasis should be placed on ensuring acquisition programs consider hardening during equipment design, and test against the effects during development. This is a department-wide issue. All services need to buy into hardening against EMP. If not, portions of C4ISR networks that are vulnerable to EMP effects will impact other systems. Redundancy must also be considered.

Chapter 20. Countering Attacks on U.S. and Allied Space Assets

The United States and its allies depend heavily on space assets to enable many critical services, including ISR, precision navigation and attack capabilities, beyond line-of-site communications, and weather and environmental data. U.S. adversaries recognize this dependence on space and will most certainly attack U.S. and allied space assets. The United States must assume that it will be challenged in space and should expect to respond to attacks in space. If the armed forces are not well trained and equipped to respond to such attacks and capable of maintaining space superiority, an adversary may very well attempt to use attacks in space to drive a wedge between the United States and its warfighting partners. The less prepared the nation is to defend its space capabilities, the greater the likelihood that these assets will be attacked.

Three key elements of any effort to counter attacks on U.S. and allied space assets are:

1. gaining and maintaining space situational awareness
2. conducting defensive and offensive counter-space operations
3. conducting combat operations when space capabilities are degraded

Impact of Attacks on Space Assets

Recently, space has ceased to be the above-the-battle "sanctuary" it was in the past. Forty-four countries now have assets in space. No nation, including the United States, is well prepared to defend against attacks in space. A serious attack against U.S. space assets would have grave consequences not only for the United States and its allies, but also for the world economy. Due to their technological sophistication, the United States and its allies are particularly vulnerable to a catastrophic attack in space.

Such an attack would not only severely degrade U.S. and allied military capabilities but also would create troubling economic and political issues worldwide. Economically, an attack on space assets can impact international exchange and stock markets and banking systems, and degrade commercial navigation. Political leaders will have to face allies who will look to the United

States for leadership and assistance in response to such an attack. Alliances, coalitions, and partnerships could be undermined based on the U.S. response.

The types of attacks on U.S. space assets that could deny the United States critical space situational awareness, and seriously degrade its command, control, intelligence, surveillance and reconnaissance (C2ISR) capabilities include:

- attacks against the U.S. GPS capability, leaving navigation and precision attack capabilities seriously degraded or denied
- jamming sophisticated military weapons systems that rely heavily on a precise GPS timing signal
- degrading satellite communications systems that carry essential military voice and data transmissions

Conducting joint warfighting operations in such an environment will be, at best, extremely challenging for U.S. forces. At worst, it could mean defeat for the United States and its allies. Action must be taken now to reduce military reliance on space capabilities. Furthermore, the United States must develop the capability to carry out defensive and offensive counter-space operations in defense of its space assets.

Space Situational Awareness

Space situational awareness is important to protecting space capabilities. If DOD forces cannot assess, characterize, or attribute an attack to its source, then executing an effective response will be all but impossible. Yet maintaining situational awareness in space is becoming increasingly difficult. From 1957–1961, only four objects existed in low earth orbit to track and catalog. In the decades since, forty-four nations and several commercial enterprises have placed objects in space. Low-earth orbit and geosynchronous earth orbit positions are becoming increasingly crowded. With both government and commercial entities launching tactical mini- and nano-satellites, space objects are becoming smaller and more numerous. All of this makes the job of maintaining space situational awareness much more complicated.

Moreover, space debris is becoming a bigger problem. Recently, government and commercial satellites have been maneuvered to avoid collisions with other space objects. Services from those satellites are normally suspended during the maneuver and precious onboard fuel is consumed.

The number of objects in space will continue to grow and their average size will become smaller, making the maintenance of situational awareness in space ever more difficult. The United States and allies will have to develop and implement the capability to detect and track micro- and nano-satellites, as well as debris from objects that break up in space. Physical attacks on satellites or other objects in space will produce debris that must be tracked and catalogued in order to maintain an accurate situational awareness.

Figure 6-2 illustrates the tremendous growth in the number of objects orbiting the earth since the launch of Sputnik in 1957. The blue line (top) depicts the total number of objects cataloged over time; the red line (middle) the number of objects that have decayed; and the yellow line (bottom) the number of objects currently catalogued on orbit. The sharp upward spike in cataloged orbital objects in 2007 was caused by debris from the Chinese anti-satellite test—which demonstrated China's capability (and perhaps intent) to attack satellites in low-earth orbit.

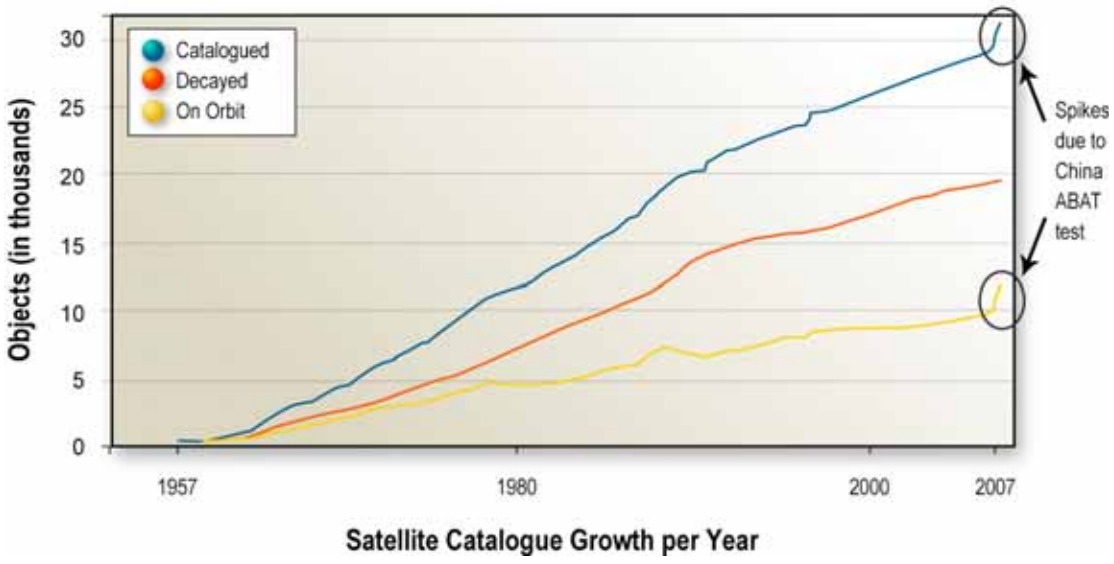


Figure 6-2. Growth Challenges to Space Situational Awareness

In light of this demonstrated capability, this study recommends that DOD immediately initiate a program to upgrade the U.S. Space Surveillance Network (SSN) to enable it to track the growing class of smaller objects in space. It would be extremely difficult to maintain accurate space situational awareness if an adversary simultaneously attacked multiple satellites due to the amount of debris that would be created. The SSN would become oversaturated with the sheer

number of objects it would have to process and catalog. Further, with current sensor technologies, very small debris may be impossible to track.

Additionally, DOD should consider initiating a program to develop the capability to de-orbit objects (debris) from space. In the future, this mission may be carried out by small solid-state lasers.

Another major shortfall in the current SSN is the inability to cover space objects in the southern hemisphere (Figure 6-3). The current network was developed during the Cold War when there was little need for southern hemisphere coverage (Soviet launches were all to the north). However, with a shift away from Cold War coverage requirements and significant change in the global political and military landscape, the need for the United States to have solid southern hemisphere space coverage has become more critical.

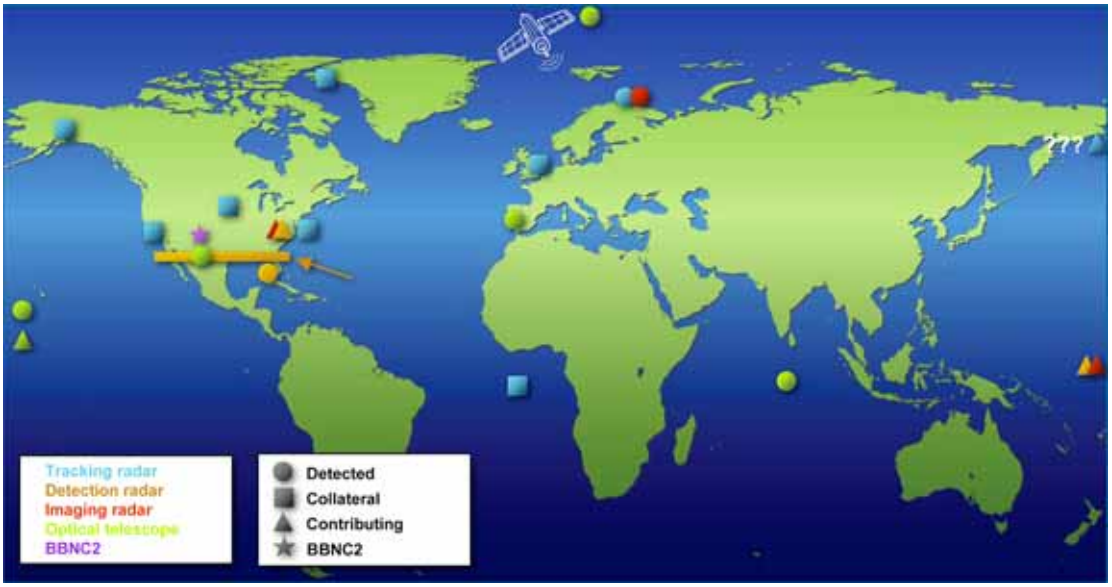


Figure 6-3. Current Space Surveillance Network

The Chinese are well aware of the gap in coverage of the southern hemisphere and frequently launch into those coverage gaps. The significance of a launch into these gaps is that it takes much longer to find, identify, and catalogue an object that would otherwise be tracked and tagged in a few hours. The gap in coverage makes it far more difficult to discern the true purpose or activities of a launched object with respect to U.S. space assets during the period of time that it

is undetected and unidentified. Therefore, the study recommends that DOD improve SSN coverage, especially in the southern hemisphere.

With the steady increase in the number of objects orbiting the earth, the SSN is becoming saturated. The SSN's processing capabilities have remained unchanged since 1994. Consequently, the task of tracking and cataloging space objects is becoming increasingly difficult. Often, small debris cannot be tracked at all. Some universities are now teaching the process of developing and launching micro- and nano-satellites—so the information is becoming more widely available. These very small satellites can now be rather easily launched into orbits where the SSN cannot see them.

Therefore, new ground-based sensor capabilities—like solid-state laser radars or light detection and ranging (LIDAR) lasers—need to be developed and integrated into a modernized SSN. Space-based components of the network may be needed as well. Furthermore, legacy radio frequency radar sensors in the SSN will most certainly need to be upgraded, and more processing power added to ensure the United States has the capability to detect, identify, catalog, and track what is projected to be even more numerous and ever smaller objects in space.

Another major issue with regard to maintaining space situational awareness is the lack of an automated space common operating picture or a "single integrated space picture." Current displays in command centers are created manually and information about who is doing what in space is spread among several disparate databases that reside in a variety of locations. It will be virtually impossible for personnel working in command centers to manually track what is occurring in space if an adversary begins to attack multiple assets over a short period of time. Attack assessment and target characterization will be next to impossible if the space common operating picture remains a manual system.

More intelligence resources need to be focused in the space area, as well. Space has been a sanctuary in the past; thus, few national resources have been dedicated to gathering intelligence in this area. Since there are several indications (including the Chinese ASAT test) that the threat to U.S. space capabilities is increasing, more intelligence is needed on what nations are developing capabilities in this area. Special emphasis should be placed on gathering foreign intelligence about offensive space capabilities that are in development.

Furthermore, the process for determining space post-attack response options is not well defined. For example, if an attack in space occurs, there is not an agreed process for how attack notification occurs and who is responsible for making those notifications. Furthermore, there is no national process for how

potential response options will be developed, debated, and/or executed. Finally, there is currently no process for how allies will be notified and/or how commercial entities will be involved if one of their assets is attacked or involved in post-attack maneuvers. Needless to say, much work is needed in this area if post-attack responses are to be well-conceived, properly debated, and effectively executed in a timely manner.

Tools and systems for countering attacks in space are insufficient given the documented threat. While there have been some initial defensive and offensive capabilities considered, these capabilities have not been proliferated in any number, nor have sufficient military units with such capabilities been fielded. As threats to U.S. and allied space capabilities increase, much more work will be needed to develop this capability.

DOD needs to undertake a major effort to provide a sound intellectual foundation for protecting assets in space and for conducting space control negation and prevention. The Department also needs to improve policy guidance, joint space warfighting doctrine, delineation of responsibilities, and rules of engagement.

Additionally, today the United States and its allies have a very limited capability to know when an attack in space occurs. Attack characterization and assessment capabilities need significant improvement, and better ways to determine the identity of the attacker are needed. Furthermore, there currently is not an effective process for coordinating an international response to an attack in space. This is an area where further discussions among nations will be needed as threats to international space capabilities increase.

These are some of the reasons why the study has concluded that improving space situational awareness is really "job one." As previously noted, if DOD forces cannot assess, characterize, or attribute an attack to its source, executing an effective response will be all but impossible.

RECOMMENDATIONS: SPACE SITUATIONAL AWARENESS

DOD needs to field an improved Space Surveillance Network that produces an automated single integrated space picture; incorporates southern hemisphere coverage and new sensor capabilities; and supports distributed, collaborative space command and control operations.

Improvements are needed to the Department's space situational awareness capabilities. The first is to field launch, flight trajectory following, and tracking sensors/fences to expand the SSN coverage from its current northern hemisphere focus into the southern hemisphere. Sensor improvements, including capabilities to track small objects and laser-derived tracking and surveillance, are needed as well. Moreover, application of air-, space-, and ground-based sensors to space surveillance should be considered. The development and the fielding of a program for a common operational picture for space awareness and a collaborative information environment for space control, both of which must be operable at multiple security levels and include inputs from coalition, commercial, other DOD, and intelligence community assets, are also recommended.

The services need to begin incorporating attack assessment/attack reporting sensors on key space assets.

Development of sensors capable of attack indications and warning, and their incorporation on key designated space assets prior to launch, will provide significant leverage to space situational awareness.

Under Secretary of Defense for Intelligence request the Director of National Intelligence to focus additional national intelligence resources on collecting and analyzing space intelligence.

Critical, too, is an emphasis by the intelligence community on allocating more resources focused on collecting, analyzing, and reporting space-related intelligence.

Space Control

DOD must improve its training, education, and exercise efforts to incorporate much more realism with respect to adversary attack and exploitation of space capabilities, and the use of effective counter-attack and counter-space measures in the wake of such attacks. The work the Department has already undertaken to develop an effective information operations training "range" should be expanded to include similarly effective space capabilities. Perhaps even more important, DOD needs to develop and field a responsive, viable reconstitution program (*i.e.,* in a matter of hours to days, vice months or years).

The Department can and should pursue a number of options to mitigate against catastrophic loss of critical space-based capabilities, as described in Figure 6-4. These options focus either on time-sensitive (within hours-to-days vice months or years) reconstitution of lost space-borne capabilities, or on establishing alternatives that can even be fielded today that would reduce reliance on space.

Space Capability	Orbit	Vulnerability Kinetic/Non-kinetic	Alternate Sources	Reconstitution Priority	Reconstitution Need (within hours)
Imagery Intelligence	LEO	High/High	Aircraft and UASs	2	UAS, NT-ISR, LTA UAS
Satellite Communications	LEO & GEO	LEO High/High GEO Low/High	Terrestrial towers, line-of-sight and airborne relay	4	ORS, HAE UAS, LTA UAS
Precision Navigation	MEO	Medium/ Medium	No alternate source	1	Pseudolites, LTA UAS
Signals Intelligence	LEO & GEO	LEO High/High GEO Low/High	Aircraft and UASs	3	ORS, UAS, LTA UAS
Weather	LEO & GEO	LEO High/High GEO Low/High	Terrestrial observations and aircraft	5	ORS, LTA UAS

Figure 6-4. Space Reconstitution Program Options Needed

Some of these options entail non-space alternatives. ISR sensors, communications, and other payloads could be flown on "near-space" (*i.e.,* 65,000 to 325,000 feet altitude) lighter-than-air, unmanned aerial systems (UAS). Some research and development work in this area has been accomplished (DARPA's "ISIS" project, for instance), but the study recommends a more concerted approach leading to fielded operational platforms and systems.

Likewise, DOD is fielding next-generation weapon systems such as the F-22 Raptor and F-35 (Joint Strike Fighter) that, along with certain older platforms like the F/A-18 and F-15E, carry a plethora of highly capable radar and other sensors. These potential sources of "non-traditional ISR" could be networked via common data-linked airborne and surface communications gateways—offering significant potential for complementing conventional but low density/high demand architecture of space-based and air-breathing ISR capabilities.

DOD should also continue efforts looking at flight testing and eventually fielding a number of launch-on-demand "operationally responsive" space capabilities. These small, low earth orbit satellites could provide a capability to rapidly reconstitute at least some functionality in the wake of catastrophic attack against space-based ISR, navigation, and/or communication systems.

RECOMMENDATIONS: SPACE CONTROL

Under Secretary of Defense for Policy articulate policy on protecting U.S. and allied space capabilities. Include guidance on sharing space situational awareness information and coordinating response options.

U.S. Strategic Command develop joint space control doctrine; concepts of operations; and tactics, techniques, and procedures

Services improve both defensive and offensive space control capabilities. Harden satellites, add attack detection sensors, improve ground station physical security, and add redundant and secure communication means.

Develop a rapid global strike capability.

U.S. Joint Forces Command incorporate realistic space threats and space control play into education, training, and exercise programs. Also upgrade information operations range to incorporate space range capabilities.

U.S. Strategic Command develop a responsive space reconstitution program.

Operations in a Degraded Space Environment

Equally vital is the need to improve capabilities to operate despite a degraded space environment. An important element of such capabilities is to field the Global Information Grid (GIG) with a robust network that has redundant communications means, alternative waveforms, redundant data sources, and automatic communications rerouting capabilities. It should be engineered in such a way that a loss of satellite communications will not impact the operational user.

The Air Force's Objective Gateway program is just initiating the development of an airborne communications gateway that interfaces with ground communications nodes (RAIDRS) that will allow interoperability with the commercially available global fiber network. When this capability is fully developed, military communications (voice and data) can be routed either

through space or, if satellite communications are degraded or denied for any reason, via airborne communications relay capabilities and then through ground nodes connected into the global fiber network. When auto communications relay capabilities can be integrated into such an architecture, the GIG will be much more robust and reliable than what is available today to support global military operations.

Potential adversaries will recognize the critical importance of GPS to U.S. and allied military capabilities. It is therefore likely that they will attack the GPS constellation or attempt to jam the signal with GPS jammers. GPS jamming was already attempted in Operation Iraqi Freedom. In order to reduce U.S. reliance on the presence of an uninterrupted and accurate GPS signal, accurate inertial measurement units (IMUs) and "atomic clocks on a chip" should be integrated into DOD systems whenever practicable. IMUs have already been integrated into many GPS-based navigation and attack systems to compensate for positioning errors, but technical capabilities in this area are constantly improving. Better IMUs should be incorporated into new systems and added to older systems as they are being modified, whenever possible.

DARPA is about to field an "atomic clock on a chip," which would allow very accurate system timing to be maintained during times when GPS signals are interrupted. These chips should be incorporated into future systems along with more accurate IMUs. An accurate timing signal is as important to some systems as an accurate positioning signal is to other systems. A disruption of GPS in the United States could result in difficulty supporting a deployed force.

Another way to limit U.S. reliance on space capabilities is to ensure that a mix of weapons and terminal guidance systems is maintained in U.S. arsenals. Currently this is the situation because legacy weapon systems did not rely on GPS. However, as weapons and weapon systems are modernized, a mix of capabilities should be retained. Developers should resist the temptation to go to all GPS-based systems, for example. Electro-optical and laser-guided systems, as well as TERCOM-type guidance systems should remain in the overall U.S. and allied weapons inventories.

Finally, U.S. Joint Forces Command and geographic combatant commands should incorporate realistic degraded space scenarios into future joint and combined war games and exercises. Also, improved modeling and simulation capabilities may be required to create a realistic "degraded space environment." In addition to better modeling and simulation capabilities, the study recommends

that JFC seek to incorporate both information operations and space range training capabilities onto live-fly and maneuver ranges so that realistic training can be conducted to prepare the joint force for future conflict.

RECOMMENDATIONS: DEGRADED SPACE ENVIRONMENT

The Assistant Secretary of Defense for Networks and Information Integration, the Defense Information Systems Agency, and the Services field a Global Information Grid that has redundant communication means and waveforms with auto-communication rerouting capabilities.

Services field systems with highly accurate and reliable inertial measurement units and incorporate "atomic clocks on a chip" for timing signal.

Services ensure a mix of terminal guidance systems and weapons in the nation's arsenal—not only GPS-guided weapons.

Joint Forces Command incorporate realistic exercise scenarios into joint and combined exercise that emphasize degraded space capabilities.

Services incorporate training in degraded space environment on live-fire training ranges.

Chapter 21. Cyber Warfare Against Information and Networks

Cyber attacks can be launched against the networks through which information is transferred, or against the information itself with the objective of destroying or corrupting it. Two themes pervade this chapter:

1. Defense against cyber attacks is not just about ensuring networks remain operable and the information uncorrupted. It is also about preparing traditional kinetic forces to operate in an environment where the networks and information they use are under attack.
2. Cyber defense is not just defense *per se*, but also the integrated application of cyber attack and exploitation in support of defense.

In keeping with these two themes, cyber warfare is defined as actions conducted in cyberspace—computer network defense, attack, and exploitation—plus the actions taken by kinetic forces to conduct operations in the face of cyberspace attacks. While some parties consider electronic warfare and directed energy to be part of cyber warfare, they are not included here. In addition, for the scope of this work, cyber attack is included insofar as it supports cyber defense, but not as an offensive means for other purposes (*e.g.,* to disable an air defense system).

The Cyber Warfare Threat

Adversaries conduct cyberspace operations against the military forces of the United States and its allies and partners for two reasons: 1) attack to degrade the effective use of information and 2) exploitation to steal classified and unclassified information about our cyber and kinetic capabilities. More specifically, the objectives of cyber attack are: denial of information access and/or transfer, corruption of information and services, and destruction of information and services. Corruption is perhaps of most concern. If military forces lose network capacity, they understand what has happened and possibly can deal with it; but if data are found to have been altered, then trust may be lost in the validity of all data.

Attack and exploitation are executed in three ways: 1) remote access in which operators on a network illegitimately gain access to their adversary's networks and nodes, 2) close access in which the adversary's networks and nodes are physically penetrated, and 3) life cycle insertion in which illegitimate hardware and software are surreptitiously implanted during the life cycle of network and nodal components (*e.g.,* in development or maintenance), with the intent of later using these implants for attack or exploitation. Close access is typically used against closed networks (*i.e.,* those not accessible from the Internet), which would typically be classified and, in some cases, highly sensitive. Remote access would be used against the numerous DOD and civilian networks accessible from the Internet, but could also extend to classified networks connected to unclassified ones if the guards providing the connection could be subverted.

While particulars are classified, the following key observations can be made about the implications of existing and anticipated threats:

- Real-world incidents and red team activities show U.S. military networks have **major, widespread vulnerabilities.** Peer or near-peer adversary capability to penetrate U.S. military networks must be accepted as a fundamental planning assumption.
- **Attacks against U.S. and allied/partner civilian infrastructure are a high-leverage option for coercive purposes.** For example, in the face of a pending military operation, or even a serious political or economic dispute, an adversary could attack U.S. utility or financial systems as a warning to the general population that the United States should back off, or even greater pain could be inflicted.
- **Major adversaries may exceed the United States in cyber capabilities.** The relevant technology is global, so it is not likely the United States would have a significant advantage in technology. Highly skilled technical people are a critical component of the capability, too, and some potential adversaries have a much larger base of such people than does the United States.
- While high visibility Internet attacks can focus attention on remote access attacks, **close-access penetration and life cycle insertion may be the most serious threats in the long term.** These two threats, which are getting the least attention now, could be the hardest to defend against and could affect the most sensitive U.S. systems. Peer or near-peer intelligence agencies are expected to be well practiced in close-access and life cycle insertion, as well as in remote access attacks.

Cyber Attack and Exploitation

Cyber attacks can disrupt operational forces in a number of ways. Not only could their access to information be denied, but possibly more important, the information could be corrupted, thereby leading to a loss of confidence in all information.

However, the cyber threat is not a case of "one size fits all." A few spectacular penetration examples do not imply the complete vulnerability of the force. Rather, there are significant differences in the ease and means of penetration depending on command involvement and level of preparedness, the type of network (NIPRNET and SIPRNET [DOD's unclassified and classified networks], other wide-area classified networks, and tactical networks), and effects sought from the attack or exploitation. Examples of the type of effects that might be sought include disruption of command and control of forces, deny or corrupt situational awareness, deny or corrupt mission support information (targeting, navigation, intelligence, logistics), disrupt battle management and weapon system execution, compromise force status and location information, compromise plans and intelligence, and disrupt force deployment and sustainment. Thus, to counter the threat, planners of military operations must proceed in a systematic way by considering the specifics of the threat, the vulnerabilities of the different networks employed, the protection provided by in-place defensive measures, and the objectives of the forces affected.

Cyber attacks against the civilian infrastructure could include several types. Two particularly stressing kinds would be attacks against financial and banking systems, and attacks against the supervisory control and data acquisition systems that control, for example, electricity generation and water distribution. Cyber attacks against U.S. infrastructure have long been a concern. Because of their coercive potential, attacking the infrastructure of allies and partners can also have serious and direct ramifications for the United States. That is, an adversary could inflict cyber "pain" on civilian populations of allies and partners as a means to get them to withdraw their support (troops, basing rights, etc.) for the United States in a crisis or conflict. To remain a credible partner, the United States would have to provide defensive support to the attacked country. This type of contingency does not seem to have received much consideration in DOD (although the recent Estonia attacks may have spurred some planning efforts).

There are two critical aspects to the development and execution of successful counters to cyber attack and exploitation. The first is recognizing that

responsibilities fall to both operational commanders and technical specialists—commanders of the "old fashioned" kinetic forces must prepare those forces to operate in an environment of degraded networks and information. Contingency plans and reconstitution processes must be thought through and practiced in advance. The second critical aspect is that U.S. cyber exploitation and attack need to be fully applied to its cyber defense. U.S. forces use computer network exploitation to understand the battle space, and computer network attack to respond to and defeat attackers.

To expand on the second point above, the following gives a systematic set of steps for conducting cyber defense with integrated support of cyber offense:

- apply computer network exploitation and "traditional" intelligence to understand the nature of the threat
- maintain situational awareness of networks
- provide indications and warning of impending attacks/exploitation
- maintain computer network defense in depth
- detect network penetrations rapidly
- respond rapidly to control damage and counterattack, possibly employing preemptive attack
- restore degraded networks and corrupted data

In short, defense against cyber attacks and exploitation should apply the broadest set of means possible, as is the case in any warfighting operation.

Improvement Efforts

The task force examined a number of ongoing efforts aimed at enhancing the U.S. posture for countering the cyber warfare threat, including national activities that cannot be further discussed here. While each of the efforts differs in its maturity and level of effort, significant shortcomings remain in DOD's readiness and capability to respond to cyber attacks:

- U.S. Strategic Command operational centers overseeing computer network defense and integrated support from National Security Agency (NSA) assets

- operational activities under service commands, such as the Army's 1st Information Operations Command, Navy's Network Warfare Command, and the Air Force's Cyber Command
- combatant command and service exercises assessing information assurance preparedness
- Chairman, Joint Chiefs of Staff development of *National Military Strategy for Cyberspace Operation* and follow-on products
- Deputy Secretary of Defense directed GIG mission assurance effort to ensure execution of essential functions in the face of cyber attacks
- Assistant Secretary of Defense for Networks and Information Integration (ASD [NII])/DOD Chief Information Officer (CIO) development of information assurance compliance policy
- programmatic developments, including several parties, such as ASD (NII)/DOD CIO, USD (I), NSA, and the Defense Security Agency
- classified national activities

Assessment and Recommendations

Given the nature of the threat and the actions being taken to counter the threat, including knowledge of the activities listed in the previous section, the study members chose eight assessment areas on which to focus. The eight areas are characterized as follows:

1. How well-**prepared are operational forces** to conduct their missions in the face of cyberspace attacks?
2. Are **inter-organizational relations** adequate for preparing for and responding to cyberspace attacks?
3. Have proper **command and control concepts and procedures** been developed for conducting cyberspace operations?
4. Is the **workforce** adequate for conducting cyberspace operations?
5. Are existing **acquisition plans and programs** adequate for defending against cyberspace attacks, and what improvements are required?
6. Are changes in **policy and legislation** necessary to enhance the ability to conduct cyberspace defense?
7. What is the role and responsibility of DOD in defense against **cyber attacks on the U.S. homeland**?
8. What concepts can be developed to **deter** cyberspace attacks?

Each area was carefully reviewed during the course of the study and a set of significant findings and recommendations determined. The recommendations fall into two categories: principal recommendations and additional recommendations. The difference is not intended to imply that the additional recommendations are less important. Rather, it was possible to build more substantial recommendations in the areas identified as principal.

Before moving to the individual assessments and recommendations, it is useful to identify the higher-order objectives that guided their development. The cyber warfare recommendations put forth in the following sections will enable DOD to:

- Gain a much deeper understanding of the effects of cyber attacks on operations, both current and future. It is difficult to develop strategies, plans, and programs without "ground truth."
- Strengthen defense against cyber attacks through the integrated application of attack and exploitation in support of defense, while paying particular attention to intelligence and situational awareness.
- Greatly expand preparation to operate in conditions of degraded information assurance. Even exquisite defense against cyber attacks cannot guarantee success.
- Be prepared to assume a role in homeland cyber defense, if that role should be assigned. Critical attacks on the homeland could lead the President to direct DOD support.

Preparedness of Operational Forces

To gain an understanding of the preparedness of the nation's operational forces, a set of questions about operational preparedness was posed to each of the military services. However, the clearest, most specific set of data on the subject came from the synopsized Information Assurance and Interoperability (IA&I) assessments of combatant commands and (to a lesser extent) individual service exercises. These assessments were prepared by the office of the Director, Operational Test and Evaluation (DOT&E). The detailed OT&E assessments for the individual exercises are carried out by each of the service's Operational Test Agency (OTA) in support of the combatant commands and the services.

Congress mandated that the DOT&E conduct information assurance assessments of Combatant Command and Service exercises. Since 2003, over 60

exercises have been assessed. The set of exercises for which DOT&E has conducted assessments is shown at the top of Figure 6-5. (Bold type indicates the exercises with the most significant information assurance assessments.)

Note: Congressionally mandated information assurance assessments begun in 2003 – 60+ conducted to date.

Source: Office of the Director, Operational Test and Evaluation

Figure 6-5. DOT&E Exercise Assessments

The results of these assessments are presented to combatant commands (typically to command J6s organizations) for their use in addressing vulnerabilities. The extent to which fixes have been implemented varies significantly from command to command.

There are two general questions to be assessed in the exercise results:

1. How good are the exercises from a cyber warfare perspective?
2. What do these exercises reveal about the operational preparedness of the U.S. forces?

The findings derived from the exercise results are:

- Cyber attacks are played regularly in combatant command exercises—but not all combatant commands are strongly engaged. Furthermore, red team activities are often restrained (a pending CJCS directive may strengthen cyber play in exercises).

- Red teams are allowed to test penetrations, but usually not allowed to exercise the consequences of those penetrations (data corruption, etc.).
- Extensive exercise data assessing policy compliance now exists, but assessments are just starting to address operational effectiveness.
- While exercises show some improvement in force preparedness, significant deficiencies remain.
- Exercise red team results indicate the ability to penetrate networks (details classified).

In sum, exercises continue to grow in terms of analytical sophistication (the data presented in the table in Figure 6-5 has become available only recently), but the means to truly assess operational impacts are just beginning to be developed. Additionally, significant shortcomings in the operational preparedness of the forces were routinely found.

The table at the bottom of Figure 6-5 is a summary, provided by DOT&E, of 52 assessments of policy compliance conducted from fiscal years 2005–2007, showing both current status and changes over the past three years. (This is a stoplight chart without any green; an orange assessment is intermediate between yellow and red.) Policy compliance is, in turn, one measure of the operational preparedness of the forces for dealing with cyber attack.

Two points follow from this table:

1. Improvements over the three-year span are limited and significant deficiencies remain.
2. The most significant deficiency is in the recovery and restoration category, which measures the ability of a force to resume an operationally effective state after being attacked.

After evaluating these assessments, the task force concludes that while regular series of exercise are conducted, these exercises provide little operational understanding of consequences of cyber attack. As a result, there are significant, continuing deficiencies in the information assurance posture of U.S. forces.

The information assurance assessments of combatant command exercises and discussions with joint and Service representatives indicate that a significant portion of the operations community is not seriously committed to preparing for and

operating against cyberspace threats. All too often, commanders and operators view cyber preparedness as a technical responsibility, not an operational one. Key to addressing this deficiency is the application of exercises and experiments, as well as "readiness reporting," to assess and report how well the deficiencies found in the exercises are being addressed.

While the combatant command exercises have been quite valuable in identifying cyber vulnerabilities and increasing awareness that they exist, exercises have generally stopped well short of putting stress on the forces in the way a capable adversary could. The forces need to be so stressed to bring home to them the operational consequences of such vulnerabilities and to test the plans the forces have developed for dealing with those vulnerabilities. Steps to provide for more stressing and operationally focused exercises are:

- progress from currently measuring information assurance compliance to measuring operational effectiveness in the face of cyberspace threats
- allow consequences of red team attacks to be played through fully (may require "resetting the clock" to allow the exercise to continue)
- institute process led by the combatant commands for capturing and disseminating tactics, techniques, and procedures, and lessons learned from exercises and real world operations for countering cyber attacks

One argument against playing stressing cyber threats through is they could lead to premature termination of an exercise if the force were wholly defeated, and thus preclude achieving other exercise objectives. This objection can be overcome by "resetting the clock" and resuming the exercise without playing the threat to its full extent the second time through.

Experiments allow greater free play and exploration than do exercises (while not providing as much of a venue for training). Extensive series of experiments are required for two reasons. First, to allow "traditional" forces to develop concepts of operations for dealing with cyberspace threats and operating with the degradations those threats will impose. The second reason is to develop the concepts for operating within cyberspace, which will require a high degree of interplay in highly time-sensitive situations between cyber defense, attack, and exploitation.

Given role of Joint Forces Command in joint concept development and experimentation and U.S. Strategic Command's role in computer network operations, both commands can collaboratively play a lead role in seeing that such experiments are undertaken. Outputs of the experiments in both cases

should include understanding how given cyberspace threats would affect operational effectiveness. Experiments in the second case (operating within cyberspace) will allow development of concepts for "cyber command and control," and should address such factors as rules of engagement, delegation of authority, and enabling "100 ms" responses. These experiments can build on and extend current activities using information operation ranges.

Ultimately, experiments and development of concepts for operating traditional forces in a cyber threat environment and operations within cyberspace should be carried out together, since they both contribute to overall operational effectiveness. But in the beginning, the two types of activities are probably best kept separate (but ongoing in parallel) because of the difficulties involved in executing each.

PRINCIPAL RECOMMENDATION: OPERATIONAL FORCES

The Chairman, Joint Chiefs of Staff, combatant commanders, and service chiefs provide greater buy-in and participation by operations community in countering cyberspace threats.

- Need two-way interaction between operations ("J3") and network ("J6") communities.
- Combatant commands and services commit to more rigorously addressing cyberspace threats in exercises. Play consequences of red team attacks through fully. Understand operational effectiveness in the face of threats.
- Combatant commands and services should be formally required to address deficiencies identified in exercises. Report to the Secretary of Defense; Chairman, Joint Chiefs of Staff; and service chiefs on progress.
- Combatant commands and services develop robust series of experiments to develop operational concepts for dealing with cyber threats.

Organizational Relationships

Many effective inter-organizational relationships are required to meet cyber attacks. Examples include the relationships between operational and technical communities, between cyber defense and cyber offense components, and between

military and intelligence communities. The findings in this area, based on extensive briefings and discussions, are:

- Technical organizations are diligent in tracking the health of networks, but they tend to neglect performance measures immediately relevant to end-users (*e.g.*, to see if e-mail and chat are working properly).
- Cooperation among operational computer network defense, attack, and exploitation elements (in particular Joint Task Force-Global Network Operations [JTF-GNO] and NSA components) has developed substantially over the last few years.
- There is an argument that the Cyber JIATF, which coordinates cyber-efforts across relevant government departments and agencies, needs more formal authorities. It is now a "coalition of the willing," albeit a seemingly responsive and effective one.
- There are separations of cyber defense and offense responsibilities in the Office of the Secretary of Defense (ASD [NII] and USD [I]) and the Joint Staff (J6 and J3) that impede decision making and defense-offense coordination.
- U.S. Strategic Command's Joint Functional Component Command for Network Warfare (JFCC-NW) (the attack component) has no forces assigned, which could impede the timeliness of its response. This is primarily an issue for service components, since NSA assets are readily transferable.
- "Traditional" intelligence support for cyberspace defense is lacking; a discipline and community to analyze and assess the cyber threat has not yet been developed. This involves much more than computer network exploitation.

The assessment in this area is mixed. On the one hand, cooperation promoting coordination of defense and offense has strengthened significantly. At the same time, the lack of "traditional" intelligence support for cyberspace defense remains a significant deficiency, given the importance of timely, accurate, and actionable intelligence to planning and operations.

Dealing with cyberspace threats requires dedicated and specialized intelligence support, as does any major threat. The most extensive example of such support is how the intelligence community organized to understand the Soviet threat during the Cold War. No organized process or established community has yet been

formed to help understand the cyber threat, especially as it exists in states that are peers or near-peers in cyberspace. Overall, a dedicated and comprehensive effort is needed to provide the proper intelligence support for understanding and countering the cyberspace threat. The following recommendation outlines steps to achieve such a capability.

PRINCIPAL RECOMMENDATION: INTELLIGENCE SUPPORT

USD (I), with support of DIA, establish a process for enhancing "traditional" intelligence about the cyberspace threat.

- Develop statement of intelligence requirements from the operations and network communities.
- Review current collection priorities and assess if they need to be adjusted.
- Develop an analytical cadre at DIA and CIA, open to new thinking, to assess the threat.
- Keep intelligence analysts closely coupled with the end-users.

Cyber Command and Control

The fundamental differences between cyber warfare and kinetic warfare require that new command and control concepts (and associated procedures and technical capabilities) be developed for cyber warfare. At the very least, "traditional" command and control concepts must be assessed and modified for application to cyber warfare. Some initial work has been done in this area. This work includes crafting the Chairman's *National Military Strategy for Cyberspace Operations* and drafting an operational concept for cyberspace operations. Additionally, there have been related activities within the services, such as the Air Force's Cybervision war games. Nevertheless, much more work needs to be done. For example:

- Fundamental concepts for cyber command and control are not articulated.
- Among the questions to be addressed: How is a commander's intent expressed? What is "maneuver" in cyberspace? How are offense and defense integrated?
- Additionally, delegation of authority issues for timely response by theater commanders has not (in general) been addressed.

- "Cyber situational awareness" is lacking. The status of network connectivity is routinely displayed, but operational implications are not addressed.
- Cyber command and control requires very timely action (sometimes within 100s of milliseconds), which currently is not possible, in general.

Closely associated with command and control is the need for situational awareness. As noted above, lack of cyber situational awareness is a significant shortcoming. While displays exist showing the status of networks, there are as yet neither means nor procedures to show the operational state of red and blue assets in the "cyber battle space."

Finally, effective operations in cyberspace require very rapid action and reaction since attacks can propagate across global networks in hundreds of milliseconds. Anticipation and timely reaction require the development of rules of engagement and delegation of authority. Additionally, necessary technical capabilities must also be developed (*e.g.*, rule-based machine-to-machine interactions to avoid slow human-in-the-loop decision cycles, and increased automation for critical activities like reviewing audit logs). These actions have been taken to an extent, but much further development is needed.

Thus, fundamental concepts for command and control of cyberspace operations are at the rudimentary stage; operational situational awareness is limited at best. The recommendations described above in the section on preparation of operational forces offer a solution to remedy these deficiencies as well.

Workforce Development

An adequate workforce, with specialized and unique technical and operational skills, is a critical component of overall capability to operate in cyberspace. With regard to the workforce, the study found that:

- Responses from the services and agencies indicate the size of the workforce is significantly smaller than what is needed for effective cyberspace operations.
- The DOT&E IA&I assessments indicate deficiencies in the training of the network operators ("yellow" in Figure 6-5, discussed in the previous section on operational preparedness).

- Three levels of capabilities are needed
  - network and systems administrators
  - personnel with advanced technical capabilities to lead network defense activities
  - individuals with "exquisite" technical skills for cyber attack and exploitation
- Skilled workforce members are lost to non-related assignments due to the absence of career paths, and to better paying career opportunities outside government.
- Necessary training programs generally exist, but are not fully available to the workforce at large.

In short, the workforce needed to operate in cyberspace is a critical component of the overall cyber warfare capability. Workforce development is an area warranting much further attention, especially given that major adversaries almost certainly have a significant workforce advantage over the United States.

As mentioned previously, the DOT&E assessments indicate deficiencies in the training of network operators. But other skill sets are also needed. In particular, more highly skilled individuals are needed to lead network defense activities and to conduct computer network attack and exploitation. Creating this workforce will be a difficult challenge, given all the other personnel demands on the services and agencies as well as the opportunities for these individuals outside DOD. But the critical need for this workforce requires that DOD make its development a high priority. Military personnel with the requisite technical skills are already serving in the National Guard and Reserves. The challenge and opportunity is to include these reserve components in cyber missions to leverage their civilian exposure to leading edge technical developments.

PRINCIPAL RECOMMENDATION: WORKFORCE DEVELOPMENT

The Under Secretary of Defense for Personnel and Readiness, in conjunction with ASD (NII)/DOD CIO and the Service chiefs, implement efforts to establish an adequate workforce for cyberspace defense.

- Estimate number and type of personnel required and compare to current staffing at three levels: network and systems administration, advanced

technical skills for network defense, and "exquisite" skills for attack and exploitation.

- Identify sources for personnel in greater numbers and with expanded technical expertise—possibly drawing from sources such as the guard and reserve components.
- Establish and refine career fields within the services for developing and retaining the necessary personnel.
- Review training and identify where enhanced training and leader development are required.

Acquisition Plans and Programs

Two subjects fall within this general assessment area: overall programmatic development, and the test and evaluation of acquisition programs (as distinct from the test and evaluation of fielded systems, discussed above for the exercise programs). The findings in the first area are as follows:

- Defensive capabilities have been increasing but significant deficiencies remain.
- Capabilities are still required to defend against mid-level threats; fortunately, those needs are largely understood.
- Capabilities against advanced threats are also required, but these are not well understood.
- The Deputy Secretary of Defense has initiated the GIG mission-assurance effort to develop a major assessment and plan to ensure the execution of essential functions in the face of cyber attack. This effort is engaged in policy development now with programmatic recommendations to be addressed later.
- NSA's GIG Information Assurance Portfolio lays out a broad plan for improving cyber defenses, but it does not address the use of attack and exploitation to aid defense.

Accordingly, DOD has been making a major effort to enhance its cyber defense capabilities through, for example, the concerted efforts of the ASD(NII)/DOD CIO working in concert with the Services and combat support agencies. However, this matter is still very challenging. There is at present no

plan that provides a comprehensive capability for cyber operations (including associated attack and exploitation capabilities in support of defense), identifies associated investments, and ties operational benefits to those investments.

The second area—test and evaluation of acquisition programs— refers to cyber defense systems *per se*, and to any system (*e.g.*, weapons systems, sensors) that connects to the GIG. The study finds that:

- Information assurance requirements in capability acquisition programs are inadequate and do not realistically reflect current and future operating environments.
- Information assurance developmental test and evaluation (DT&E) is not being extensively pursued in existing programs.
- Information assurance considerations in DT&E are largely confined to contractor activities, particularly given the de-emphasis of DT&E in OUSD (AT&L).
- New incremental information technology development methods offer the opportunity (and need) for enhanced information assurance test and evaluation.
- OT&E information assurance policy for all acquisition programs has recently been strengthened, but efforts by programs to initiate compliance activities have been limited thus far.

With regard to the information assurance OT&E of acquisition programs, new and strengthened guidance was issued by the DOT&E in the fall of 2006. However, as of June 2007, the preparation by acquisition programs for such OT&E has been limited—only 6 of 25 Tier 1 programs under DOT&E oversight for information assurance assessment were deemed by DOT&E to have adequate OT&E interaction. The fact is that fielded systems have shown significant information assurance shortcomings. At the same time, no acquisition program to date has failed information assurance OT&E, which could indicate that information assurance OT&E was not sufficiently stressing or that it did not fully reflect the operational environment into which the program was fielded. These environments can vary significantly over the lifetime of the systems involved.

In summary, significant acquisition planning efforts are underway. But an operationally driven plan, with an expeditious sense of implementation, is lacking. Further, test and evaluation of acquisition programs does not reflect the changing life cycle environment.

OT&E, conducted just prior to system fielding, is receiving significant attention. But test and evaluation is required throughout the life cycle of systems, from development through their use in the field. This need is particularly heightened with the incremental development of systems and services, and the rapid evolution of the threat.

One important requirement is for a network test bed, such as might be obtained by the broad application of the Federated Development and Certification Environment (FDCE) concept being developed by the Defense Information Systems Agency (DISA). By federating disparate development and test infrastructure; employing net-centric principles; and instituting standardized testing, evaluating, and certifying processes with the right governance, DOD can speed transition, capturing both risk and opportunity costs and achieving higher levels of mission assurance.

The intent is that the GIG FDCE will provide for a persistent, operationally realistic environment in which materiel provider, test and evaluation, service provider/consumer, and user communities can execute their responsibilities to develop, evaluate, and certify new capabilities prior to their being fully deployed onto the GIG. Existing and new development and test infrastructure, along with existing GIG transport services, will be connected to provide the foundation for rapid development and delivery of new capabilities. Under policy established by the DOD CIO, procedures will be implemented to rapidly enable the employment of these assets in support of GIG capability development and testing by any materiel provider. DISA will establish a GIG FDCE operations and maintenance entity in support of materiel provider, test and evaluation, service provider/consumer, and user activities and responsibilities.

PRINCIPAL RECOMMENDATION: ACQUISITION

USD (AT&L), working with the DOT&E and ASD (NII)/DOD CIO, establish an information assurance test and evaluation process that spans the life cycle of systems.

- Needed because of rapid evolution of threat and continual software and hardware upgrades.
- For all systems (information technology, weapon, and sensor), establish guidelines for the extent of information assurance testing required in DT&E; include red teams.

- Characterize target run-time environments for candidate capability areas (*e.g.,* command and control and intelligence) for capability acquisitions.
- Mature the DISA FDCE process and apply to all information technology systems development. Ensure representative operator involvement in FDCE execution.
- Feed the lessons learned from combatant command information assurance assessments involving federal systems back into acquisition programs.

DOD devotes much effort to planning for cyberspace defense investments, but the work can often be slow in coming to fruition and not directly associated with operational benefits. The following recommendation details steps to redress those deficiencies. Key is the exercise of leadership in the face of complex DOD processes.

ADDITIONAL RECOMMENDATION

ASD (NII)/DOD CIO ensure that investment and compliance activities for addressing cyberspace threats are conducted in an expeditious and operationally focused manner.

- Lead effort to identify the operational benefits associated with proposed investments.
- In the face of continuous process and study, provide leadership to identify particular investments with high operational benefit to make now. Design and test for resilience (continuity of operations is a subset).
- Continue promoting information assurance compliance measures, but do so in context of their operational benefits, not simply "compliance for compliance's sake."

Policy and Legislation

Policy and legislation strongly influence the actions that can be carried out in cyber defense as well as in attack and exploitation in support of defense. The key issue is that adversaries can attack and exploit the United States from any location within the global reach of cyberspace, but U.S. authorities to counter such attacks change organizational jurisdiction based on the origin of the incursion.

- Most legislation and some policy applying to cyberspace operations predate the modern era of globally distributed networks and information access.
- Cyberspace is borderless, but organizational jurisdiction changes across U.S. borders (*e.g.*, between DOD and FBI). This slows the ability to respond to and track attacks, and gather intelligence. Adversaries take advantage of these limitations.
- A comprehensive assessment of policy and legislation is needed. The politically sensitive nature of factors involved requires a public dialogue to gain necessary understanding and support; this especially applies to issues of access versus privacy.

Policy matters involved include delegation of authority and resolution of interagency coordination issues. Examples of relevant legislation are the Foreign Intelligence Surveillance Act of 1978, the Computer Security Act of 1987, and the Federal Information Management Security Act of 2002. The issue is both whether adequate authorities exist and how existing authorities can be streamlined and de-conflicted across departments and agencies. An important issue to consider is whether authorities and procedures could be less restrictive in time of crisis or war than their peacetime counterparts. The sensitivity of the issues involved requires that the review of policy and legislation, and any subsequent efforts to alter them, should be carried out in a manner to gain public support and endure through the transition of Presidential administrations. Some activity to address these matters is ongoing (specifics classified).

The inside-outside U.S. distinction of organization authorities is at odds with the borderless nature of cyberspace.

Policy and legislation define the actions allowed in cyber defense and offense. An assessment of policy and legislation is needed to ensure that the proper actions are allowed, consistent with the overall principles of the U.S. government and society. These actions occur both across interagency lines and within the military chain of command.

The administration has activities ongoing to address the interagency dimension, but actions within the military operational chain must also be considered. The military must have the flexibility necessary to enable timely response to cyber attacks, to include from the perspective of the field commander, who may not have the time to go "up the chain" for approval to act.

RECOMMENDATION: POLICY AND LEGISLATION

USD (P), with ASD (NII)/DOD CIO and the Commander of U.S. Strategic Command, identify changes in policy and legislation needed to enhance effectiveness of countering cyberspace threats.

- Work with interagency partners to develop processes needed for coordinated cyber operations between DOD, intelligence, law enforcement, and homeland security communities. Political sensitivities involved (such as privacy issues) require that the U.S. government have a "strategic communication" plan before rolling out this issue publicly.
- Implement military operational processes to enable nearly instantaneous defensive and offensive responses to cyber attacks. Meet needs of field commanders as well as strategic needs. Establish delegation of authority and rules of engagement for both peacetime and wartime situations.

Homeland Cyber Defense

Cyber attacks against the U.S. homeland could affect U.S. military forces in two ways. Either directly by destruction or degradation of assets required by the forces (*e.g.,* logistics and transportation capabilities), or indirectly through "pain" on the civil society influencing the population and the political leadership.

- DHS has the lead for securing the United States against cyber attacks, but in event of a major attack the President could turn to DOD, and the department must be prepared.
- DOD-developed technical capabilities have applicability to wider government and civil cyber defense.
- Interagency coordination is essential for effective defense (*e.g.,* coupling of legal, intelligence, and defense).
- Cyber attacks on the homeland (as well as WMD attacks) could require a "national command and control" capability to effect necessary interagency response. The DHS-led National Command and Coordination Capability (NCCC) effort, as currently construed, is not likely to provide the necessary capability.

DOD's responsibility (in particular, U.S. Strategic Command) to be prepared for cyber attacks on the civilian infrastructure may be made explicit in the *Unified*

Command Plan for 2007, now under preparation. In addition, some activity (specifics classified) to address the matters raised above is ongoing.

A related issue, noted under the last bullet above, is the need to establish a "command and control" capability at the national level to deal with any major catastrophic event affecting the United States. An effort in that direction is the NCCC, being led by DHS. However, that effort is now concerned primarily with matters of communications connectivity. A far broader approach focused on senior-level decision-making and means to reassure the nation would be required to deal with truly catastrophic events.

Cyber attacks against the U.S. government or the U.S. economy and populace in general represent a critical threat that a peer or near-peer could employ against the United States for coercive or deterrent purposes.

DOD must contribute to planning for such contingencies and be prepared to accept an operational role if such occurs. In fact, *Unified Command Plan* 2007 is expected to assign Strategic Command the responsibility to be so prepared, which would allow DOD to aggressively pursue the recommendation outlined below.

PRINCIPAL RECOMMENDATION: HOMELAND CYBERDEFENSE

The Secretary of Defense, with the Secretary of Homeland Security, determine how DOD can best contribute to national cyber defense planning and be prepared to assume greater responsibilities during major cyber attacks affecting U.S. government and civilian infrastructure.

- Establish a well-defined set of procedures for integration of DOD and DHS cyber defense activities.
- Participate in interagency coordination required for effective defense.
- Participate in developing a national command and controls and situational awareness capability, considering how such might grow from existing and planned DOD capabilities.
- Apply, as feasible, DOD developed technologies for broader national cyber defense.
- Determine the role DOD can play in strengthening cyber defense capabilities in and through industry (such as establishing policies for technical cooperation).

Deterrence

Deterrence is critical to the overall cyber warfare posture, just as it is to "traditional" warfighting. The findings in this area are:

- A brief review of the literature and related discussions reveals no substantive deterrence concepts based on currently realistic capabilities.
- A strong defense and effective counter-attack capability contribute to deterrence. This is not the case today, but possible in the future.
- Deterrence in cyberspace may hold at risk assets outside cyberspace.
- Deterrence considerations must address the meaning and consequence of escalation in cyberspace attack and counter-attack.
- Attribution is critical to any concept of deterrence. This is very difficult to accomplish today; it is an open question as to how much improvement can be made.

Thus, while there are fragments of ideas relating to deterrence, no substantive concepts based on currently realistic capabilities have been developed. All that can really be said at this time as a conclusion is that efforts to develop such concepts and capabilities should continue.

The subject of attribution (identification of the attacking party) is worth some further discussion, however. Attribution is obviously critical in order to retaliate against an attacker, but it is very difficult to obtain because the perpetrator of an attack can mask his or her identity by operating through an intermediate site located far from the attacker's actual location. Currently, attribution can require detailed forensic analysis and take from days to months (or longer). There are, however, some technical developments (specifics classified) that could make attribution simpler in the future.

Chapter 22. Crosscutting Observations

Four observations apply across the three asymmetric environments examined in the preceding chapters:

1. U.S. forces are ill-prepared to operate in or "fight through" the environments such attacks would create because:
   - They are insufficiently trained and equipped to do so.
   - They have highly vulnerable systems that can be improved.
   - They do not exercise rigorously to measure readiness or progress.
2. Determining precisely who initiated a WMD, space, or cyber attack can be difficult or impossible without the right sensors and continuous situational awareness.
3. U.S. forces generally do not have standing tactics, techniques, procedures, or equipment to rapidly reconstitute key elements of space or networking capabilities if they are rendered inoperable by an attack.
4. The nation has chosen not to develop and publicly deploy offensive capabilities in the space and cyber realms.

The study concludes that in every case, military forces must be able to operate effectively for extended periods of time and to WIN in degraded environments. This is a tall order but critically important. Potential asymmetric capabilities could have catastrophic consequences in future combat operations unless action is taken now to offset these vulnerabilities. The assessment offered here should sharpen the understanding within DOD about the need for investments in countering WMD, and for preparing to conduct operations in space and cyberspace.

War against adversaries who use asymmetric capabilities against the United States will be a new experience for the armed forces. An intellectual foundation is needed as a basis for developing concepts of operations. Such a foundation should serve as the basis for training and leadership development programs in operational warfighting that are not presently available. Experimentation, exercises, and assessments are necessary to gain experience and refine operational concepts. Although not discussed in much detail in this report because of security concerns, offense in each of these areas is equally if not more important than defense and certainly both are required.

Part VII

Strategic Communication: Another Instrument of U.S. Power

Chapter 23. The Importance of Strategic Communication

The cost of employing military force to advance national interests is on the rise—not only financial cost but also loss of life and global standing. And these costs will be on the rise even if all recommendations proposed in the preceding chapters are fully implemented. Technology will continue to proliferate, our homeland will continue to be insecure. Thus, our national security strategy should seek to apply both "hard" and "soft" instruments of power to achieve the nation's objectives—employing coordinated defense, diplomacy, and development. Greater attention needs to be paid to instruments of national power other than military force. Diplomacy (e.g., treaties, negotiation) and development (e.g., foreign aid, fiscal and monetary policy, trade policy) are additional instruments. Strategic communication can amplify or diminish the effect of defense, diplomacy, and development. Accordingly, strategic communication was chosen as a unique focus of this study.

Strategic communication is an integrated process that includes the development, implementation, assessment, and evolution of public actions and messages in support of policies, interests, and long-term goals. This challenging, senior-level management responsibility spans complex organizational capabilities, broad geographies, diverse audiences, collaborative partnerships, and timeframes. In successful strategic communication, "actions" are often the most authentic "messages."

Strategic communication differs from public relations and public affairs. It includes but goes beyond media affairs and short-term news streams to focus on mid-range and long-term objectives that require multi-disciplinary capabilities, engagement in a dialogue of ideas, and durable partnerships with civil society organizations. As such, strategic communication is more "long-term strategic." Public affairs is more "short-term tactical." Coordination between them is vital and facilitated in the Department of Defense (DOD) through development of an Integrated Strategic Communication Plan.

In recent years, private sector and civil sector organizations around the globe have embraced the capabilities associated with integrated strategic communication. Many have reorganized and resourced their organizations to

enhance the capacity of strategic communication to support mission accomplishment as well as to mitigate potential competitive threats.

The release of the first U.S. *National Strategy for Public Diplomacy and Strategic Communication* has recently elevated the role of strategic communication in achieving long-term U.S. national security goals However, the U.S. government has yet to identify the comprehensive leadership structure, interagency coordination process, and resource levels through which sustained long-range planning and implementation of "whole of government" integrated strategic communication can be achieved.

This study sought to assess U.S. government capability gaps in strategic communication in the face of innovative technologies, systems, operational concepts, and management processes that have developed since the 2004 report of the *Defense Science Board Task Force on Strategic Communication.* The chapters that follow summarize key findings and recommend opportunities to strengthen the strategic communication management process to enhance its ability to serve U.S. national interests in an increasingly complex and multi-dimensional policy environment.

Effective Strategic Communication is Vital to Achieve U.S. Strategic Objectives

The *U.S. National Security Strategy*[85] and the *U.S. National Strategy for Public Diplomacy and Strategic Communication*[86] list the following strategic objectives:

- champion aspirations for human dignity
- strengthen alliances to defeat global terrorism and work to prevent attacks against us and our friends
- work with others to defuse regional conflicts
- prevent our enemies from threatening us, our allies, and our friends with weapons of mass destruction (WMD)
- ignite a new era of global economic growth through free markets and free trade

85. See www.whitehouse.gov/nss/2006/
86. See U.S. National Strategy for Public Diplomacy and Strategic Communication, http://www.state.gov/documents/organization/87427.pdf

- expand the circle of development by opening societies and building the infrastructure of democracy
- develop agendas for cooperative action with other main centers of global power
- transform America's national security institutions to meet the challenges and opportunities of the 21st century
- engage the opportunities and confront the challenges of globalization

Strategic communication is critical to achieving all U.S. strategic objectives. It is an increasingly powerful instrument, essential to the success of persuasive, cooperative, and coercive instruments of national power. It involves significant and sustained investments across all departments and agencies; and it requires coordinated policies, programs, messages, and actions.

Positive Changes Implemented: Department of State

Since the publication of the *2004 Defense Science Board Report on Strategic Communication*, progress has been made in improving the nation's strategic communication capability.[87] Perhaps the most important advance has been in establishing strategic communication as a priority at the highest levels of the U.S. government. In April 2006 a Policy Coordinating Committee (PCC) chaired by Under Secretary of State for Public Diplomacy and Public Affairs Karen P. Hughes, was established.[88] In June 2007, the PCC released a U.S. National Strategy for Public Diplomacy and Strategic Communication.[89] This document presents a clear and well-articulated strategy intended to serve as a framework for strategic communication implementation plans across the interagency. Agencies are in the process of preparing and submitting to the PCC their specific strategic communications plans.

In order to achieve greater agility in communicating U.S. policy, the Department of State has established three public diplomacy "hubs" in Dubai, London and Brussels.[90] These operations are in response to the increasingly regional nature of today's media, which transcend national borders and require that

87. See http://www.acq.osd.mil/dsb/reports/2004-09-Strategic_Communication.pdf
88. A discussion of roles and responsibilities of the PCC is included in U.S. *National Strategy on Public Diplomacy and Strategic Communication,* June 2007.
89. See http://www.state.gov/documents/organization/87427.pdf
90. See http://www.state.gov/documents/organization/84970.pdf

U.S. government spokespersons get into regional news cycles, not those in Washington D.C. In Dubai, for example, more than one thousand media operations are represented.[91] The public diplomacy hubs have increased the U.S. presence in pan-Arab media by more than thirty percent since they were established in 2006.[92] In addition, Under Secretary Hughes has issued a set of "rules" to empower the nation's diplomats to seize media opportunities in making the case for U.S. policies without the slow headquarters clearance process that previously characterized media operations in the Department of State.[93]

When the 2004 DSB report was written, the U.S. government had no effective, agile way to respond to what international media were communicating to mass audiences (in Arabic, Farsi, or other regional languages) about America, its policies, and its military operations. The State Department's new Rapid Response Unit—consisting of a state-of-the-art broadcast center—now constantly monitors international media, with the help of the Intelligence Community's Open Source Center, and produces a daily report that informs policy makers of what is driving world news from Europe, the Middle East, and Latin America. The Rapid Response Unit provides the U.S. position on many of those issues in an email to several thousand senior officials, from cabinet secretaries to combatant commanders. Some combatant commands have similar rapid response units.

With significant assistance from the DODand the Open Source Center, the Department of State has set up an interagency Counter Terrorism Communication Center to develop culturally sensitive messages to undermine ideological support for terror.

The Department of State also has begun a Digital Outreach initiative, in which American Arabic language bloggers counteract the misinformation and disinformation rampant in the Arab blogosphere about the United States, its policies, and actions.[94] These individuals, who clearly identify themselves as employees of the Department of State, face off daily against an army of anonymous bloggers unbound by any standard of "truth," providing verifiable, factual information to anyone reading Arab language blogs.

---

91. See http://www.state.gov/r/us/2007/88630.htm
92. See http://www.state.gov/r/us/2007/88630.htm
93. See http://www.state.gov/r/us/64106.htm
94. "At State Department Blog Team Joins Muslim Debate," http://www.nytimes.com/2007/09/22/Washington/22bloggers.html

The national strategy recognizes that perhaps the most effective tool of strategic communication over the last fifty years has been educational exchange programs in critical areas. Since the 2004 DSB report, there has been a substantial increase in the number of exchange participants, from approximately 27,000 to almost 39,000 in 2006. Following a decline in the number of student visas issued in the aftermath of September 11, 2001, which reached a low of 473,719 in 2003, the downward trend has been reversed. More than 591,000 student visas were issued in 2006 and the Department of State has partnered with America's higher education community to send a clear message that the United States wants the future leaders of the world to come to the United States to study and get to know its culture, social values, and political system.

Similar gains have been made in other programs. The flagship Fulbright Exchange program has seen substantial increases both in the number of American students and researchers studying abroad and in the numbers of foreign scholars and researchers coming to the United States to teach and conduct research.

English as a Second Language (ESL) instruction programs and infrastructure are expanding, and currently the State Department is funding ESL programs reaching more than 10,000 young people—often from marginalized populations—in more than 40 Muslim-majority countries. ESL instruction provides young people with an employable skill and opens the door to dialogue with America and its values.

Promising steps have been taken to institute a culture of measurement in the field of public diplomacy. Under Secretary Hughes established a unified Public Diplomacy Evaluation Office to undertake a range of evaluation and performance-measurement initiatives. This office has developed an evaluation strategy encompassing the Bureau of Educational and Cultural Affairs, the Bureau of International Information Programs, and overseas missions; a core set of public diplomacy performance indicators; a global public diplomacy tracking system; and the first pilot study to attempt to quantify the aggregate impact of public diplomacy programs and products.

Positive Changes Implemented: Department of Defense

The study reviewed the DOD activities involving strategic communication since the DSB 2004 report and is encouraged that several recommendations from

that report are being pursued. Significant capability shortfalls in several combatant commands remain, however, and should be resourced without further delay.

Notably, the *2005 Quadrennial Review* process included for the first time a Strategic Communication Working Group. That group produced a Strategic Communication Roadmap signed by the Deputy Secretary of Defense on September 25, 2006.

As members of the Strategic Communication Integration Group (SCIG), the Principal Deputy Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Public Affairs, the Director of the Joint Staff, and representatives from the Under Secretary of Defense for Intelligence and the Assistant Secretary of Defense for Legislative Affairs formed an executive committee that meets on a weekly basis, with bi-weekly meetings with the deputy secretary.

A high-level mechanism for re-allocating resources within DOD, the deputy secretary's Advisory Working Group now includes SCIG-recommended resource requirements in its issues for decision.

A new Deputy Assistant Secretary for Joint Communications was established in the public affairs office in the Office of the Secretary of Defense to support SCIG activities, oversee initial compliance with the Strategic Communication Roadmap tasks, and better define the role of public affairs personnel in supporting combatant commanders and joint task force commanders overseas.

The Under Secretary of Defense for Policy established a separate office, Support to Public Diplomacy, in January 2007, with a deputy assistant secretary reporting directly to the principal deputy—paralleling a specific recommendation by the DSB in 2004. That office is now coordinating across functional and regional offices in the Office of the Secretary of Defense and the Joint Staff to institutionalize the development of strategic communication plans to counter ideological support to terrorism.

At the combatant commands, U.S. Central Command plans and operates in the information environment through a Strategic Effects cell in Baghdad and an analogous function with NATO forces in Kabul. An Arab media engagement cell was established in Dubai in 2005[95], and Central Command representatives are working with Open Source Center and Defense Intelligence Agency

95. This cell was disestablished in the wake of the new State Department hub in Dubai.

representatives to fashion a regionally focused media analysis and response center in Qatar.

DOD Regional Centers for Security Studies, and the war colleges, provide counter ideological support for terrorism strategies to future foreign civilian and military leaders involved in security functions in their countries.

The Under Secretary of Defense for Intelligence, in cooperation with the Under Secretary of Defense for Policy and the Open Source Center, provides unclassified daily reports on Arab media and terrorist use of the Internet relevant to the geographic combatant commanders, as well as situational awareness briefings concerning terrorist propaganda to US forces deploying to Iraq.

U.S. European Command has re-organized its information activities around a concept called Operation Assured Voice, which has a combined information operation and public affairs cell reporting to the Chief of Staff. Websites aimed at the Balkans and North Africa carry content in the appropriate languages to support the commander's mission to shape the environment in his area of responsibility. The European Command approach is a model for other combatant commands to consider.

U.S. Southern Command has established a separate office for strategic communication for "launching ideas, not Tomahawks."

U.S. Strategic Command, designated to support the geographic combatant commands with respect to information operations, currently provides a daily report and weekly summaries to regional commanders highlighting foreign print media in their regions. Strategic Command's Joint Information Operations Warfare Command is partnering with U.S. Special Operations Command to examine better ways to use psychological operations messaging and products to influence key target audiences in the war on terror.

Special Operations Command, as both a supported and supporting command, has developed a trans-regional website initiative and has expanded its trans-regional psychological operations (PSYOP) program under the auspices of its Joint PSYOP Support Element. More than a dozen Special Operation Command Military Information Support Teams are deployed worldwide in support of Embassy Country Teams.

As a government legacy support, the Open Source Center (formally the Foreign Broadcast Information Service) has expanded monitoring and reporting of foreign broadcasting and the internet, and carries foreign media products generated by DOD components on its global website. The Open Source Center has recently created a new Emerging Media Center designed to draw outside experts to support its work in this area.

While many positive steps have been taken within the Departments of State and Defense, many of these actions have been organizational and tactically reactive. Fundamental transformation in the goals, methods, and structures of strategic communication is vital to the national interest. Collaboration between government and civil society on an unprecedented scale is imperative. Significant reforms are essential in the way strategic communication is directed and funded. Strategic communication can no longer be hostage to three-year cycles of short-term commitment followed by short-term inattention. Changes must be substantial and durable. These kinds of changes can only occur when led by a President with bipartisan Congressional support.

Chapter 24. What is Strategic Communication and Why Does it Matter?

Strategic communication is vital to U.S. national security. It is an increasingly powerful, multi-dimensional instrument that is critical to America's interests and to achieving the nation's strategic goals.

Although attention to strategic communication is widespread, its power and potential are generally misunderstood. Too often it is an afterthought in determining strategic priorities. For many it is simply a matter of crafting and disseminating messages. Today's threats and opportunities call for a radically different approach. Asymmetric threats abroad and vulnerabilities at home are decreasing the effectiveness of military force and increasing the need to invest in other instruments of power.[96] At the same time, significant new opportunities exist to leverage national capacity within government and to mobilize talent, expertise, and creativity outside government. The nation needs to build capacity in both with much greater emphasis on institutions that connect government and civil society.[97]

The United States can no longer depend on an instrument that is low priority, reactive, and episodic—something "discovered" after an attack and addressed only in occasional bursts of national commitment. National needs require a proactive and durable means to engage and influence the attitudes and behavior of global publics on a broad range of consequential issues.

Strategic communication is essential to the successful use of all persuasive, cooperative, and coercive instruments of national power. It can amplify or diminish their effects. It is necessary long before, during, and after armed conflict. It can help prevent or limit conflict. It is central to the formulation and implementation of strategies, and it must be treated accordingly.

---

96. For an expanded analysis of this point, see the forthcoming report of the *DSB 2007 Summer Study on Challenges to Military Operations in Support of National Interests.* See also John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization,* (Hoboken, NJ: John Wiley & Sons, Inc. 2007).
97. By "civil society" we mean the totality of voluntary civic, social, and commercial organizations and institutions that form the basis of a functioning society as opposed to the structures of a state.

Strategic Communication is an Interactive Process

Strategic communication is a sustained and coherent set of activities that include:[98]

- **understanding** identities, attitudes, behaviors, and cultures; media trends and information flows; social and influence networks; political, social, economic, and religious motivations.
- **advising** policymakers, diplomats, and military commanders on the public opinion and communication implications of their strategic and policy choices—and on the best ways to communicate their strategies and policies.
- **engaging** in a dialogue of ideas between people and institutions that support national interests and, wherever possible, common interests and shared values.
- **influencing** attitudes and behavior through communication strategies supported by a broad range of government and civil society activities.
- **measuring** the impact of activities comprehensively and over time.

These activities are elements in a continuous, dynamic, and iterative process that begins with choices among strategic priorities and deep comprehension of attitudes and cultures. This means more than just an appreciation of the opinions and motivations of others. It means seeing ourselves as others see us, rather than through the "looking glass" of our own perceptions. It means full use of the rich variety of interpretive tools available for penetrating analysis of cultures and influence networks. Planning, advising leaders, building relationships, advocacy campaigns, assessment of impact, and adaptation to changing circumstances follow, as illustrated in Figure 7-1.

Strategic communication takes place in three timeframes:

1. short-term news streams
2. medium-range campaigns on high-value policies
3. long-term engagement

---

98. See also Defense Science Board Task Force on Strategic Communication, *Strategic Communication*, September 2004, pp. 11-13. http://www.acq.osd.mil/dsb/reports/2004-09-Strategic_Communication.pdf

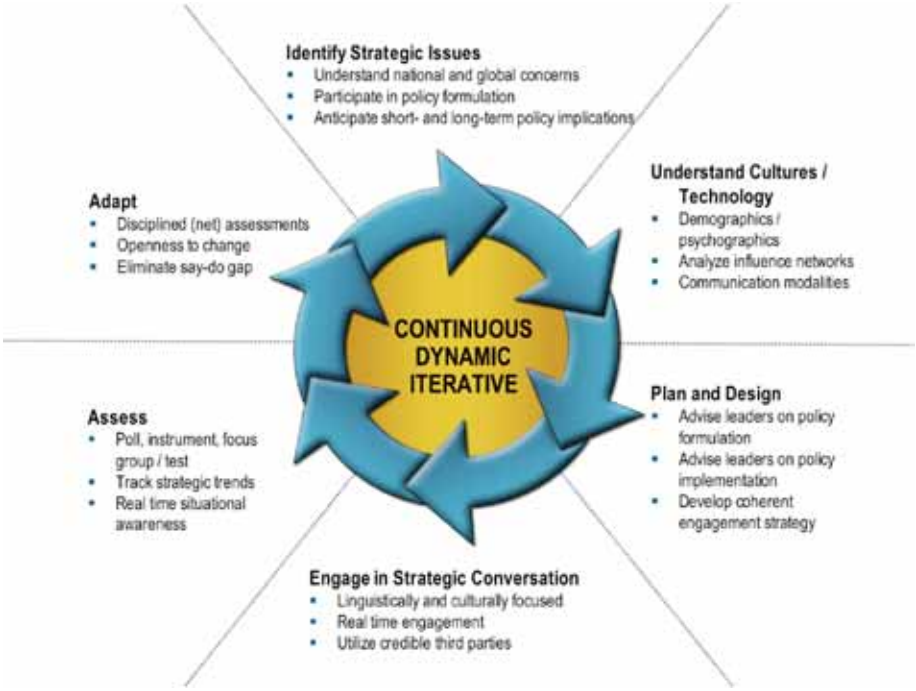


Figure 7-1. Strategic Communication Process

Strategic communication is conducted not just by the Departments of State and Defense, but by at least 64 U.S. government agencies, 50 states, many U.S. cities, coalition partners, and a wide variety of civil society organizations. Public diplomacy, military civil affairs, military international education and training programs, cultural diplomacy, public affairs, international broadcasting, and support for democracy are among the means by which it is carried out.

Strategic communication differs from education, journalism, advertising, branding, and public relations. To succeed, however, it depends on strong relationships with civil society and uses many of civil society's methods, skills, and norms.[99] Strategic communication is an instrument of statecraft that depends

99. On differences between strategic communication by governments and civil society, and the value of importing civil society's methods, see Todd C. Helmus, Christopher Paul, and Russell W. Glenn, *Enlisting Madison Avenue: The Marketing Approach to Earning Popular Support in Theaters of Operation* (Washington, DC: 2007) http://www.rand.org/pubs/monographs/2007/RAND_MG607.pdf; U.S. General Accountability Office, *Actions Needed to Improve Strategic Use and Coordination of Research,* GAO-07-904, Washington, DC, July 2007; http://www.gao.gov/new.items/d07904.pdf; and Bruce Gregory, "Public Diplomacy as Strategic Communication," Chapter 17, pp. 336-357, in James J. F. Forest (editor), *Countering Terrorism and Insurgency in the 21st Century,* volume 1, (Westport, CT: Praeger); earlier version in "Public Diplomacy and Strategic

on shared knowledge and adaptive networks—both within government and between government and society. It must be understood, directed, coordinated, funded, and conducted in ways that leverage relationships with civil society in support of the nation's interests at home and abroad.

Strategic Communication Depends on Cultural Context

While "all politics is local," all communication is now global. Gaps between what the nation says and does—and gaps between what it says and what others hear—have strategic consequences. These "say-do" and "say-hear" gaps affect U.S. interests in ways that can be measured in lives, dollars, and lost opportunities. We, as a nation, continue to underestimate them to our disadvantage.

Successful strategic communication requires an interactive relationship between senders and receivers.[100] People understand and relate to ideas and information when they identify with what is conveyed. Successful communicators enlist interest and evoke common ground.[101] They enlist interest through credible symbols (actions, images, and words) that resonate with others. They evoke common ground by focusing on culturally independent concepts that are globally valued—human dignity, health, personal safety, education, the environment, and economic well-being—and do so in ways that build support and mobilize allies. The opinions of others should not determine U.S. strategies, but taking them into account is critically important to any successful strategy.

Deep appreciation that what the nation says often is not what others hear is also critical. Words such as "democracy," "rule of law," and "freedom" have different meanings in different cultures at different stages of their development. When the United States says democracy, our message may be self-rule; but others may hear chaos. To U.S. citizens, rule of law means order; for others it may mean oppression. To some, jihad means terrorism; to others it means holy war or

---

Communication: Cultures, Firewalls, and Imported Norms," Paper presented at the American Political Science Association Conference on International Communication and Conflict, Washington, DC, August 31, 2005, http://www8.georgetown.edu/cct/apsa/papers/gregory.pdf#search=%22gregory%20firewalls%22.

100. Steven R. Corman, Angela Trethewey, and Bud Goodall, *A 21st Century Model for Communication in a Gobal War of Ideas: From Simplistic Influence to Pragmatic Complexity,* Report #0701, Consortium for Strategic Communication, Arizona State University, April 3, 2007.

101. See the section on "Historic Strategic Communication Successes" later in this chapter.

purification. Understanding the "pictures in the heads" of others is a crucial first step in strategic communication.

Actions are more important than carefully crafted messages. Additionally, it is important to avoid message vulnerabilities. Messages intended to galvanize support at home often have negative impact internationally—such as "global war on terror," "fighting them there so we don't have to fight them here." Images, body language, and media context in real and virtual worlds are messages as well—messages that often conflict with actions and words.[102]

Most people don't choose between true and false messages. In a complex globalizing world they choose between trustworthy and untrustworthy messengers. For presidents, policymakers, diplomats, and military commanders, credibility and "message authority" matter more than the message.

Strategic Communication Must Be Agile

Strategic communication is engaged in a generational and global struggle about ideas. This is not a war between the West and Islam. It is not a war against terrorism, although it is about challenging ideas that give rise to terrorism. Strategic communication is an instrument that can be used to engage and influence global publics on a broad range of strategic issues (such as nuclear proliferation, trade, energy, global pandemics, climate change, and a variety of challenges from state and non-state actors).

To succeed, strategic communicators must be agile and adaptive. Events and actions provide opportunities for interpreting positive values in fresh and effective ways. Some events and actions—by the United States, its allies, and its adversaries—can be anticipated. Engagement and influence strategies can be planned in advance. Other events and actions are surprises. Skilled communicators need a basic understanding of issues and themes. But in a world of rapid change, they also need the support of rapid response capabilities that monitor the forces and media frames driving events. They need both the mindsets and the tools that will enable them to seize opportunities and adapt. Agility is critical.

---

102. Images of Saddam Hussein talking with visibly frightened children during Operation Desert Storm in 1991 and the "Mission Accomplished" sign behind President Bush on the USS Abraham Lincoln after major combat in Iraq in 2003 make the point.

Adversaries present opportunities to offer a contrasting positive vision based on shared values where they exist, as well as to de-legitimize their actions and messages. This means emphasizing actions, relationships, images, and messages that build on shared values. It means empowering surrogates and credible third parties (exchange participants, religious leaders, foreign media, and academics) without undermining their legitimacy.

The United States also must identify its opponent's weaknesses and exploit them vigorously. The nation should emphasize actions and statements that are inconsistent with prior statements or with the core values and cultures of the communities it seeks to influence. Attention to failures, inconsistencies, and falsehoods—time after time—can create a compelling story that isolates extremists, undermines their efforts, and possibly changes opinions and actions.

The identities and beliefs of the audience are key. For example, the image of a child suicide bomber shows a violation of sacred values. To many Muslims and non-Muslims alike, the image of a mosque destroyed by Muslims may be an unexplained inconsistency and a desecration. Sometimes a single statement or image persists in the mind of the listeners or viewers. For example, John Kennedy's statement "Ich bin ein Berliner" had lasting impact. The single image of an Iraqi woman holding up her finger coated with purple ink to indicate that she had voted had immediate impact and staying power.

Rapid response is challenging because of the many media organizations that are operating 24/7 and responding to the same situations.[103] Citizen reporters who can transmit via a multiplicity of channels— websites, blogs, listserves, and virtual platforms such as YouTube—add to the challenge. All have access to rapid communication. Media frames of events travel across the world with light

103. See Chapter 26 for an expansion on this issue.

speed. They shape the perceptions of competing elites and global publics. Media frames reflect different cultural contexts and the mindsets of reporters and editors. In breaking news environments, media frames are not likely to change what people think, but they are powerful agents in telling people what to think about.


Department of Defense

Rapid responses and generational struggle are not inconsistent. Strategic communication requires sprinters and long-distance runners.

Historic Strategic Communication Successes

Americans have had many strategic communication successes. In some cases it was a single document or speech (the Declaration of Independence, the Gettysburg address) or an image (the moon landing). In other cases, success was a product of actions, complemented by images and words, in the context of strategic objectives (the Marshall Plan, Dayton Accords, HIV/AIDs initiatives). In still other cases, long-term relationships between people and institutions led to success (the Fulbright program, large-scale educational and scientific exchanges).


NASA

What were the elements of success?

- Strategic objectives were defined at the nexus of national interests and shared values.
- Sustained Presidential leadership, bipartisan support, and generous funding were linked to comprehensive strategies.
- Civilian and military departments and agencies collaborated.
- Programs and activities were culturally, politically, and/or economically relevant.
- Activities were understood, timely, focused, credible, meaningful, and accessible to the intended populations.
- Significant government and non-government resources were involved.
- Successes were often scientifically and/or technologically enabled.

Not every element was relevant to every success, but lessons were taught and can be learned (Table 7-1). Effective communication strategies in the past were grounded in actions, relationships, images, and words. They were sustained, comprehensive, relevant, and adequately resourced. Presidential leadership and bipartisan support were critical.

Table 7-1. Lessons Taught from Successful Strategic Communication Activities

Actions trump words	Relationships are critical
Partners count	Coordination is critical
Messenger authority	Trusted voices
Language matters	Images matter
Speed counts	Endurance counts

Strategic Communication Challenges

Effective strategic communication is inherently difficult. As the examples of historic communication successes illustrate, shared values and a genuine, positive correlation of interests are necessary. Ironically, the explosion of new communications media and the attendant social change it is spawning will make it more difficult to frame positive outcomes in the foreseeable future. As traditional barriers to information flow fall, the speed with which information circulates and its ubiquity will overwhelm the ability to distinguish important from trivial. More and more, image will overwhelm context.

The "say-do gap," always a challenge for powerful nations that must balance competing and often conflicting interests, will be more obvious. The ability of the U.S. government to operate in secrecy or to control messages, perceptions, and attitudes will be greatly diminished.

The growing youth bulge adds to complexity. In many developing societies the percentage of youth in the population is rising rapidly, as that percentage decreases in most developed countries. Young people have access to new information sources that will often amplify distrust of traditional sources.

The viral nature of electronic media, coupled with the growing proliferation of electronic communication devices, means that almost every action or operation that can be witnessed can also be recorded, distributed, manipulated,

and distorted. Individual actions will be amplified. In military situations, small, tactical actions will be viewed globally and take on strategic significance.

A thoughtful, sustained, and comprehensive response is essential. The United States will have to think and operate differently and must learn to think and communicate in ways that unite rather than divide. Polarizing rhetoric may have short-term benefits in motivating support at home, but abroad it can have adverse long-term consequences that reduce the willingness of potential allies to collaborate and give unwarranted legitimacy and unity of effort to dispersed adversaries.

The more difficult interpersonal communication is, the more important it becomes. The more difficult it is to engage potential adversaries in a common search for solutions, the more important it is to try. The easier it is to employ military power to respond to challenges to national interests, the more important it becomes to consider alternative responses.

Transforming Strategic Communication

The world is changing with profound consequences for how the United States considers and uses strategic communication. During the hot and cold wars of the 20th century, states were dominant actors. Relatively few non-state actors occupied the world stage. Contests about ideas were secular struggles between authoritarian and democratic worldviews. Bright lines separated war and peace. Information systems used analog technologies. Governments organized on hierarchical principles. National armies fought on battlefields with industrial age weapons.

That world no longer exists. Globalism, networks, non-state actors, ideas, advanced technologies, and new forms of warfare are transforming strategic communication and all other instruments of 21st century statecraft. The United States will struggle to engage in effective strategic communication in a world where states are becoming more limited in their legitimacy and in their capacity to satisfy human needs. Highly centralized, prescriptive, top-down communication strategies will matter far less. Resilient strategies grounded in deep comprehension of the attitudes, cultures, and goals of others will matter much more. Strong networks, rather than hierarchies, will be critical to these strategies—networks characterized by openness, trust, access, and collaborative effort by multiple public and private actors with diverse motives.

A fundamental transformation in the goals, methods, and structures of strategic communication is vital to the national interest. Collaboration between government and civil society on an unprecedented scale is imperative. Significant reforms are essential in the way strategic communication is directed and funded. Strategic communication can no longer be hostage to cycles of short-term commitment followed by inattention. Change must be substantial and durable. This kind of change can only occur when led by a President with bipartisan Congressional support.

Chapter 25. The World is Changing

The world has changed in fundamental ways that profoundly affect the significance and role of strategic communication. It has become increasingly interdependent (global economies, environment, and media), urbanized (over half the world's population live in cities[104]), and influenced by youth (44 percent of the world's population is under 25, and 27 percent is under 15[105]). Failed states have provided enabling conditions and safe havens for non-state actors to develop and engage in global terrorism. The spread of the Internet, information technology, and communications has accelerated globalization and further enabled terrorism. According to independent polling, the United States faces continuing decay in support for U.S. policy and rising anti-Americanism which challenges national interests.[106] Actions and words with global impact are increasingly important in this interdependent world as evidenced by activities such as the Peace Corps and U.S. support to the Indonesian Tsunami relief. Unfortunately, the U.S. government has a poor understanding of foreign languages and cultures which exacerbates the challenge. This chapter details global changes, identifies opportunities and threats, and articulates their implications for strategic communication.

Multiple Dimensions of Change

Accelerating Globalization

Faster, deeper, cheaper interdependencies at transcontinental distances are transforming social consciousness and concrete connections between states and between states and non-state actors.[107] While globalism is not new, the speed and density of globalism are new.

---

104. UN General Assembly, GA/EF/3160, 26 October 2006. See http://www.un.org/News/Press/docs/2006/gaef3160.doc.htm
105. U.S. Census Bureau, see http://www.census.gov/cgi-bin/ipc/idbagg
106. Pew Global Attitudes Project
107. Robert O. Keohane and Joseph S. Nye, Jr., "Governance in a Globalizing World," in Robert O. Keohane, ed., *Power and Governance in a Partially Globalizing World,* (London: Routledge, 2002), pp. 193-218.

Demographics, Migration, Urbanization

More people, more people on the move, and more young people are creating formidable challenges. The U.S. Census Bureau estimates that 44 percent of the world's population is under the age of 25[108] and projects a population increase worldwide from 6 billion in 1999 to 9 billion in 2042[109], with highest growth rates in an arc extending from Brazil, through Africa, the Middle East and the Caucuses to South and Southeast Asia. Academic and government studies show that a youth bulge in this arc increases the likelihood of instability, extremism, and outbreaks of civil conflict.[110] People on the move include highly skilled professionals, economic migrants with few skills, and large numbers of refugees and displaced persons.[111] For the first time in history, according to United Nation and World Bank reports, more than half of the world's people live in cities.[112]

Layered Governance

More governance occurs in global, regional, sub-national, and non-territorial public spheres. State actors still dominate on many global issues. Increasingly, however, rules governing behavior and means to satisfy human needs and wants exist in:

- global and regional associations of states (United Nations, World Trade Organization, and the European Union)
- sub-state connections between provinces, cities, "countries within countries" (Quebec and Kurdistan)
- networks of government professionals focused on single issues
- the activities of a multitude of civil society actors at all levels

---

108. U.S. Census Bureau, see http://www.census.gov/cgi-bin/ipc/idbagg
109. U.S. Census Bureau, see http://www.census.gov/ipc/www/idb/worldpopinfo.html
110. See for example http://www.foia.cia.gov/2020/2020.pdf
111. Robert P. Cincotta, Robert Engleman, Daniele Anastasion, *The Security Demographic: Population and Civil Conflict After the Cold War, Population Action International,* Washington, DC, 2003http://www.populationaction.org/Publications/Reports/The_Security_Demographic/The_Security_Demographic_Population_and_Civil_Conflict_After_the_Cold_War.pdf; UNHCR, *2006 Global Trends: Refugees, Asylum Seekers, Returnees, Internally Displaced and Stateless Persons,* June 2007 http://www.rms.org.nz/document/UNHCR%20global%20trends%202006.pdf
112. UN General Assembly, GA/EF/3160, 26 October 2006. See http://www.un.org/News/Press/docs/2006/gaef3160.doc.htm

Many "Big Ideas"

A contested mix of secular and religious ideas—globalization, fundamentalism, terrorism, multiculturalism, post-colonialism, and anti-Americanism—has replaced the secular ideological struggles of the last century.[113] Leaders, practitioners, scholars, and publics now debate "clashes of civilizations," "plural identities," "religious and secular authority in governance," "terrorism," "zones of democratic peace," "support for democracy," "climate change," "the promise and perils of globalism," and varieties of "anti-Americanism." Within Islam, the contrasting views of Sunni and Shia, and adherents of violent and non-violent means in each, are shaping geopolitics and the future of one of the world's great religions.

Networks and Non-State Actors

Driven by globalization and a digitized information environment, networks are becoming the dominant architecture of society and politics.[114] Rapid change and reversible processes flatten hierarchies. Vertically, command and control models matter less, but they still matter. Horizontally, "social capital" models matter more. Global problems outrun the capacities of stovepiped institutions. Small events have systemic effects. Extraordinary growth is occurring in networks of regional and global groups with activist, corporate, religious, ethnic, terrorist, criminal, and knowledge-based agendas.

New Paradigm of War

Armed conflict within civilian populations by state and non-state contestants in frequent long-term conflicts is now the norm. Wars between states are rare.[115] Today, adversaries with global reach and no fixed location successfully challenge sovereign states with fixed borders and known vulnerabilities. The media are a

---

113. See, for example, Amartya Sen, Identtity and Violence: The Illusion of Destiny, (New York: W.W. Norton & Company, 2006).
114. Manuel Castells, The Rise of the Network Society, Vol 1 of The Information Age: Economy, Society, and Culture, (Malden, MA, Blackwell Publihsers, 2006).
115. As Philip Bobbitt states: "National security will cease to be defined in terms of borders alone because both the links among societies as well as attacks on them exist in psychological and infrastructural dimensions, not on an invaded plain marked by the seizure and holding of territory." *The Shield of Achilles: War, Peace, and the Course of History,* (New York: Vintage Books, 2002), p. 813. Rupert Smith argues similarly, that "war as battle in a field between men and machinery, war as a massive deciding event in a dispute in international affairs: such war no longer exits." *The Utility of Force: The Art of War in the Modern World,* (New York: Alfred A. Knopf, 2007), p. 3.

decisive theater of operations. Virtual conflict and "perceptual damage" are as important as real conflict and real damage.

Digital Technologies[116]

The Internet is transforming diplomacy, markets, media, civil society, and war. North America, Oceana/Australia, and Europe lead the world in Internet penetration as a percentage of population. Asia, Europe, and North America have the greatest numbers of users. The highest rates of usage growth, however, are in Africa, Latin America, and the Middle East. Mobile devices, expanded bandwidth, software innovation, and an explosion in use by non-Westerners are generating new forms of horizontal collaboration and competition. The Internet is enabling discovery, innovation, and value creation on an unprecedented global scale. Likewise unprecedented is its use by terrorists and insurgents for planning, publicity, recruitment, fundraising, and training. Society's dependence on the Internet increases vulnerabilities to cyber attacks. More than other form of media, the Internet detaches content from sender identity and social frames that give credibility and meaning. Source and context are not necessarily self-evident (Al Qaeda's terrorists, Second Life's avatars), and tactical events become instant strategic problems (Abu Ghraib, Danish cartoons).

Climate Change, Scarce Water, and Energy

A growing scientific consensus argues that global warming is accelerating, sea levels are rising, and weather severity is increasing. According to the 2007 *UN Human Development Report*, "Climate change is the greatest challenge facing humanity at the start of the 21st Century" raising the "specter of unprecedented reversals in human development."[117] The same report finds that a "water crisis is deepening around the world," that "more than one billion people lack clean water for drinking," and that 2.6 billion "lack sanitation." Dwindling supplies of cheap petroleum and other energy sources is coupled with increasing demand. Government-controlled national oil companies dominate oil supplies and prices. The search for more oil and alternative energy sources is creating an energy transition and changing geopolitics.

---

116. See Chapter 26 for an expansion on this topic.
117. *Human Development Report 2007/2008. Fighting climate change: Human solidarity in a divided world.* United Nations Development Programme. 2007.

Global Media

Advanced technologies are transforming global media and creating new media forms—24/7 news streams, satellite and cable television, video for high broadband, video for cell phones, blogs, video games, and more. Western media no longer dominate. Challenges come not only from Al Jazeera (Arabic, English), pan-Arab media, and robust Asian and Latin American satellite networks, but also from rapid growth in low budget, good quality local media around the world. The United States and many other countries are experiencing a decline in appointment news and print media consumption, and a rise in multi-channel Internet, cable, and talk radio news. Pervasive many-to-many communication raises central investment and production issues for one-to-many broadcasting by government and commercial services. The viral spread of unmediated information creates formidable problems for all stakeholders, political leaders, media organizations, and news consumers.

State Challenges

States are changing too. China, India, Russia, and Iran are projecting more regional and global influence with new hard and soft power assets. Petroleum-based autocracies (such as Venezuela) with surplus resources play on the world stage. Demographic pressures, group grievances, poverty, and a host of other drivers of instability are creating failed states, including prominently Sudan, Iraq, Somalia, Zimbabwe, and Afghanistan.

Positive Trends: Opportunities

Not all change is bad. There are positive global trends and opportunities as well. These positive trends include the fact that freedom and democracy has had a 30-year gain—from 42 "free" countries in 1976 to 90 "free" countries in 2006, although it has been flat since its 1998 peak.[118] There has been an increase in international assistance by non-governmental organizations (Doctors without Borders, Gates Foundation, and Oxfam). Increased innovation and a rapid rise in the use of the Internet, mobile devices, bandwidth, and collaboration software are enabling communities of interest and new forms of value creation in a global community. The life expectancy gap is closing between developing and high-

118. Arch Puddington, *Freedom in the World 2007: Freedom Stagnation Amid Pushback Against Democracy.* See http://www.freedomhouse.org/template.cfm?page=130&year=2007.

income countries. Survival rates of children are increasing with 2.1 million fewer deaths in 2004 than in 1990. Adult literacy has increased from 75 to 90 percent since 1990 and primary school enrollment is up. Since 1990, the percent of people around the globe living under $1 per day is down from 28 to 21 percent. Taken together, these improvements in wealth, health, education, freedom, civil society engagement and technology provide hope and new opportunities.

Negative Trends: Threats

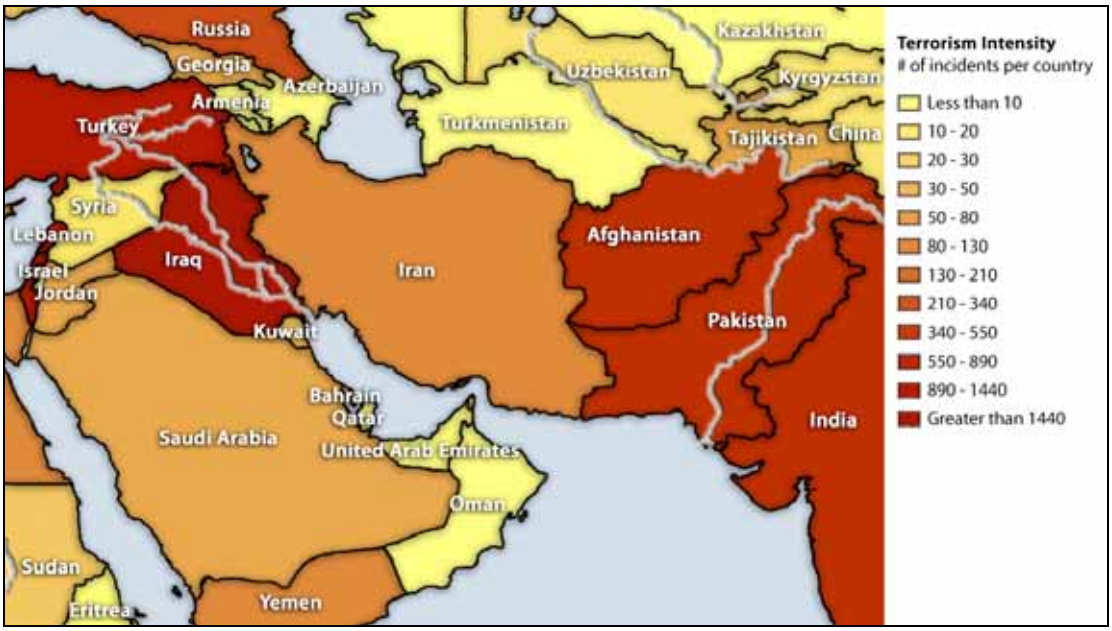
Unfortunately, these positive trends are countered by a number of negative trends. Between 1959 and 1999 the world population grew from 3 billion to 6 billion, and is projected to grow to 9 billion by 2042, with a notable youth bulge in vulnerable countries. In addition, the United Nations (UN) warns that climate change (e.g., rising sea levels) will be the "greatest challenge facing humanity." The UN also notes the "water crisis is deepening" with more than 1 billion people lacking clean water and 2.6 billion lacking proper sanitation. While many search for alternative fuels, global fossil fuel demand is up and supply is down driving higher prices as government oil companies dominate (Saudi Arabia, Venezuela, Russia). Based on an index of instability indicators, a number of states are considered "failed" including Sudan, Congo, Ivory Coast, Iraq, Zimbabwe, Chad, Somalia, Haiti, Pakistan, and Afghanistan.

The Internet is been used as an asymmetric weapon by terrorists (for secure communication, planning, publicity, recruitment) and represents a vulnerable critical infrastructure subject to cyber attack. Also, global communications can make instant strategic problems out of tactical events (such as Abu Ghraib). Illicit networks, such as AQ Kahn, have increased the risk of proliferation of nuclear weapons, materials, and knowledge to state and non-state actors.

According to the UN High Commissioner for Refugees, the number of worldwide refugees has surged (driven by Iraq) to 9.9 million, including 4.3 million Palestinians. Worldwide there are 24.5 million displaced persons. By 2010, more than half the world's population will live in cities. Infectious disease remains a threat, especially HIV/AIDs in Africa as well as global risks of tuberculosis, severe diarrhea, repertory infections, and malaria.

According to the National Counterterrorism Center (NCTC) Worldwide Incident Tracking System, in 2006 terrorist attacks increased over 25 percent (to

14,000) resulting in a 40 percent increase in deaths (20,000), the majority of which have occurred in Iraq.[119] As illustrated in Figure 7-2, nearly all of the attacks with more than 10 deaths have occurred in the Near East and South Asia, while attacks elsewhere have declined. A worrisome trend is that sub-Saharan Africa incidents are up 64 percent from last year, from 256 to 422 incidents. Global changes that occur faster than people can accept them breed frustration and humiliation. In the words of author Thomas Friedman, terrorism is spawned by a poverty of dignity, not a poverty of money.[120] Finally, UN statistics show a rise in crime in all countries.



Source: Terrorism Knowledge Base, see www.tkb.org

Figure 7-2. Terrorism Intensity across the Middle East

In conclusion, leveraging opportunities is as important in strategic communication as defending against threats. Positive trends that provide new strategic communication opportunities include:

- an increase in the world's democracies (Freedom House finds 90 countries were "free" in 2006, compared with 42 in 1976.)

119. See www.nctc.gov
120. Thomas L. Friedman, "A Poverty of Dignity and a Wealth of Rage", The New York Times, July 15, 2005. See http://thomasfriedman.blogspot.com/2005/07/poverty-of-dignity-and-wealth-of-rage.html

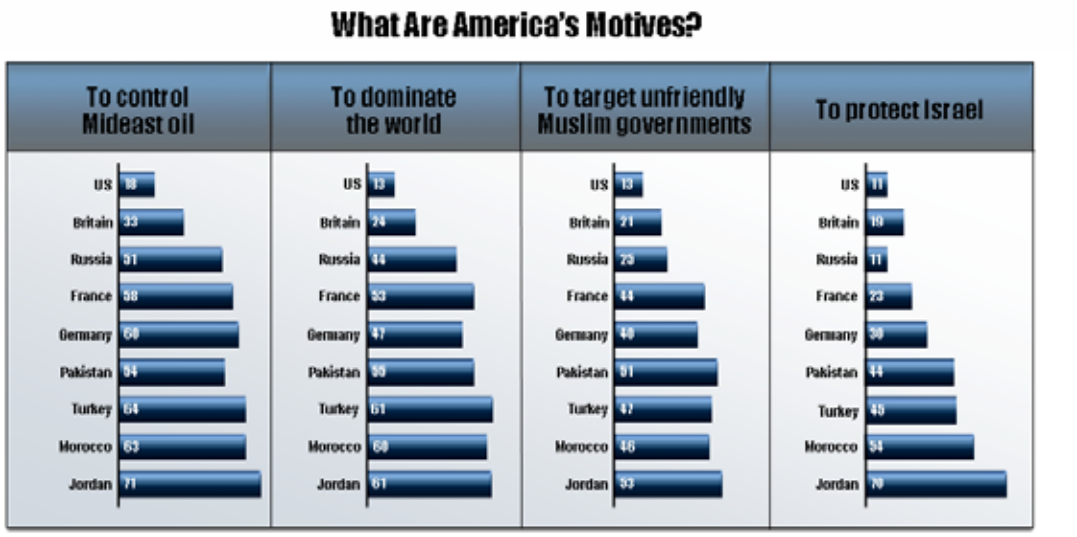
- an explosion of humanitarian and nongovernment organizations (Oxfam, Medecins Sans Frontieres, the Gates Foundation)
- newly empowered individuals at all levels of society collaborating and sharing knowledge with mobile and virtual technologies
- an increase in average life expectancy
- a decrease in child mortality
- a rise in adult literacy and primary school enrollment rates coupled with a shrinking gender gap
- an overall decline in income poverty generated by high economic growth rates in China and India

Negative trends with particular relevance to strategic communication include:

- social unrest driven by the size and location of youth populations
- economic migrants, refugees, and displaced persons
- the spread of infectious disease
- extremism and religious militancy born of frustration, humiliation, and change that is faster and deeper than people and cultures can accept

Anti-Americanism on the Rise

One particularly negative trend worthy of highlighting is that America suffers an image problem around the globe. This problem includes attacks on America's policies as well as suspicions of America's intentions. For example, via a series of multinational surveys focusing on worldwide issues, the Pew Global Attitudes Project has found America's motives are questioned. The Pew Foundation (Kohut 2007) found widespread opposition to the war in Iraq with strong anti-American sentiments among Muslim publics. A 2005 Pew poll found that many in Muslim countries believed suicide attacks against Americans and other Westerners in Iraq were justifiable. Pew's 2006 poll showed that majorities in Jordan, Turkey, Egypt, Indonesia, and Pakistan believe the war in Iraq has made the world more dangerous. More startling, their 2005 poll found about half of Moroccans (56%) and Jordanians (49%) and about one-in-four in Turkey believe suicide attacks against Americans and other Westerners in Iraq are justifiable. Many foreign publics in the Mideast, Europe, and beyond question America's motives. As shown in Figure 7-3, majorities in Pakistan, Turkey, Morocco, and Jordan believe U.S. motives are to control Mideast oil, to dominate the world, to target unfriendly Muslim governments, and to protect Israel.



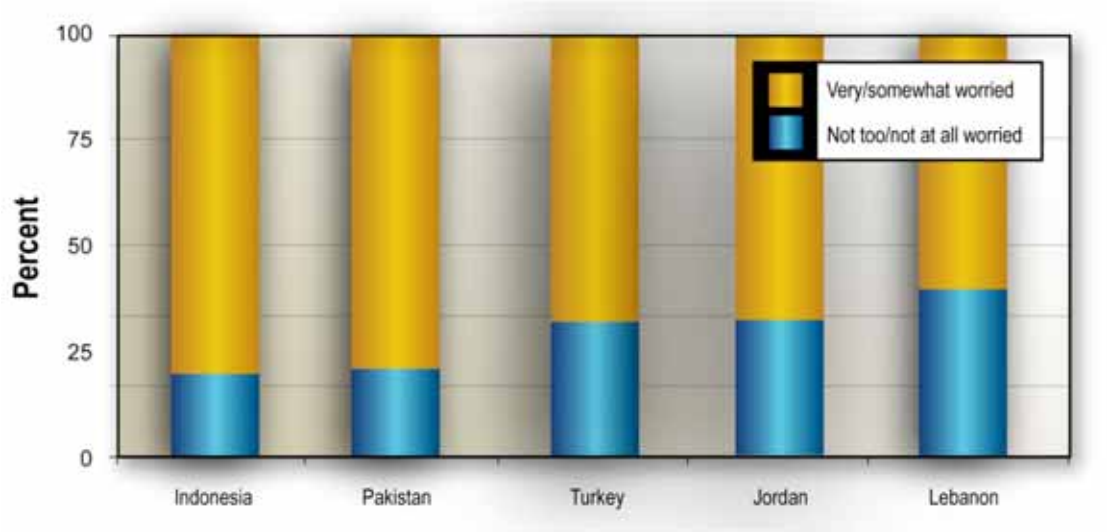
Questions asked of those who believe the war on terrorism is not a sincere effort, or have mixed views. Percentages show the percent of the TOTAL POPULATION who believe each is an important reason the U.S. is conducting the war on terrorism.

Source: Pew Report, A Year After Iraq War

Figure 7-3. Suspicions of American Power

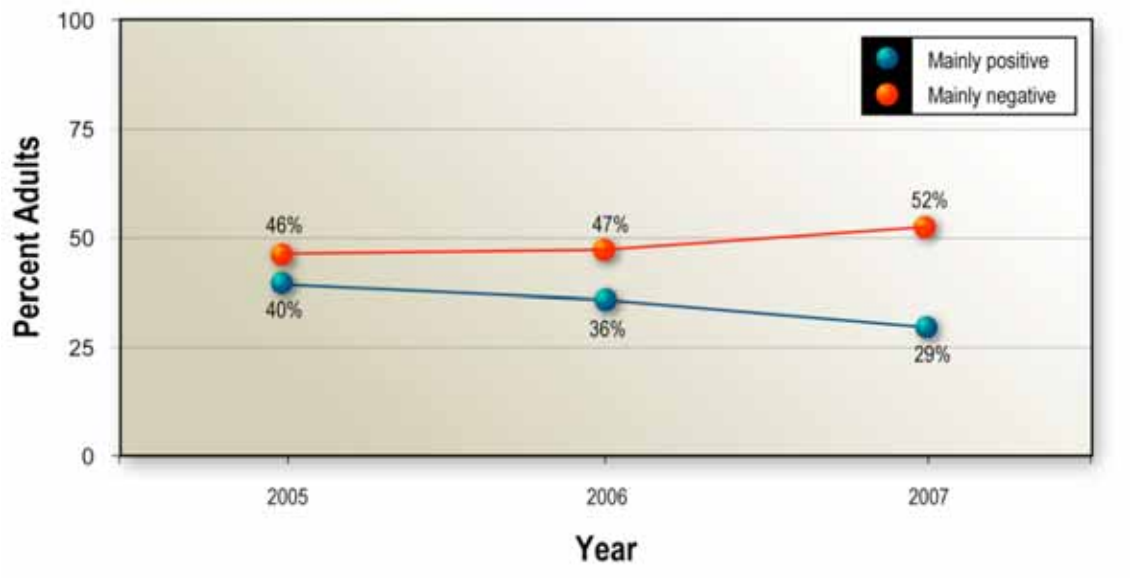
As illustrated in Figure 7-4, all five majority Muslim countries now see the United States as a threat to their country.[121] Even the majority (nearly 70%) of the public polled in NATO member Turkey were "very" or "somewhat" worried that the United States could be a military threat against their country. Further, a BBC World Service poll of more than 18,000 adults in 18 different countries shows an increasingly negative view of the United States influence (Figure 7-5).[122] The Pew study found the United States was viewed around the world to be as dangerous as Iran and North Korea to world peace. Even 60 percent of Britons found the war in Iraq has made the world more dangerous.

121. Pew 2006.
122. BBC January 2007. See http://www.worldpublicopinion.org/pipa/articles/international_security_bt/306.php?nid=&id=&pnt=306&lb=btis



Source: Pew Report, A Year After Iraq War

Figure 7-4. United States Seen as Threat to Muslim Countries

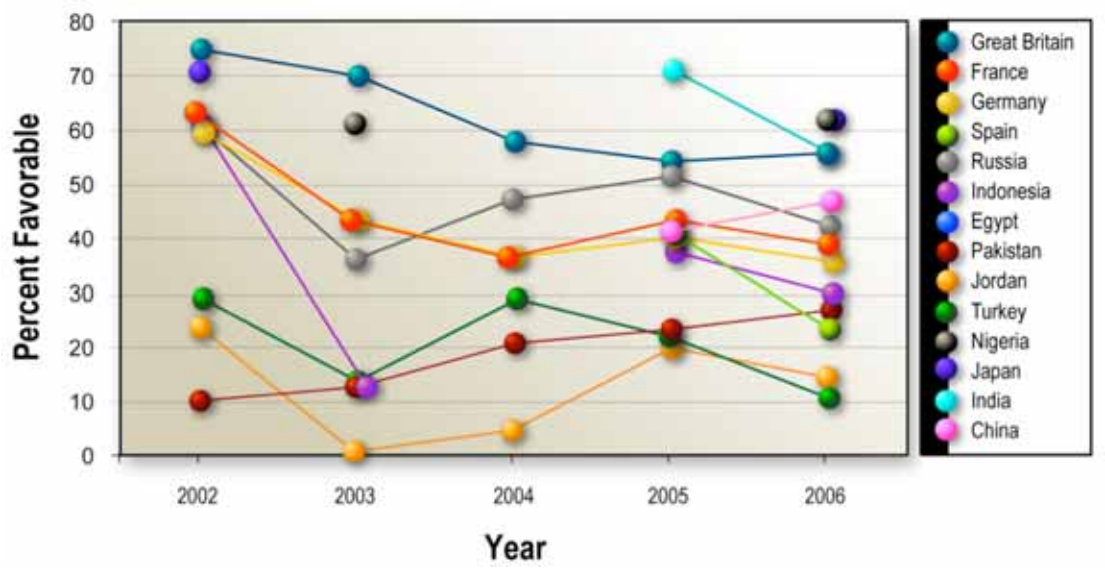


Source: BBC, January 2007

Figure 7-5. U.S. Influence Viewed Negatively

Figure 7-6 shows a multiyear trend of Pew surveys, which, except in Pakistan, illustrates a downward trend in favorable opinion of the United States in many countries.[123] Not only is the United States viewed with increasing disfavor, but also favorable views toward individual Americans (as distinct from the United States as a nation) have decreased, as shown in Figure 7-7.

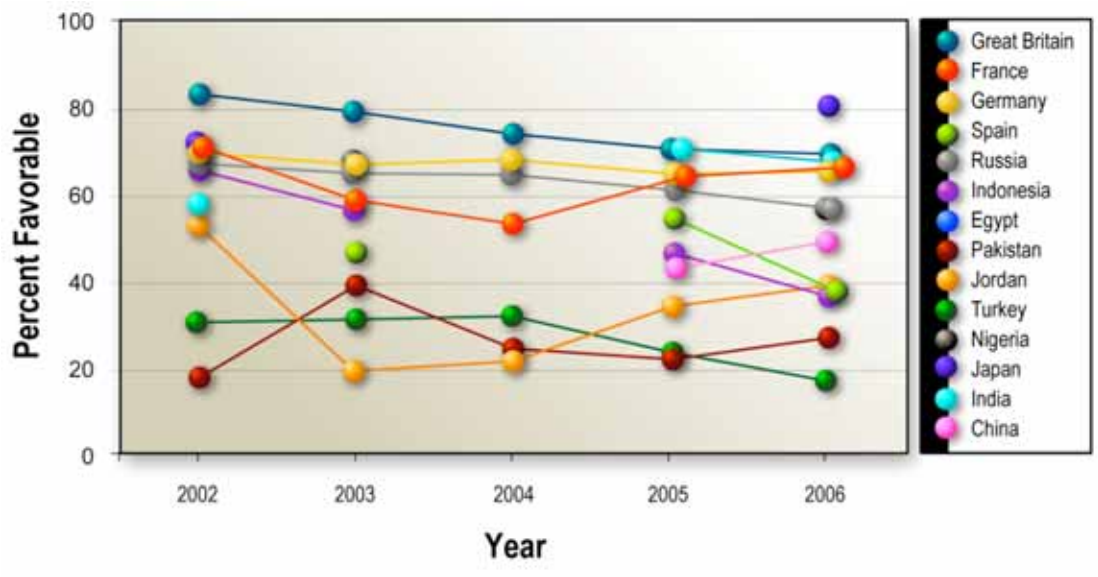
In spite of these negative perceptions abroad, however, there is some hope. For example, America's humanitarian response to the horrific December 2004 tsunami helped improve its image in the world's largest Muslim country, Indonesia. Following a significant drop of public support for American in response to the Iraq war, American aid resulted in more than doubling of support (from 15 to 38%) for Americans (see Figure 7-8).[124] Although less pronounced, Pew noted a similar pattern in Pakistan following U.S. aid for the October 2005 earthquake, from 23 percent in 2005 to 27 percent in 2006.



Source: Pew Global Attitudes Project

Figure 7-6. Downward Trend in Favorable Opinions of the United States

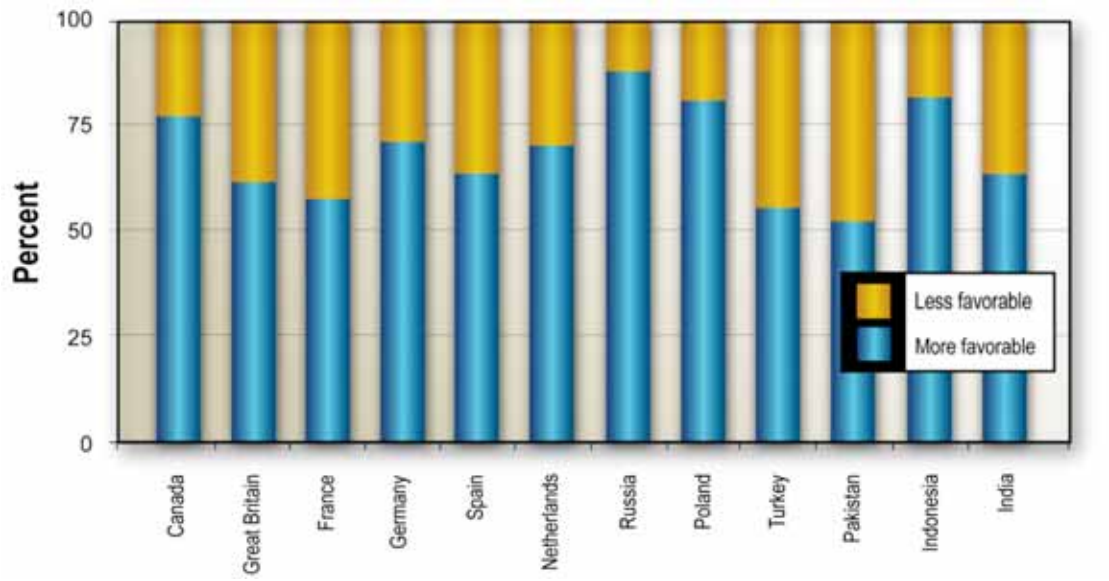
123. Pew, 2006. Pew Global Attitudes Project. *Conflicting Views in a Divided World: How Global Publics View: Muslim-Western Relations, Global Issues, U.S. Role in the World, Asian Rivalries.* See http://pewglobal.org/reports/pdf/DividedWorld2006.pdf.
124. Kohut, Andrew. 2007. America's Image in the World: Findings from the Pew Global Attitudes Project. Testimony to Subcommittee on International Organizations, Human Rights, and Oversight Committee on Foreign Affairs U.S. House of Representatives, March 14, 2007.



Source: Pew Global Attitudes Project

Note: Percent favorable indicates those responding with a very or somewhat favorable opinion of Americans.

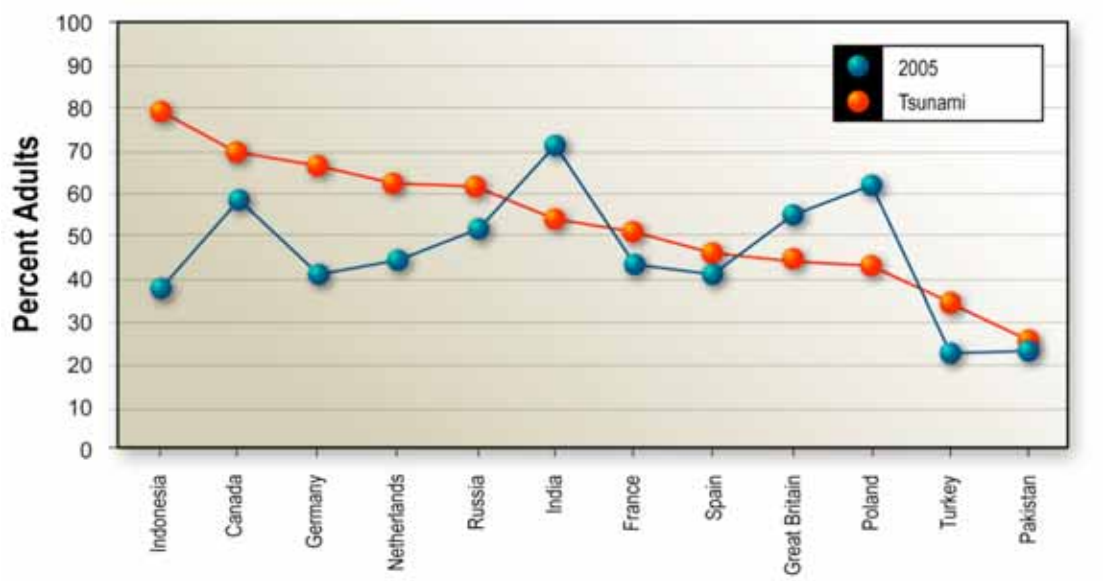
Figure 7-7. Downward Trend in Favorable Opinions of Americans



Source: America's Image in the World: Findings from the Pew Global Attitudes Project

Figure 7-8. Tsunami Relief Boosts U.S. Image

While it is difficult to ascribe favorable opinions of the United States as the result of particular incidents, favorability can be compared when polling similar populations on differing topics at the same time. With the caveat that correlation does not equate to causation, Figure 7-9 juxtaposes 2005 opinions of the United States in general and opinions of the U.S. Tsunami relief effort. In all but three countries surveyed (India, Britain, and Poland), the U.S. Tsunami relief efforts were viewed more positively than the United States in general.



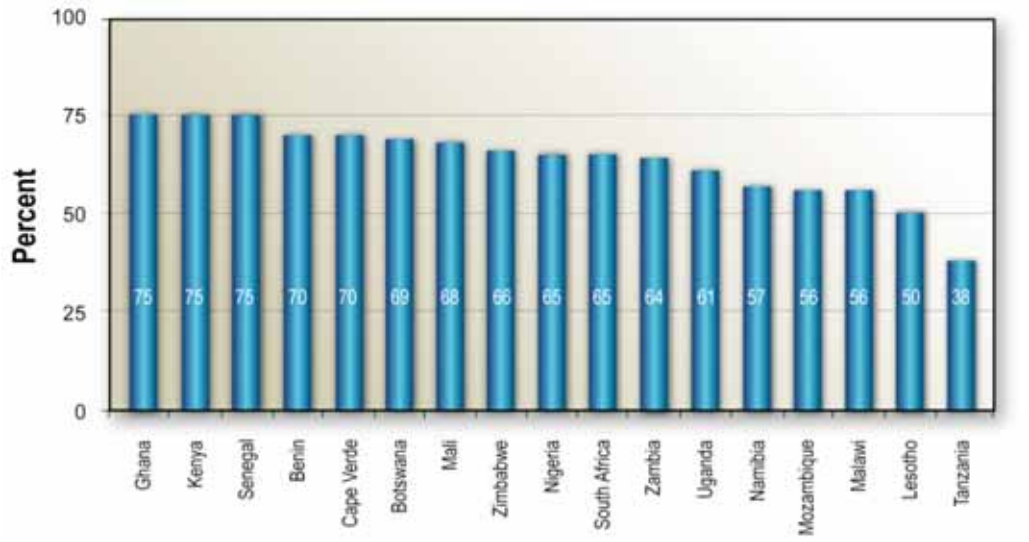
Source: Data from the Pew Global Attitudes Project.

Figure 7-9. Comparison of Favorability of the U.S. and Tsunami Relief

The United States need not be perfect, but simply better than the alternative peer or non-peer competitors. There are some indicators of hope. For example, the majority of publics in Africa prefer democracy to any other kind of government (Figure 7-10).[125] A 2005 sample of 2,089 Afghan adults found that 81 percent held a negative view of Al-Queda's influence on the world, 88 percent held a negative view of the Taliban, and 90 percent held an unfavorable (75% very unfavorable) view of Osama bin Laden.[126] That same poll found an 83

125. Afrobarometer, 2005. See http://www.worldpublicopinion.org/pipa/articles/brafricara/209.php?nid=&id=&pnt=209&lb=braf
126. Afghan, 2005. See http://www.worldpublicopinion.org/pipa/articles/brasiapacificra/155.php?nid=&id=&pnt=155&lb=bras

percent favorable (39% very favorable) rating of "the US military forces in our country." A 2007 poll found that 74 percent of Iranians have an unfavorable view of bin Laden.[127]



Source: Afrobarometer, 2005

Note: Percent saying "Democracy is preferable to any other kind of government."

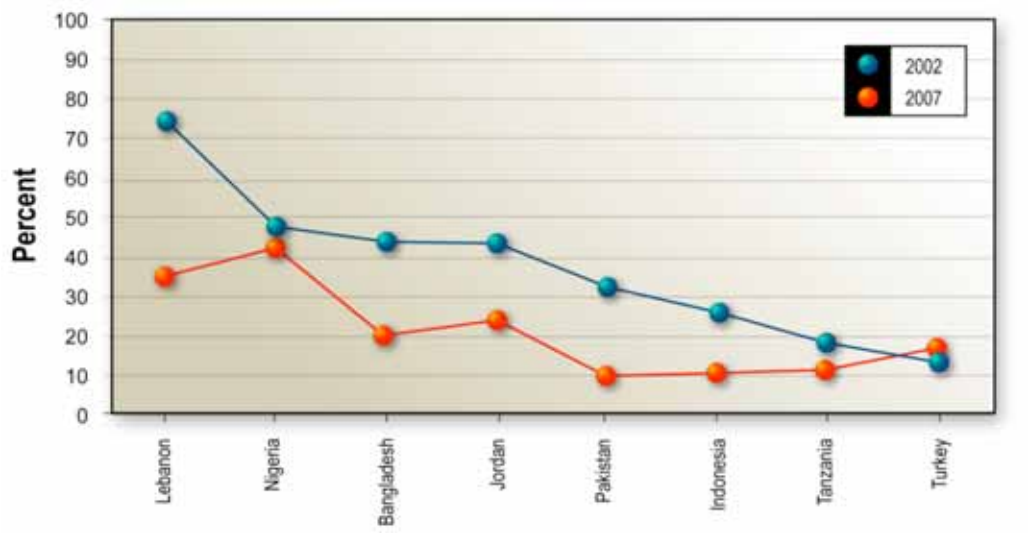
Figure 7-10. Democracy Preferred in Africa

There is also some optimism suggested by other trends in Arab opinion polls. A worrisome 2005 Pew Global Attitudes Project poll indicated that many in Muslim countries believed suicide attacks against Americans and other westerners in Iraq were justifiable. In that poll, just over half of Moroccans (56%) and nearly half of Jordanians (49%) thought such attacks justifiable. Even in Turkey, where bin Laden is unpopular and support for terrorism is generally low, about one-in-four said suicide bombings against Americans and Westerners in Iraq can be justified. Fortunately, as Figure 7-11 illustrates, many Muslim publics have shown reductions in support for suicide bombings against civilians, in some cases as much as 40 percentage point change in attitudes in the past five years. Unfortunately, a persistent worry is that 70 percent of respondents from Palestinian territories (roughly equally proportional across gender, ages, and

127. See http://www.worldpublicopinion.org/pipa/articles/brmiddleeastnafricara/313.php?nid=&id=&pnt=313&lb=btis

religiosity) believe suicide bombing against civilians can be often or sometimes justified. Also a concern, Muslim majorities in Lebanon, Kuwait, Jordan, and the Palestinian territories believe that tensions between the Sunnis and Shia are a problem beyond Iraq, although these views are not shared in Asian countries with large Muslim populations.[128] Muslim populations both in the Middle East and Asian continue to see the U.S. as a military threat.[129]

Except within the Palestinian territories where confidence remains high (57%), Muslims overall show very low confidence that bin Laden is a leader who will do the right thing in world affairs. For example, while four years ago 56 percent of Jordanians supported bin Laden, that support has dropped to only 20 percent in 2007.[130]



Source: About the Pew Global Attitudes Project, July 2007
Note: Percent who believe suicide bombing justified

Figure 7-11. Suicide Bombing Never Justified (Muslim Respondents)

128. Pew Global Opinion Trends 2002-2007: *A Rising Tide Lifts Mood in the Developing World. Sharp Decline in Support for Suicide Bombing in Muslim Countries*. July 24, 2007. http://pewglobal.org/reports/pdf/257.pdf, p. 58.
129. Ibid.. p. 58.
130. Ibid.. p. 148.

Implications for Strategic Communication

The future will not be just a projection of current trends. Surprise and punctuating events are inevitable. Nevertheless, understanding how the world is changing points to discernable implications for planning and investment priorities in strategic communication.

Durable, Expanded, Resourceful, Forward Leaning

The United States no longer has the luxury of a strategic communication instrument that is limited, reactive, and employed only episodically. Strategic communication is required before, during, and after violent conflicts, at home and abroad.

"No One Size Fits All"

Preoccupation with terrorism and current conflicts (Iraq and Afghanistan) marginalizes the use of strategic communication on other pressing issues: governance, economic growth, the distribution of public goods, and cross-border challenges.

Net-Centric Tools and Structures

Stovepipes, gatekeepers, and tribal cultures still dominate. Hierarchies have a role. However, today's information technologies and social structures favor networks and much stronger and more imaginative links between governments and civil society. Achieving this requires unusual leaders, hybrid institutions, and flexible practitioners. In strategic communication, as in other instruments of statecraft, the strategies employed, the skills developed, and the tools used need to be based on networking mindsets.

New Communications Paradigm

Strategic communication will require a much larger investment in "listening" understood as deep comprehension of cultures, attitudes, and influence network. It will require practitioners willing to take risks and policymakers comfortable with "edgy" attention-getting content. Strategic communication calls for varsity play in the next generation Internet, and rethinking the government's one-to-many mass audience broadcasting model from top to bottom. Diplomats and

soldiers must learn to operate successfully in the space between state and non-state actors on multiple issues in constantly changing patterns of interaction.

Trust and Attention Counts More than Information

Fifty years ago, governments took advantage of widespread demand for news and information. Today, information saturation creates an attention deficit. The signal-to-noise ratio makes communication more difficult. Disseminating information and "getting the message right" are not top priorities. Trust, credibility, actions, legitimacy, and reputations are critical to success.

Bridging the Challenge/Reform Disconnect

That the world is changing more rapidly than leaders, practitioners, and their institutions is not news. Reports with recommendations calling for change abound but few offer implementing roadmaps, and too many focus on change from within. Fixing strategic communication only from within means change that is marginal and slow. Fixing strategic communication requires focused attention and political courage from presidents and lawmakers. Radical transformation will take years.

Prepare for Uncertainty

Strategic communication requires leaders and practitioners recruited and trained to adapt quickly in a world in which unexpected personalities, low probability, high-impact events, and technology breakthroughs will play unforeseen roles.

Chapter 26. Technology is Changing

The previous chapter examined the positive and negative trends in the world and implications for strategic communication. This chapter considers the revolutionary changes in the ways people access and share information—principally as a consequence of the global spread of satellite television and the rise of the Internet.

Media Transformation

In the last two decades, revolutionary changes have occurred in the ways people access and share information, driven principally by the global spread of satellite television and the rise of the Internet (Figure 7-12). Today people everywhere have many alternative sources for news and entertainment; state control of content is becoming technically impossible; and the physical means of transport is no longer the primary concern as it has been in the past, when shortwave radio was the primary means of reaching citizens in foreign countries.

Figure 7-12. Media Access Then and Now

Traditional Media are Losing their Influence

Satellite and cable television have changed the nature of broadcast media by opening up an abundance of alternative channels to international audiences. Instead of being limited to a handful of broadcast channels, viewers are now offered an almost unlimited choice of channels. People are free to choose content that closely matches their own interests and biases. With the audience splintering and the variety in available viewpoints, the great trusted and unifying voices, such as Walter Cronkite, have been irrevocably lost. The media now serves to amplify any latent polarization, and the very presence of so many differing viewpoints has caused people to lose their trust in media itself.

A Pew Research poll released in August 2007 highlights some of these trends in the U.S. audience:[131]

On the trust in media:

> In 1985, most Americans (55%) said news organizations get the facts straight. Since the late 1990s, consistent majorities – including 53% in the current survey— have expressed the belief that news stories are often inaccurate. As a consequence, the believability ratings for individual news organizations are lower today than they were in the 1980s and 1990s.

On the growing partisan divide:

> In the current survey, however, fewer than half of Republicans (41%) express a favorable opinion of major national newspapers, a 38-point decline when compared with 1985.

Thirty years ago Americans typically had a choice of seven channels; now according to the Nielsen reports, the average U.S. home receives 104 channels.[132] In the competition for eyeballs this plentiful choice exacerbates the polarization of media. As Fox News turns right, CNN is forced to the left to retain its share. The same systemic behavior might be expected elsewhere in the world.

---

131. *Internet News Audience Highly Critical of News Organizations: Views of Press Values and Performance: 1985-2007*. The Pew Research Center, August 2007, see http://people-press.org/reports/display.php3?ReportID=348

132. See http://www.nielsenmedia.com/nc/portal/site/Public/menuitem.55dc65b4a7d5adff3f65936147a062a0/?vgnextoid=48839bc66a961110VgnVCM100000ac0a260aRCRD

Worldwide Satellite Access

Satellite television is now the primary means of media access in most of the world. In the Middle East and North Africa only Afghanistan relies more on radio than television for news and entertainment. In other countries the use of television exceeds that of radio by more than 2 to 1. Even in Iran, perhaps the most tightly controlled regime for media, citizens are able to access uncontrolled content on satellite television. The Islamic Republic of Iran Broadcasting approves and monitors all television and radio programming put on the air. However, in their quest for alternative perspectives and lighter fare, Iranians tune to expatriate-run satellite stations, flouting the official ban on dish ownership. Los Angeles-based stations garner more than 10 percent weekly viewership in spite of the Islamic Republic's crackdowns on dish ownership.[133] In addition, Voice of America Persian TV has significant weekly audience reach.

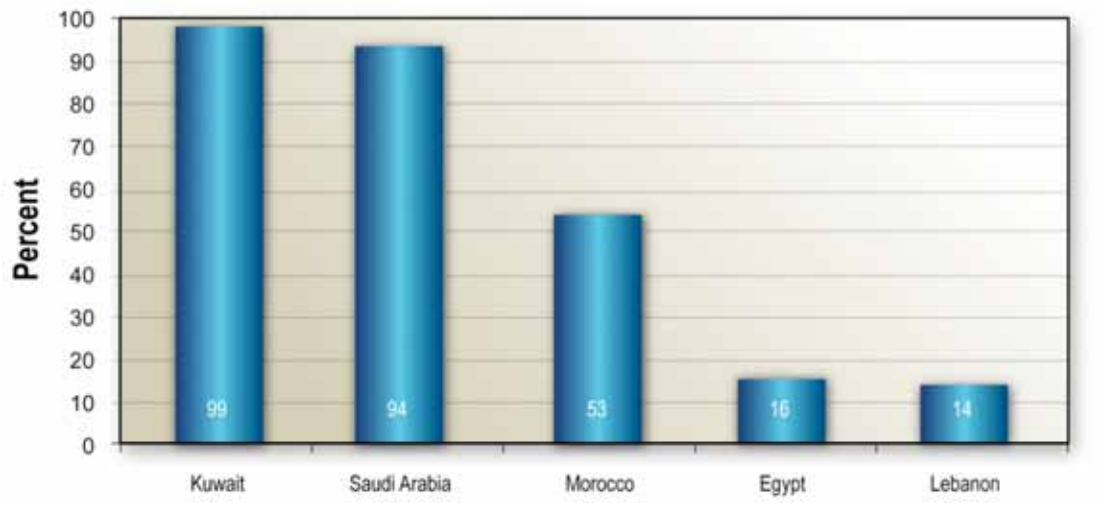
Direct-to-home television now serves about 24 percent of households in the Mideast, and Arab consumers typically have access to some 55-60 free-to-air Arabic language services (Figure 7-13). Al Jazeera was launched in 1996 out of Qatar, and now rivals the BBC in the number of worldwide viewers in the range of 40–50 million. Al Jazeera's viewing tops 70 percent in the Gulf Kingdoms and almost 60 percent of adults in Morocco and Tunisia. This popularity has largely been achieved by taking on subjects that were once considered politically or culturally taboo, and in spite of provoking the ire of regional governments and socially conservation elements. The prevalence of satellite dishes in the Middle East is best illustrated by this picture of an Arab village (Figure 7-14).

Popular programming in the Middle East may not be that different than in the United States—entertainment, news, reality shows, call-in shows, and even "Who Wants to be a Millionaire" or "Star Search," modeled after "American Idol." A representative from Intermedia, experienced in researching Middle East audiences, explained to study partipcipants that "allowing self-criticism" was the best way to acquire credibility for U.S. content in this region.

In their quest for increased viewership, broadcast news coverage everywhere invariably emphasizes sensational events, giving terrorists and insurgents an easy and automatic way to publicize their actions. The nightly news leads with videos of bombings, and the building of a new school doesn't even make the cut. News

133. Intermedia.

is, almost by definition, bad news. Consumers are usually looking for entertainment, and crime, mayhem, tragedies, and the like are considered entertaining. The strategic communication problem is to make good news as entertaining as bad news. Needless to say, this is a considerable challenge.



Source: Intermedia

Note: Percent of adults who report owning a satellite dish

Figure 7-13. Dish Ownership in the Middle East

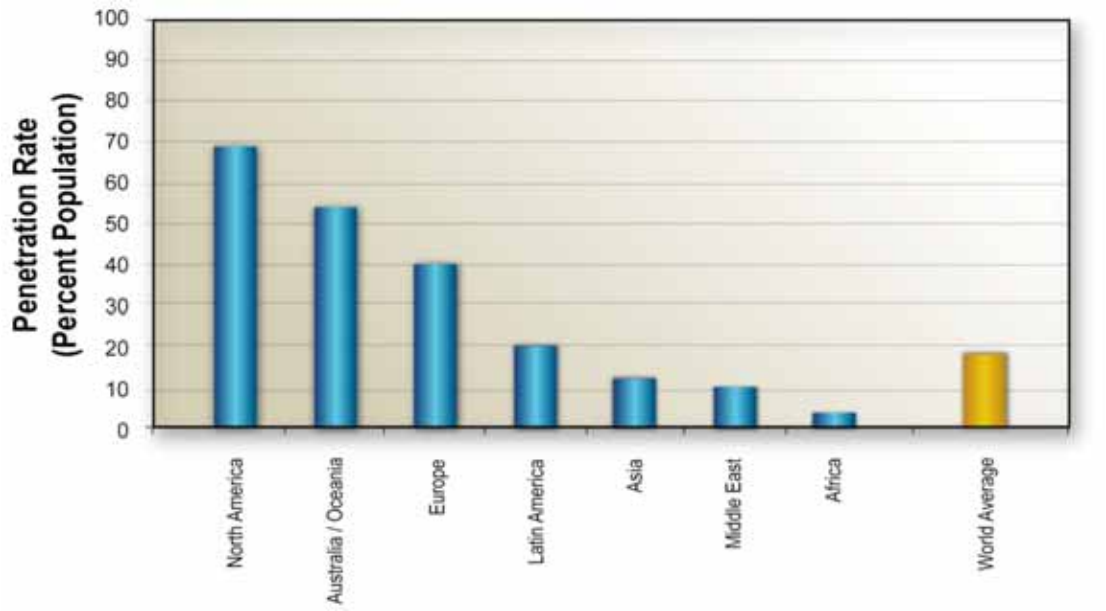
Source: Intermedia

Figure 7-14. Satellite Dishes in an Arab Village

Terrorists also have other advantages in their use of media. They have fast response and great flexibility, enabled by a decentralized leadership with local autonomy. Moreover, they are unconstrained by considerations of truth. Their concern with communication is exemplified by actions that seemed to have been planned with media attention as the primary objective.

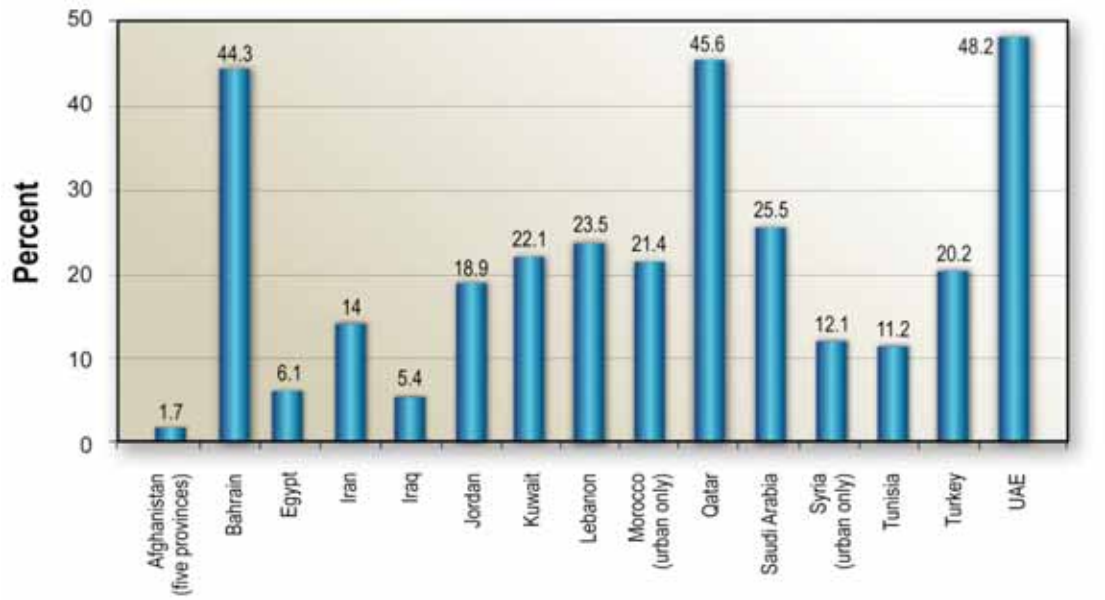
The Global Rise of the Internet

About a quarter of Americans currently use the Internet as their primary news source. These Internet users tend to be younger and better educated than the public as a whole, and a recent Pew survey finds that they hold relatively unfavorable opinions of the mainstream media. The United States is, of course, relatively advanced in its use and reliance on the Internet. Much of the rest of the world is still evolving in its Internet access, and may follow the general rule of exponential growth with an annual doubling in the number of users (Figure 7-15). Although the penetration of the Internet in the Middle East is only estimated at only 10 percent, a larger number of people may occasionally access the Internet in public kiosks, such as at Internet cafes. A poll from Intermedia breaks down access based on weekly usage as shown in Figure 7-16.



Source: www.internetworldstats.com

Figure 7-15. Internet Penetration by World Region



Source: Intermedia

Figure 7-16. Percentage Using the Internet Weekly in Mideast Countries

This survey data may obscure the possibility that the relatively small number of Internet users may be among the most influential people in the country. Moreover, the information these users gain on the Internet may be spread by word-of-mouth, or reported by the more conventional media. Thus, it is hard to determine the overall importance of the Internet in influencing opinions abroad. However, it is certain that is that the number of Internet users is inevitably growing.

Information Flows on the Internet

The Internet has broken the traditional broadcast paradigm. Instead of one-to-many, as in the broadcast media, the primary flows are one-to-one. The paradigm here is *pull*, rather than *push*. Consequently, it is observed that on the Internet broadcast is hard, but conspiracy is easy. While satellite television has both dramatically increased the reach of broadcast media and splintered its audience, the rise of the Internet has personalized news, empowered the individual to become a news source, and facilitated the gatherings of like-minded people.

The Internet offers a number of different models for information flow. The closest to the traditional broadcast model is the handful of mega-sites devoted to news, such as CNN, MSN, the New York Times, and other print and television organizations looking to expand the reach of their content into the new medium.

According to figures tracked by Nielsen/NetRatings, nytimes.com attracted about 12.5 million readers worldwide in June 2007. That is a huge global audience for news, and approximately ten times the *Times'* print circulation.

There is a phenomenon on the Internet known as the "long tail." Access is dominated by a few popular sites, followed by a multitude of sites (the long tail), each with very few viewers. The Internet greatly exacerbates the splintering evident in satellite television; instead of a thousand channels, there is an unlimited number, and the cost of broadcast is almost zero. Anyone can be a broadcaster, and everyone can easily find a source of content that exactly matches his or her own biases.

Many of these "broadcast channels" take advantage of the Internet paradigm by enabling individual visitors to post comments. For example, the Al Jazeera English web site posts comments from individuals, many of which are critical of the Al Jazeera coverage. Such critical comments appear to contribute positively to the overall credibility of the site.

The most popular web sites on the Internet do not vary greatly from country to country. Table 7-2 compares the list of site popularity in the United States with that in Iran. The list is dominated by the search engines, connectivity suppliers, and repositories of basic information.

The popular search engines Yahoo, Google, and MSN, have enormous power in information space; so much so that there have been instances where states have censored their search results. In a sense, these engines are politically and culturally neutral, depending on computer algorithms to determine best fits for queries. Google uses a page-rank algorithm, which uses a link analysis of the web to determine which sites are most linked by other sites on a given topic. (There are other factors considered in addition, and the algorithm is kept secret.) In whatever manner the rankings are determined, they shape the world opinion on important subjects. Furthermore, these search engines are used to derive a great deal of contextual information relevant to strategic communication.

In addition to search engines and commercial information providers, there are a number of enormously popular sites that enable or facilitate individuals to post and exchange views, information, images, and opinions. In the United States, those sites on the list include Myspace (social interactions), YouTube (videos), Facebook (social interactions), eBay (auction), Craigslist (lodging), Wikipedia (encyclopedia entries), Blogger.com (tools for blogs), Photobucket (images), and Flickr (photos).

Table 7-2. Most Popular Web Sites, August 2007

	United States	Iran
1	Yahoo	Yahoo
2	Google	Google
3	Myspace	Rapidshare
4	YouTube	MSN
5	MSN	Megaupload
6	Wikipedia	Persianblog.com*
7	Amazon.com	Tinypic
8	AOL	Wikipedia
9	Blogger.com	4Shared
10	Go	Window Live
11	Megaupload	Farsnews*
12	CNN	Lana.ir*
13	Internet movie database	Mobile9.com
14	Photobucket	GSM.ir
15	Comcast	Internet movie database
16	Microsoft	Parseek.com*
17	Flickr	Islamic Republic News Agency

*In Persian

Source: Alexa International

A second model for information flow on the Internet is exemplified by Wikipedia, which has become the international authority on encyclopedia-style information by implementing an open source model where entries are iteratively corrected by users. (There is moderation by a steering committee.) Supposedly, the information is self-correcting, and entries eventually settle to a communal "truth" that in some cases may exhibit a bias representing the main view of the interested community. Wikipedia might be taken as an instance of the phenomenon known as "the wisdom of crowds."

Viral Information

Perhaps the most important model of information flow on the Internet is that of viral connectivity. Sites like Myspace, YouTube, Facebook, Blogger, Photobucket, and Flickr enable the exchange of information from one individual

to another. A piece of information flows from one individual to another, with a multiplicative effect as it spreads like an epidemic. Studies have verified the popular notion of "six-degrees of separation," showing how little reach is required to achieve widespread communication.

Perhaps the power of viral communication is exemplified in how quickly good jokes can traverse the world practically overnight. In the Internet world a blogger might create a story that gets popularized by being quoted and linked by other sites. These links are noted by Google, which moves the blog site up on its ranking. Technorati.com adds the site to its current list of the most popular blogs (Figure 7-17). Both of these reports provide positive feedback to amplify the popularity of the original story—regardless of whether it is right or wrong, good or bad.

In order for this "information infection" to occur, the information must have the property of inducing replication—something that cries out for being passed along. A research question is how to create "good viruses" and how to contain the contagion of "bad viruses."

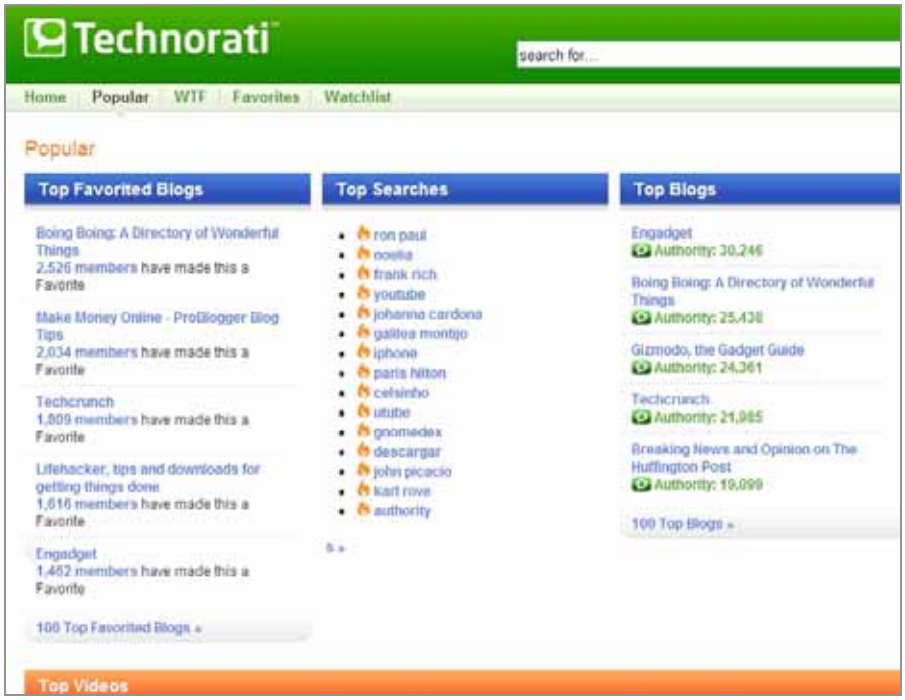


Figure 7-17. Guide to Blogs on Technorati.com

Some critics worry that blogs exacerbate social tensions by handing a powerful free electronic platform to extremists. Bad people find one another in cyberspace and so gain confidence in their ideas. The conventional media filter out extreme views to avoid offending readers, viewers and advertisers, while most bloggers have no such inhibition. On the other hand, blogs have a self-correcting mechanism of real-time criticism that is lacking in the conventional media.

There are an estimated 80 millions blogs currently on the Internet. While the great majority of all these blogs are voices in the dark, there are others that can be quite influential. Once again there is an instance of the long tail. Which few are the most popular, and/or the most influential? Taken in its totality, the "blogosphere" constitutes a treasure trove that can be mined for sociological and cultural information and opinion. For example, blogs can give insight into questions such as: What are the Islamic bloggers saying about a recent Al Qaeda action?

The United States has limited resources to counter this multitude of individual blogs. Those resources should be reserved for only the most influential blogs as determined by quantitative measurements. Even in these cases it is not clear what the rules of engagement should be. When should responses be identified as from the U.S. government, as opposed to from responsible individuals? What forms of response are most effective? In this evolving medium the United States has little experience or wisdom in means of influence.

Viral information is also exemplified in the meteoric rise of YouTube since it was founded in February 2005 (Figure 7-18). Users contribute videos, which are accessible by other users. YouTube now serves in excess of 100 million videos each day. Some of these videos become enormously popular, while most languish unseen—another "long tail." YouTube lists prominently the most popular videos, which then become famous for being famous. A popular video on YouTube can be viewed by millions of people and have considerable influence in the Internet world. The phenomenon needs study to understand the characteristics that underlie such popularity.

The world's youth is congregating in chat rooms, on MySpace and FaceBook, and in massively multiplayer online role-playing games (Figure 7-19). In 2006, the number of registered users on MySpace exceeded 100 million. In these Internet "places" young people are making friends, exchanging information and opinions, and forming coalitions in chat rooms. In many cases there is nary an adult present.

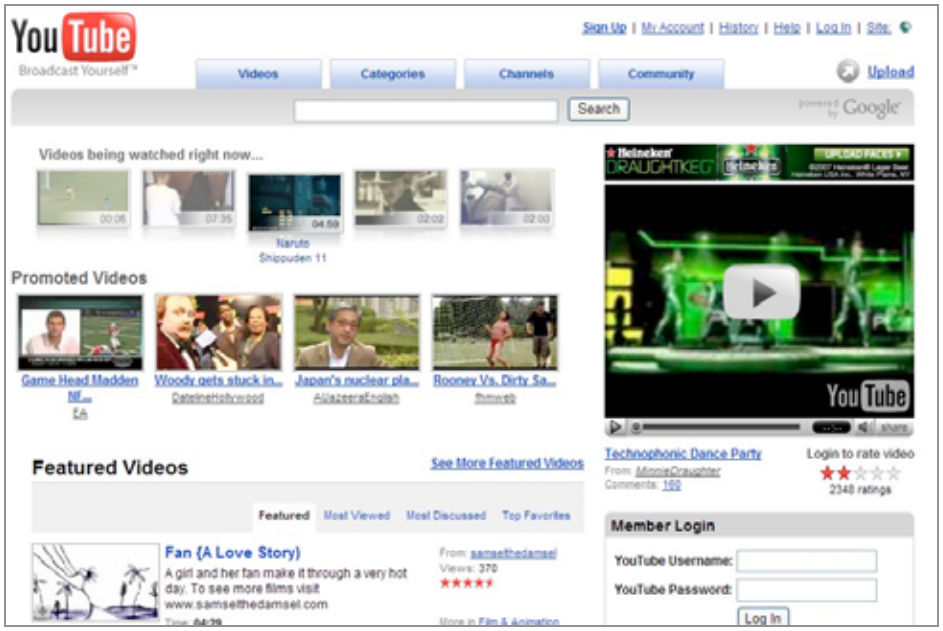


Figure 7-18. User-supplied Videos on YouTube

Figure 7-19. Where the Youth of the World Gathers

The chat rooms and multi-player online games serve as worldwide laboratories for the study of the cultures and evolving opinions of the youth. Aside such studies, it is not clear how these media can be used for influence. As in the case of blogs, the questions of if, when, and how to enter these media have no obvious answers.

Technology Transformation

Foreign Language Information Access

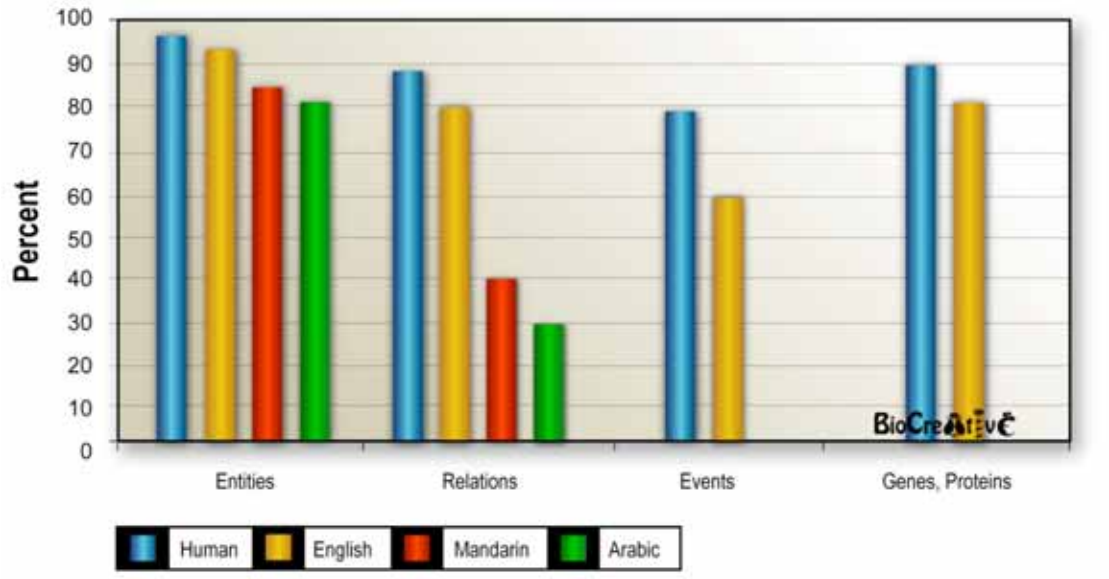
Human language technology provides a window into foreign cultures and concerns as well as a vehicle for engagement. In terms of understanding content, as Figure 7-20 illustrates for English language text the current best systems enable the automated extraction of entities (e.g., people, places, and things) at 95 percent accuracy, relations among entities (e.g., person A was the leader of organization Y at time T) at 70–80 percent accuracy, and events (e.g., organization Z purchased WMD pre-cursor material W from person Q, for example) at about 60 percent accuracy.[134]

Entity, relation, and event extraction systems are, respectively, approximately 5, 10, and 20 percent less accurate than human performance. Accuracy here is measured as a balance of precision (Did the system get only the correct items?) and recall (Did the system get all the correct items?). Performance in new domains such as biological entity extraction (e.g., genes and proteins), important for biological weapons intelligence, has already shown promising 80 percent accuracy for entity extraction after only two years of development in the National Science Foundation-supported BioCreative initiative.[135] Notably, entity and relation extraction rivals human performance in English and is advancing rapidly in some foreign languages (Chinese, Arabic).

---

134. Message Understanding Conference, Automated Content Extraction Program, Event99, and BioCreative

135. Hirschman, L., Yeh, A., Blaschke, C., and Valencia, A. 2005. *Overview of BioCreAtivE: critical assessment of information extraction for biology. BMC Bioinformatics* 2005, 6(Suppl 1):S1.



Source: Message Understanding Conference

Figure 7-20. Information Extraction Performance across Languages

Communication and Media Analysis using Machine Translation

Advances in statistical machine translation have increased accessibility to foreign documents, web sites, blogs, and even broadcast news. Government-funded community evaluations (such as trec.nist.gov) have accelerated development. Integration of emerging components has enabled new capabilities, such as content-based retrieval of foreign video and multilingual chat. For example, Figure 7-21 illustrates the integration of a broadcast news video indexing system (Virage Video Logger) together with a statistically trained commercial machine translation system (Language Weaver) to enable an end user to perform cross-language retrieval.

Figure 7-21. Retrieval and Translation of Arabic News Broadcast in Commercial

The example shows a user query of "Bin Laden," retrieval of a relevant Arabic news program, its speech transcription, and its translation into English. Related machine-translation technology is integrated with search engines to enable foreign web site browsing with instant messaging to enable multilingual chat (Figure 7-22). These capabilities can dramatically enhance both understanding of activities and interests in foreign media as well as enable direct one-on-one engagement with foreign audiences. While current methods can be employed if augmented by human linguists, further development in machine translation is required to enhance quality and expand applicability to lower density languages.

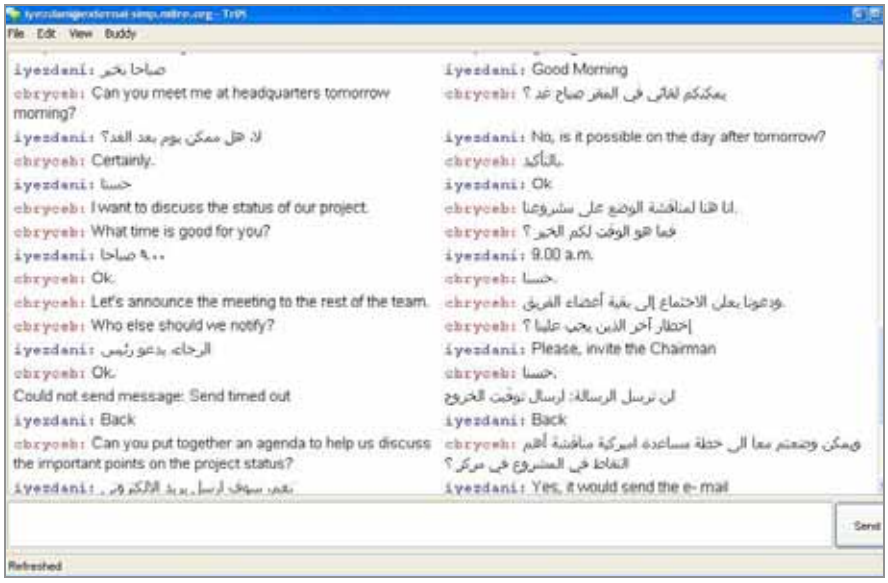
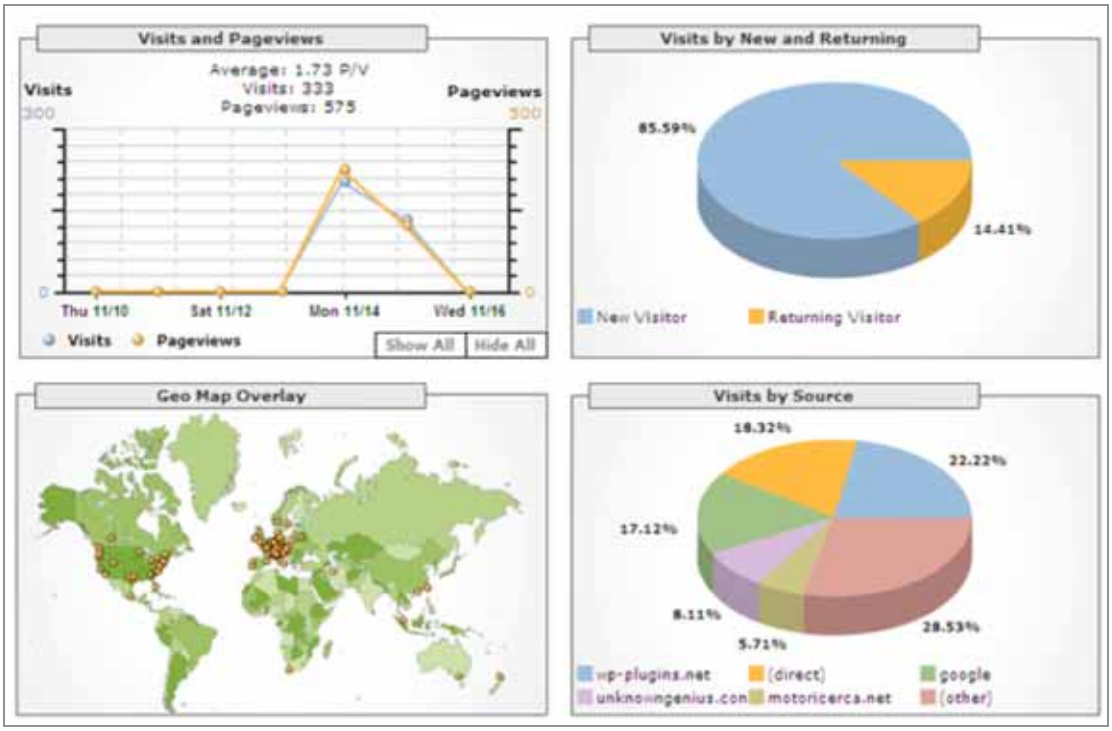


Figure 7-22. Translingual Instant Messaging (TrIM) between English and Arabic Speakers

Social Network/Influence Analysis

Tools such as Google's PageRank algorithm have successfully used analysis of links among web pages to automatically determine the popularity of a site. Simply put, PageRank considers a web page with more links to it ("inward links") as more significant than one with fewer links but also weighs links from more "important" pages more heavily. For individual web servers, tools such as Google Analytics (Figure 7-23) can enable web site managers to automatically compute usage statistics such as the volume of visits per page, the origin of searchers (by URL and geographically), if they were new or returning visitors, the number of pages viewed per visit, and the bounce rate. More generally, for larger sites, site ratings (Neilson's internet rating, Technorati, for example) can be employed to understand popular sites; however, more granular demographic data is needed (by age, economic status, religion).



Source: mycvs.org

Figure 7- 23. Google Analytics

As illustrated in the left side of Figure 7-24, information flows from ISI/Al-Qaeda to a forum to a news website to Al Jazerra TV. On the right hand side, data collected from alexa.com illustrates the geographical spread of visitors to the primary distribution sites for insurgent media (in this example, the largest number of visitors to most sites coming from Saudi Arabia and also Egypt and the Palestinian territories).

Just as it is possible to understand the importance of web pages (for both searching and assessing them) by exploiting their relationships, so too should it be possible to understand the importance of users by assessing their social influence. Researchers have already conducted significant research on social network analysis, such as information and communication flows and structures (email propagation is one example).[136] One technical opportunity that overcomes privacy concerns associated with social network analysis is to analyze public

136. Wasserman, S. and Faust, K. 1994. Social Network Analysis: Methods and Applications. Cambridge University Press.

communication fora (public blogs, listservs, text chat) in order to assess contributor frequency and communication networks—that is, who talks to whom. Further, with limited text analysis it is possible to assess which ideas or views are "picked up" by which users. Assessing how rapidly ideas spread from one user or site to another, and how broadly content is communicated can give a sense of their degree of "infectivity."

Source: Iraqi Insurgent Media: The War if Images and Ideas

Figure 7-24. Information Flow and Measurement[137]

Moreover, to the extent there is a shift in attitudes or behaviors, it is possible this could be reflected in the communication (someone expressing a change in their beliefs or promising or threatening to take some action) that might indicate the "affectivity" of the idea. It might be possible to measure the "virulence" of an idea, i.e., track "infections ideas" as a precursor to interdicting or influencing it. Developments in de-identification—i.e., removing proper names or individual identifying information from free text—promise to enable data mining while ensuring privacy.[138] Important open research questions include how individuals establish trust, form identity, and create groups in the digital domain.

Another important development on the web is the rapid expansion of social technologies. These include social networking (sites like mySpace, Facebook, LinkedIn) that enables individuals to create pages that link into friends and

137. Kimmage, D. and Ridolfo, K. 2007. *Iraqi Insurgent Media: The War of Images and Ideas*, Radio Free Europe/Radio Liberty regional analysts. Video briefing at http://www.newamerica.net/events/2007/iraqi_insurgent_media.
138. Gupta, D. Saul, M. and Gilbertson, J. 2004. *Evaluation of a Deidentification (De-Id) Software Engine to Share Pathology Reports and Clinical Documents for Research.* American Journal of Clinical Pathology. 2004 (121):176–186.

colleagues and share information. In addition, social bookmarking sites (such like del.icio.us, Flickr) enable users to bookmark and label their favorite sites and content which can then be shared with a larger community.

As might be expected, users exhibit social behavior in social media. For example, according to Gladwell, some participants take on special roles.[139] These include:

- *connectors* who are hubs in social networks
- *mavens* who are experts (such as bloggers who detect media misinformation)
- *salespeople* who persuasively influence others, often subconsciously

These individuals can wield disproportionate influence and cause "social epidemics," or sudden and often chaotic phase changes from one state to another (when a particular idea becomes viral). Finally, their contributions reflect the power law, i.e., contribution is an inverse log scale—few contribute most content; many contribute little. Figure 7-25 illustrates this long tail, power law in an example search on "Green Zone" at the photo-sharing site, Flickr. As illustrated by the graph to the right in the figure, of 482 images from 22 photographers of the Green Zone in Baghdad, 40 percent are provided by one individual, 18 percent of the contributors provide 80 percent of the content (the so called 80-20 rule), and 80 percent of the photographers provide less than 22 photos, the average per photographer. This Flickr example illustrates how a few productive or influential contributors dominate the information space.

139. Gladwell, M. 2000. *The Tipping Point: How Little Things Can Make a Big Difference*. Little Brown.

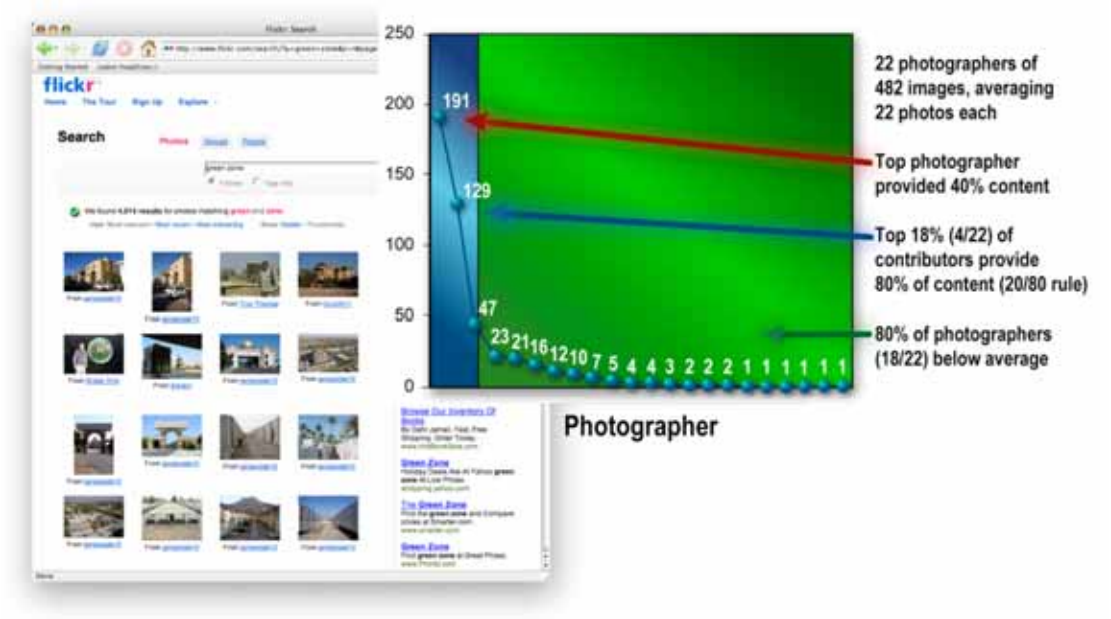


Figure 7-25. Power Law in Flickr Photo-Sharing Site

Automated Sentiment Analysis

Given the volume and importance of electronic information, distinguishing between opinions and facts[140]—or at least detecting the degree of an author's pro/con feelings toward a topic—is becoming increasingly important. Innovative approaches using language processing for sentiment detection and analysis promise scaleable and accurate measurement of positive (favorable) or negative (unfavorable) opinions in documents, websites, blogs, and chat.[141] Depending upon the source and purpose, effective sentiment analysis could require content segmentation, topic identification, information extraction, author identification, machine translation, and sentiment classification.

140. Cardie, C., Wiebe, J., Wilson, T., and Litman, D. 2003. "Combining Low-Level and Summary Representations of Opinions for Multiperspective Question Answering." In *AAAI Spring Symposium on New Directions in Question Answering,* pages 20–27.
141. Wilson, T., Hoffmann, P., Somasundaran, S., Kessler, J., Wiebe, J., Choi, Y., Cardie, C., Riloff, E., and Patwardhan, S. 2005. *OpinionFinder: A system for subjectivity analysis.* Proceedings of HLT/EMNLP 2005 Demonstration Abstracts, pages 34–35, Vancouver, October 2005.

Sentiment analysis is used for stock market analysis,[142] product reviews,[143] and analysis of multilingual political discourse.[144] In a test of opinions about an organization and pharmaceutical products, Nasukawa and Yi[145] demonstrated high precision (75–95%) in detecting sentiments in a half million web pages and a quarter million news articles, and believe these could be extended to billions of pages. These methods could provide the foundation for identifying issues of importance to an author or group, measuring their level of confidence, their agreeability/argumentativeness, and "extremeness" of their views. Important future areas of research include relating sentiment measures to identity, trust, and reverence.

Gaming

Computer games have become a multibillion-dollar industry. The Army has successfully used games for recruiting but has also found them to have unforeseen benefits in virtual basic training. Already insurgents have used games to engage and motivate youth to support Jihad. Given the availability of gaming engines as a foundation, these could have valuable strategic communication applications, including teaching English, skills for employment, and education of universal values.

Scientific Progress

While many of the above technologies can be beneficially applied today, additional research is required to advance the underlying theories and algorithms. For machine learning, data and annotated foreign language corpora for algorithm training are expensive but essential to accuracy improvements. Task-oriented evaluations, such as TREC (trec.nist.gov), have fostered community-wide progress. Simple, usable, and open solutions that focus on analytic/operational impact are essential. Finally, the nature of the strategic communication challenge will require multidisciplinary scientific teams, iterative and staged processes, and

---

142. Das, S. and Chen, M. 2001. *Yahoo! for Amazon: Sentiment Parsing from Small Talk on the Web.* August 5, 2001. EFA 2001 Barcelona Meetings.
143. Kushal, Dave, Lawrence, Steve, and Pennock, David M.. 2003. *Mining the Peanut Gallery: Opinion Extraction and Semantic Classification of Product Reviews. In WWW,* pages 519–528.
144. Mullen, T. and Malouf, R. 2006. *A Preliminary Investigation into Sentiment Analysis of Informal Political Discourse.* Proceedings of the AAAI Workshop on Analysis of Weblogs, 2006.
145. Nasukawa, T. and Yi, J. 2003. *Sentiment Analysis: Capturing Favorability Using Natural Language Processing.* International Conference On Knowledge Capture Proceedings of the 2nd International ACM Conference on Knowledge Capture. Sanibel Island, FL, 70–77.

rigorous application of the scientific method to ensure resultant capabilities that can effectively support mission requirements.

Conclusions

Advances in technology in the last two decades have led to a revolution in media, opening access to a seemingly infinite number of channels and introducing new models for the origins and flow of information.

Although technology has served as the enabler, much of the information ecology today is a social invention. The World Wide Web itself, as well as some of its most important constituents, like Wikipedia, eBay, Facebook, and YouTube, are social inventions. This invention continues at an incredible rate. YouTube, for example, went from nothing to 100 million daily videos in only a little over a year. Understanding and influencing this fast-evolving landscape is obviously a difficult matter. The pace of change may be greater than that of understanding.

With the rise of the Internet and satellite television, state censorship of content is becoming much less effective, and will ultimately become impossible. Technically it is quite difficult to control information access on the Internet. Even though some countries limit Internet connectivity through proxy servers that filter content, many users know how to circumvent these filters, and the information they access gets passed along in other ways.

With so many pathways that information can reach people, the emphasis today should be much less on the physical mechanism for delivery than it has been in the past. The problem now is crafting messages that inherently want to travel through this complex and variegated landscape.

Chapter 27. Engaging National Capability

In the fast-paced environment of real-time public and private communication, issue experts and casual observers alike are flooded with information and viewpoints. Gone are the days of limited access to the means of mass transmission of ideas as was common when governments and large private institutions were the only entities with sufficient finances to utilize mass media.

Message reach and clarity are now constrained primarily by imagination and tenacity, rather than access to communications technology or financial assets. As a result, the ability to astutely break through the cacophony of vantage points with a compelling rationale that motivates individual behavior becomes a supreme challenge for all who seek to influence future outcomes. In this complex environment, "actions" can become the most authentic "messages."

The United States has among its citizens some of the world's most accomplished experts in the skills requisite to develop and respond to strategic communication. Within the U.S. government there is also a long legacy of significant programming and communication outreach to foreign publics, with some of the most successful efforts originating in the early period of the Cold War.

Recent U.S. government strategic enhancements are attempting to address the changing communications environment. Following the release of the first *U.S. National Strategy for Public Diplomacy and Strategic Communication* in June 2007, each federal agency is now preparing its own strategic communication plan. When complete, these strategic plans will provide the groundwork for increased coordination and collaboration.

However, when compared to private and civil sector enterprises that have rapidly embraced the capabilities associated with integrated strategic communication, the U.S. government continues to have an underdeveloped strategic communication management process. This deficiency limits its ability to leverage the world-class capabilities of its citizens outside the federal government to contribute to its effort. It also makes a daunting task even more challenging since the U.S. government continues to depend on many strategic and organizational methodologies that originated in the pre-Internet, broadcasting-oriented world, further limiting its ability to collaborate to accomplish shared interagency and public/private goals.

Strategic Communication Originating in the United States has Many Sources

Many federal, state and local nongovernmental, corporate, and individual enterprises originating in the U.S. are involved in strategic communication with foreign audiences. While there is often a single enterprise performing the role of program leader, each program relies on many essential contributions from beyond the domain of its central team to accomplish its goals.

A snapshot of several of the programs sponsored by these enterprises shows the diversity of subject expertise and resource management necessary to conduct foreign outreach on behalf of U.S. interests. Also highlighted below are some of the existing and complex collaborations between public, private, and non-governmental organizations in the accomplishment of shared goals.

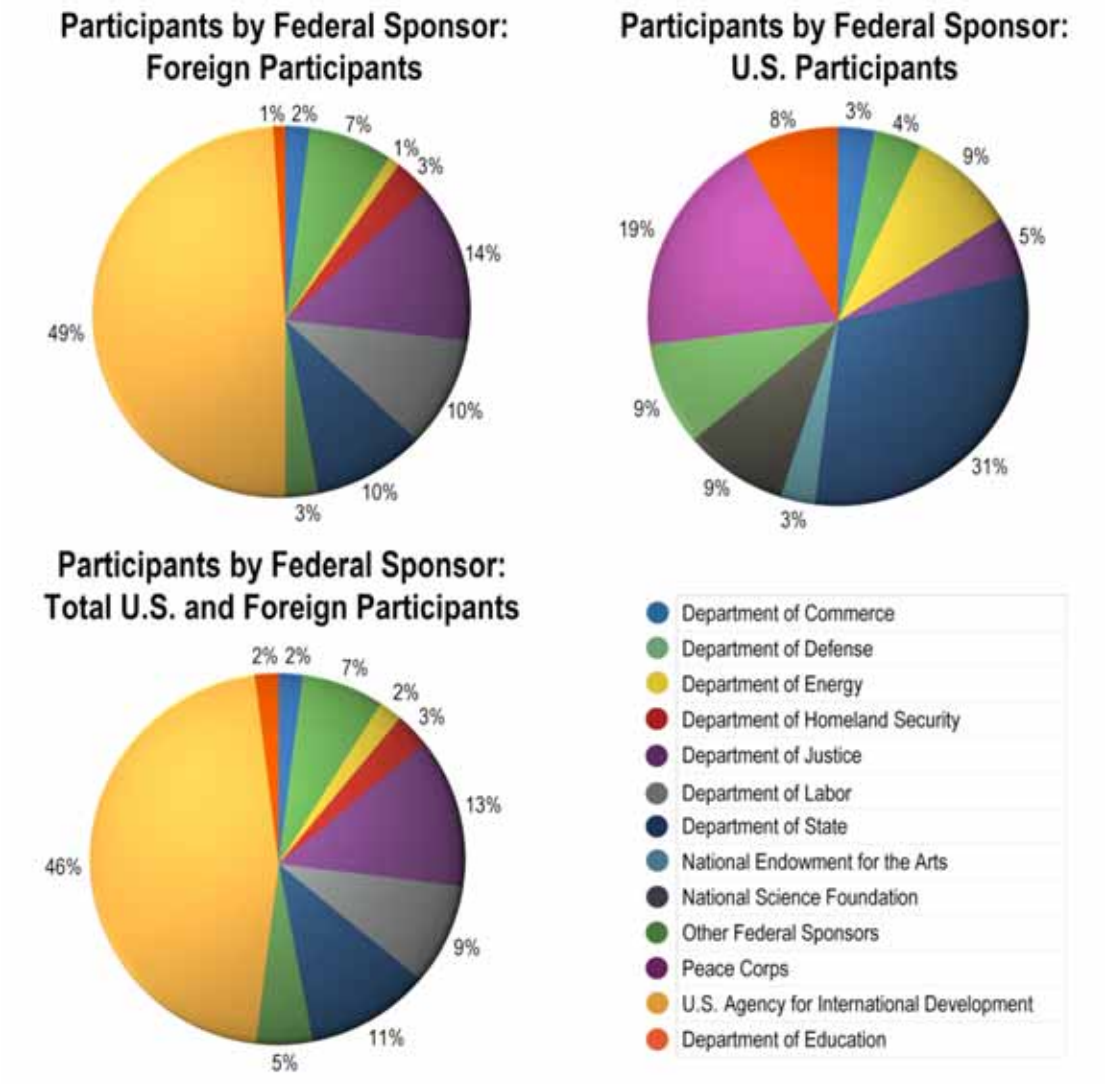
Federal: International Educational Exchange Programs

U.S. government-sponsored international exchange and training activities are defined in Congressional and Presidential mandates as the "movement of people between countries to promote the sharing of ideas, to develop skills, and to foster mutual understanding and cooperation, financed wholly or in part, directly or indirectly, with United States Government funds."[146]

During fiscal year 2005, 15 cabinet-level departments and 49 independent agencies and commissions reported management of 239 international exchange and training programs (Figure 7-26). Nearly 900,000 foreigners and U.S. citizens participated in these exchanges, ranging from academic exchanges for students, research exchanges for scholars, and professional skill development for mid-career professionals.[147] While over $1.2 billion in federal funds (63% of total) was expended to conduct these programs in fiscal year 2005, federal investment leveraged an additional $708 million (37% of total) from non-U.S. government sources (Figure 7-27)—including contributions from foreign governments, U.S. private sector, foreign private sector and international organizations.[148]

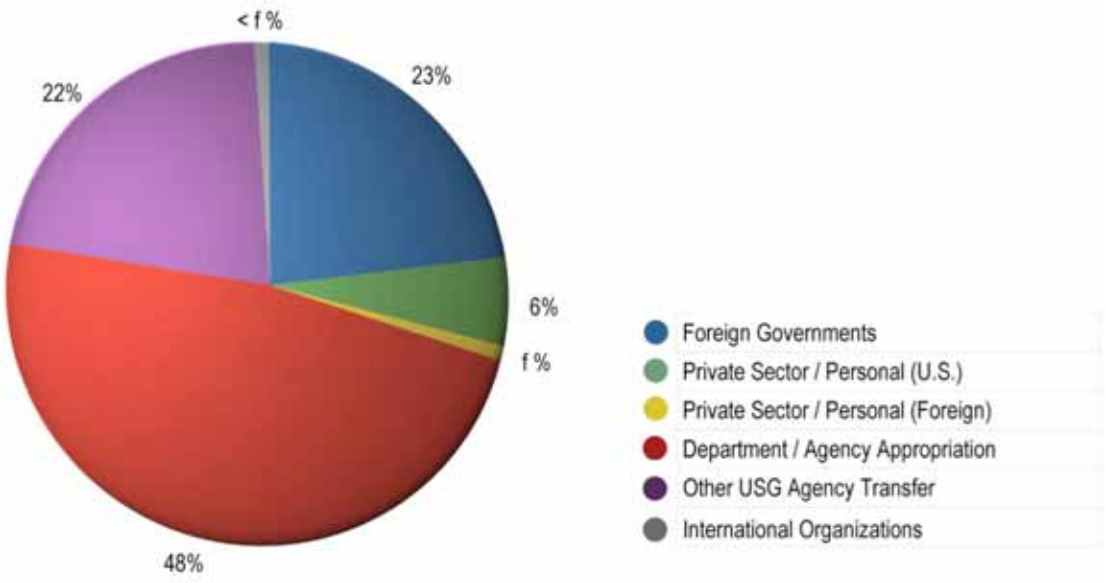
---

146. IAWG 2005 Report, see www.iawg.gov.
147. IAWG 2005 Report, "FY 2005 Participants by Federal Sponsor: Total U.S. & Foreign" p. 14, see http://www.iawg.gov/rawmedia_repository/039262c1_618a_400f_bade_4716fe743ae4
148. Interagency Working Group on U.S. Government-Sponsored International Exchanges and Training (IAWG) FY 2005 Inventory of Programs.



Source: IAWG

Figure 7-26. Fiscal Year 2005 Participants by Federal Sponsor



Source: IAWG

Figure 7-27. Fiscal Year 2005 Sources of Funding

This funding split is the result of a long-term successful international public/private partnership as well as federal interagency collaboration. While visas are coordinated through the Department of State, Bureau of Educational and Cultural Affairs, U.S. government personnel in each agency are responsible for developing, implementing and evaluating the programs, and often work through public/private partnerships with the private sector and non-governmental organizations to administer the programs.[149]

Federal: Broadcasting Board of Governors

Over 155 million people are reached each week through the international broadcasting services of the Broadcasting Board of Governors (BBG). Tracing its roots back to the creation of the U.S. Information Agency in the early 1950s, today the BBG is the sole independent federal agency that oversees all U.S. government and government–sponsored, non-military, international broadcasting. The BBG seeks to provide a strong, independent media where one does not exist. The following six broadcast units comprise the BBG:

149. IAWG 2005 Report, "FY 2005 Participants by Federal Sponsor: Total U.S. & Foreign" p. 15.

Voice of America (VOA) broadcasts on radio, television, the Internet, VOAMobile for Internet-enabled devices, Real Simple Syndication feeds, and podcasts in over 45 languages and provides news updates over VOA Internet.

Alhurra provides Arabic-language news and information to 22 countries in the Middle East.

Radio Sawa combines a mix of Western and Arabic pop music with news and information with a 24/7 Arabic-language network to reach youth in various regions of the Middle East.

Radio Free Europe/Radio Liberty (RFE/RL), offering more than 1,000 hours of programming from the Arctic Sea to the Persian Gulf in 28 languages, is streamed live and on-demand over the Internet.

Radio Free Asia (RFA) broadcasts news, information and commentary in nine languages to China, Tibet, Burma, Vietnam, Laos, Cambodia, and North Korea.

Radio and TV Marti provide news, information, and other programming to the people of Cuba. Radio Marti broadcasts 162 hours weekly of news and information (mostly live). TV Marti broadcasts 168 hours weekly of news, information, and entertainment programming via satellite and 30 hours weekly via the airborne platform. Approximately 15 hours weekly of TV Marti broadcasts are original programming. Broadcasting units are assisted by the engineering, technical, and administrative capabilities of the **International Broadcasting Bureau.**

Connectivity is an essential element of the growing social media phenomenon. While the "one-to-many" model of communication has been primarily operative in large-scale information transfer in the past, the "many-to-many" model is spreading rapidly to challenge old communication hierarchies based on corporate and state leadership of the assets needed to transmit information. As individuals, especially in younger populations, increasingly choose to acquire and forward information online, BBG has developed VOA Internet to reach this tech-enabled audience. Looking ahead, the U.S. government will need to assess whether the historic funding allocation of BBG toward broadcasting as its primary means of

message transfer should be maintained or reallocated in recognition of emerging media vehicles and audience dynamics.

State and Local: Sister Cities International

Municipal partnerships between U.S. cities, counties, and states, and similar jurisdictions in other nations provide opportunities for civic leaders and citizens to experience and explore other cultures, and to build economic ties.

Launched in 1956 following a White House summit in which President Eisenhower called for new people-to-people exchanges to enhance citizen diplomacy and cross-cultural friendship, **Sister Cities International**[150] was created to promote peace through mutual respect, understanding, and cooperation. It is a global citizen diplomacy network, originating from the town square.

Sister City International programs involve community-based efforts that draw on the skills of local government, business, and the private voluntary sector, including civil society nonprofit organizations and citizen volunteers. Areas of focus include sustainable development, youth and education, arts and culture, humanitarian assistance, and economic growth programs.

There are currently 694 Sister Cities International communities in the United States, with at least one in all 50 states, the District of Columbia, and five U.S. territories. These cities are partnered with 1,749 international communities in 134 countries. While Europe has 35 percent of all sister city relationships with the United States (an artifact of the program's origination during a period of heightened reconstruction of post World War II Europe), communities in Africa, Latin America, Asia/Oceania, the Caribbean, Eurasia, the Middle East, and Canada, are also partnered with U.S. communities.

150. See www.sister-cities.org.

Private Sector: Global Corporate Citizenship and Corporate Social Responsibility

Expressions and images associated with the United States reach across the globe. Many U.S. brands and cultural icons are widely appreciated around the world. It is not unusual for crowds of individuals who are protesting U.S. government policies overseas to be wearing apparel emblazoned with U.S. commercial logos, evidence of the frequent dichotomy that exists between the viewpoints on the U.S. government as distinguished from American culture.

In recent years, there has been phenomenal growth in the number and scope of community engagement efforts by the private sector, both in the United States and abroad. Public/private partnerships increasingly offer a means for partners to achieve common goals that are beyond the scope of their individual abilities but achievable through shared effort. Employee volunteer programs have become an important aspect of community outreach as well.

More U.S. corporations are acknowledging global responsibility to their customers, partners, employees, and shareholders as well as to the communities in which they do business. Global Corporate Citizenship and Corporate Social Responsibility are receiving increased attention as being important future indicators of corporate performance.

The United Nations Global Compact,[151] the world's leading voluntary corporate citizenship initiative, both builds on and encourages this trend as do investment analysts who are increasingly taking notice.

Campus programs such as Net Impact[152], provide training and capacity building to the next generation of business leaders interested in corporate social responsibility, sustainable enterprise, and social entrepreneurship.

151. See www.unglobalcompact.org.
152. See www.netimpact.org.

Nongovernmental and Civil Society Organizations

Nongovernmental organizations (NGOs) are generally any non-profit organizations that are independent from government. NGOs generally seek to mobilize support and voluntary contributions to impact social, economic, and political activities in communities. Voluntarism and altruism are important characteristics.

While NGOs often work in areas underserved by government aid, many receive a significant percentage of their operating income from government sources when they work together in partnership to achieve shared goals. Other NGOs seek to achieve change by exerting outside influence on the political system.

The nature and capabilities of NGOs varies widely. They range from global organizations with a large headquarters staff supported by thousands of volunteers, to mega philanthropies underwritten by wealthy individuals, to small, community-based self-help groups launched and boot-strapped through the inspiration of one social entrepreneur.

Reflecting the diversity of their programming and outreach activities, definitions across the NGO sector vary. For example, the World Bank classifies NGOs into three main groups: international organizations that implement operations in more than one country, national organizations that work in one country, and community-based membership organizations that work exclusively at the grass-roots. Alternatively, the Organization of American States refers to NGOs as civil society organizations.

Individuals: Both Nodes and Hubs in the Net-centric World

In the increasingly net-centric environment of daily life, individuals around the globe are empowered to build "communities of interest" based on new forms of idea championship that both challenge and support nation state interests. Among those individuals with direct personal access to new communication vehicles, there will continue to evolve new methods of combining the physical world with the digital world.

Net-centricity allows individuals empowered by technology to simultaneously become consumers, replicators, and disseminators of information on a massive scale. Around these "hub individuals" grow "communities of interest."

Since the most powerful information in both the physical and virtual world is transmitted by a trusted source, communications forwarded across wide networks by "hub individuals" become strategic issues for diplomatic, economic, and security planners.

Community-Building through Information Affluence

The power of ideas creates information affluence. Information can also bring individuals together. Three examples of community building through use of communication technology and techniques include First Voice International, One Laptop Per Child, and Sesame Workshop.

First Voice International Delivers Life-Saving Information to Isolated Areas

First Voice International (FVI) is a nonprofit organization with exclusive access to five percent of the WorldSpace Satellite Network and communication capacity through an expanding number of affiliated community radio stations.[153] Working through partnerships with international organizations, government agencies, and community groups, FVI provides locally relevant, and often locally produced, information to audiences with the greatest need who are living in both the urban and the most isolated areas of Africa, Asia-Pacific, and the Middle East.

FVI content emphasizes issues such as HIV/AIDS, reproductive health, good governance, natural resource management, and disaster relief. Through the approach of "one receiver, many ears," listening groups in remote areas receive the signal directly from a shared satellite radio receiver that can be purchased for as little as $68 wholesale (compared to a conventional satellite dish that can cost over $1,000). In urban areas and their surrounding communities, FVI reaches many more people through 190 community radio partners in 24 countries in Africa and Asia. While some station operators broadcast the content stream live over their AM and FM transmitters, others record it for rebroadcast or translate the programs into local languages before broadcasting.

Through its First Voice Multimedia Service, FVI enables transmission of high volumes of web-based text and multimedia material to teachers, health care providers, local government officials, and humanitarian organizations working in

153. See www.firstvoiceint.org.

areas of Africa and Asia where Internet access is unavailable, unreliable, or very expensive. This transmission is accomplished through the data ports on the FVI-enabled satellite radios that can be connected to a personal computer through adapter cards. FVI supports this technical capability with community capacity building training in the use and maintenance of the radio and multimedia equipment. It has further expanded the reach of its grassroots network by providing Community Information Centers in extremely isolated communities with computers equipped with multimedia service.

One Laptop Per Child Embraces the Collaborative Spirit of the Network

In the developing world, one in three children do not complete the third grade and most receive little, if any, formal education. This lack of education has both personal and societal consequences for them, the societies in which they live, and the world community. Without access to education and the tools to expand their personal horizons, these children are faced with the prospect of growing into adults with limited opportunity to escape poverty. Few are able to visualize a different life for themselves beyond what they observe first-hand in the lives of their parents and neighbors. With an undereducated workforce, their communities cannot be challenged to compete economically in the increasingly global information economy and their governments are not likely to be able to provide services to large populations that are not self-supporting.

One Laptop Per Child[154] seeks to provide children in developing countries with new opportunities to explore, experiment, and express themselves. It is based on the premise that children have innate capacities to learn, share, and create on their own. The mission of One Laptop Per Child is to ensure that all school-aged children in the developing

154. See www.laptop.org

world are able to engage effectively with their own personal laptop, networked to the world, so that they, their families, and their communities can openly learn. One Laptop per Child focuses on designing and manufacturing laptops. It works with national government agencies (Ministry of Education) that are responsible for the distribution of the laptops and for training teachers on their use. One Laptop per Child will also initiate a short-term "give 1 get 1" program in North America in November 2007.

The XO laptop is designed specifically for children in remote and impoverished geographies to help them "learn learning" and includes a web browser, rich media player, and e-book reader. By using the XO to access and explore information, these children will be exposed to the full range of human knowledge and use it to develop their potential to contribute to their families, neighborhoods, and nations.

Sesame Workshop International Creates Educational Television Around the World

A ground-breaking American educational children's television series when it first aired in the United States in 1969, *Sesame Street* has become one of the longest-running U.S. television shows in history. Produced by the nonprofit organization **Sesame Workshop**[155], its distinctive format of live action, animation, and colorful characters combines both education and entertainment for preschoolers. In addition to letter and word recognition and mathematics, instructional goals have included basic life and social skills, delivered through a world of humor and fun. It has received more Emmy Awards than any other television series. Over the last 35 years, *Sesame Street* has also become one of the world's most highly regarded educational programs for children. The original series has aired in 120 countries and millions of children and their parents around the world have watched the programs.

Beginning 1972, *Sesame Street* international co-productions were developed to reach diverse international audiences. New York-based producers from Sesame Workshop work with child development experts, directors, producers, and writers in each country to connect the magic and fun of *Sesame Street* with specific local

155. See www.sesameworkshop.org

language and cultural needs. This collaborative effort has resulted in customized *Sesame Street* broadcasts in Bangladesh, Brazil, Canada, China, Egypt, France, Germany, India, Indonesia, Ireland, Israel, Italy, Japan, Jordan, Kosovo, Kuwait, Mexico, Netherlands, Northern Ireland, Norway, Palestine, Philippines, Poland, Portugal, Russia, South Africa, Spain, Sweden, Turkey, and the United Kingdom.

Personal Interactions as Compelling Messages

The U.S. government and civil society have a long track record of positive actions and outreach toward communities across the globe. A snapshot of a few key programs includes the Fulbright Program, academic study abroad, the U.S. Agency for International Development, Peace Corps, public/private partnerships and inter-agency collaborations, and military-to-military exchanges.

Fulbright Program is the Flagship International Exchange Program of the United States

Since its creation under legislation introduced by then Senator J. William Fulbright in 1946, the Fulbright Program[156] has sought to "increase mutual understanding between the people of the United States and the people of other countries." Over 279,000 Fulbright scholars and professional experts (105,400 from the U.S. and 174,000 from other countries) have participated in educational and cultural exchange programs over the last 50 years. The 35th Fulbright alumnus to be awarded a Nobel Prize was Muhammad Yunus, Founder and Managing Director of Grameen Bank in Bangladesh, who was honored in 2006 for pioneering the practice of microcredit and microenterprise that creates opportunities for those living in extreme poverty.

There are Fulbright grant programs for three audiences: students, scholars and professionals, and teachers and administrators:

- The **Fulbright U.S. Student Program** offers fellowships for U.S. graduating seniors, graduate students, young professionals, and artists to study abroad. During the 2006–2007 academic year more than 1,200 Americans studied in over 140 countries through the full or partial support of this program.

156. www.exchanges.state.gov/education/fulbright/.

- The **Fulbright English Teaching Assistantships Program** facilitates the English language abilities and knowledge of the United States among foreign students by placing American scholars and teachers near capital cities in over 20 countries.

- The **Fulbright U.S. Scholar Program** supports the research and lecture programs in over 130 countries by approximately 1,100 American scholars and professionals in such diverse fields as agriculture, business, journalism, public health and technology.

- The **Fulbright Senior Specialists Program** is a short-term grant for a period of 2–6 weeks, designed to enhance collaboration with professional counterparts at non-U.S. institutions of higher learning.

- The **Fulbright Teacher and Administrator Exchange Program** primarily facilitates one-on-one exchanges between American administrators in K-12 schools, community colleges, and four-year institutions and their counterparts in more than 30 countries worldwide.

While the primary source of funding for the Fulbright programs is Congressional appropriation ($184.6 million in fiscal year 2006), participating governments and host institutions also contribute financially through cost sharing and indirect support. Other important elements of program administration are the nonprofit binational **Fulbright Commissions and Foundations** that oversee the Fulbright program abroad and propose the annual programs. Over 65 **Fulbright Alumni** associations operate as private, nonprofit organizations to facilitate relationships among former grantees and the U.S. Fulbright associations also provides hospitality and outreach for visiting Fulbright students, scholars, and teachers during their stays in the United States.

Foreign Student Study in the United States Expands Perspective

In fiscal year 2007, the United States issued a record number of 591,000 student visas for international students to come to the United States to study, reversing a period of decline following September 11, 2001.[157] According to Under Secretary of State Karen Hughes, "we are actively partnering with

157. U/S Hughes 11 July 2007 DOD Conference on Strategic Communication.

America's higher education community to send a clear message that we want the future leaders of the world to come here to study and get to know us."[158]

USAID Provides Economic and Humanitarian Assistance in more than 100 Countries

At its creation in 1961, the **U.S. Agency for International Development (USAID)**[159] combined existing government agencies to become the first U.S. foreign assistance organization whose primary emphasis was long-range economic and social development assistance efforts on a country-by-country basis.

Headquartered in Washington, D.C., USAID has field offices in many regions of the world. It works to improve the lives of millions in more than 100 developing countries through technical assistance and capacity building, training and scholarships, food aid and disaster relief, infrastructure construction, small-enterprise loans, and credit guarantees. Through this foreign assistance, USAID seeks to further U.S. foreign policy interests by working to expand democracy and free markets while improving the lives of people in the developing world.

USAID has working relationships with more than 3,500 American companies and over 300 U.S.-based private voluntary organizations. The Office of Private and Voluntary Cooperation "provides direct support to efforts made by the U.S. Private Voluntary Organization community and by its partner nongovernmental organizations to address critical needs in developing countries and emerging democracies."[160]

Since January 2006, the USAID administrator has also served as the Director of U.S. Foreign Assistance with authority over all Department of State and USAID foreign assistance funding and programs charter to ensure that U.S. foreign assistance is used as effectively as possible.

---

158. U/S Hughes 11 July 2007 DOD Conference on Strategic Communication.
159. See www.usaid.gov
160 Ibid.

Peace Corps

The **Peace Corps**[161] was established by President John F. Kennedy in 1961 to promote world peace and understanding. Its goals continue to be to help the people of interested countries meet their needs for trained men and women, to promote a better understanding of Americans on the part of the peoples served, and to promote a better understanding of other peoples on the part of Americans. Over 187,000 Peace Corps volunteers have lived and worked at the invitation of 139 host countries in the 46 years of the program's existence.

Peace Corps volunteers must be U.S. citizens and at least 18 years of age. Peace Corps service is a 27-month commitment. Today there are 7,749 volunteers working in many activity areas, including education, youth outreach and community development; business development; agriculture and environment; health and HIV/AIDS; and information technology. Specific duties and responsibilities vary widely and generally involve collaboration with local community members and nongovernmental organizations in the host countries.

In September 2007, the Peace Corps launched a website (www.peacecorps.gov/minisite/50plus/) as part of a larger initiative aimed at attracting potential Peace Corps volunteers over the age of 50. Only 5 percent of current Peace Corps volunteers are age 50 or older, yet this demographic cohort of the American population is seen as having significant professional and life experience as well as an interest in finding meaningful and rewarding opportunities for service that fits with the Peace Corps mission and goals.

Life Saving Outreach through U.S. Government Interagency and Public/Private Partnerships

The USNS *Comfort,* hospital ship conducted a four-month humanitarian mission to 12 Central American, South American and Caribbean nations during the summer of 2007. The primary objective was to address regional health service support requirements ashore, and promote clinical information

161. See www.peacecorps.gov

sharing across the region. Other missions included outpatient shipboard health service support and minor construction projects in the host country.

The USNS *Comfort* mission was coordinated with partner nations in the region, including Belize, Colombia, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Nicaragua, Panama, Peru, Suriname, and Trinidad and Tobago, to provide free outpatient health care services to communities in need. Planning, coordination, and implementation included representatives from several U.S. government departments and agencies, such as Department of State, Department of Defense, U.S. Navy, U.S. Air Force, U.S. Coast Guard, Department of Health and Human Services, and U.S. Public Health Service as well as volunteers from nongovernmental organizations such as Operation HOPE,[162] Operation Smile,[163] and Atlanta Rotary Club.

The embarked medical crew of more than 500 doctors, nurses, and healthcare professionals brought a wide range of capabilities, including medical, dental, nursing, pharmacy, veterinarian, engineering, and environmental health services. These U.S. federal government and U.S. nongovernmental organization professionals were trained and equipped to provide general outpatient surgery, ophthalmology surgery, basic medical evaluation and treatment, preventative medicine treatment, dental screenings and treatment, optometry screenings, eyewear distribution, public health training, and veterinary services.

As of early September 2007, more than 76,000 patients had been seen. Since so many patients need to be treated for more than one medical condition, this resulted in a total of 295,817 patient encounters.

Military-to-Military Exchanges

The DOD conducts International Military Education and Training (IMET) to:

- encourage mutually beneficial and increased understanding between the United States and foreign countries, improve the ability of participating foreign countries to achieve greater self-reliance by effectively utilizing their resources (including defense articles and services obtained from the United States),

162. See www.projhope.org
163. See www.operationsmile.org

- increase awareness of the national publics of countries participating in this training of issues related to internationally-recognized human rights

DOD also operates Regional Centers for Security Studies, such as the Marshall Center and the Asia Pacific Center. During 2007, military-to-military exchanges included 2,300 IMET participants and 1,900 Department of Defense Regional Center participants.

Organizing the U.S. Government for Integrated Strategic Communication

Rapid response to emerging situations is a demanding discipline requiring dedication of time, attention, and resources. Necessarily, the concept development, experimentation, and identification of new audiences and new vehicles all take a back seat to short-term exigencies.

As a result of current federal funding and resource allocation levels, U.S. government strategic communication teams are limited in their ability to explore mid-range and long-range strategic communication strategies and initiatives. Nor do they have time to formalize lessons learned for use by other U.S. government teams working on similar issues, or consistently pool social and cultural information across departments and agencies as a shared resource for future use. Pockets of exceptional U.S. government expertise are interwoven with shared blind spots.

The PCC on Public Diplomacy and Strategic Communication, the Interagency Crisis Communication Team, and the Counterterrorism Communications Center all have evolved to enhance interagency coordination. However, there is currently no formal, centralized conduit for strategic communication exchange. Only a central repository for foreign public opinion data is contemplated by the *U.S. National Strategy for Public Diplomacy and Strategic Communication.*

Without diminishing the ability of the U.S. government to manage more immediate challenges, improvements in four areas would facilitate the ability of the government to achieve integrated strategic communication as called for in the *U.S. National Strategy for Public Diplomacy and Strategic Communication*:

1. know what the U.S. government knows
2. increase social and cultural understanding
3. collaborate with outside partners and experts
4. facilitate U.S. government strategic communication integration

Know What the U.S. Government Knows

The opportunity to methodically build upon the knowledge base and lessons learned of past and current U.S. government strategic communication efforts across country teams, departments, and agencies is currently constrained by time-sensitive demands, current staffing, and funding levels.

Currently, when a department or agency faces a strategic communication informational need or skill set beyond the ability of its staff it will often contract individually with an outside supplier, not knowing that related data or skill sets already exist or are being simultaneously pursued elsewhere in the U.S. government. Not only is this wasteful in terms of time and assets, but it greatly reduces, if not eliminates, the opportunity to both build upon lessons learned elsewhere and to combine resources in a superior joint effort.

Such government-wide situational awareness is limited by the lack of a central clearinghouse for information, lessons learned, and professional resources related to U.S. government strategic communication. The lack of such a clearinghouse makes it challenging and time-consuming for any individual strategic communication team to know what other U.S. government and industry experts know and to leverage that knowledge in a time-sensitive environment to the advantage of the nation. It also reduces the ability for coordinated interagency and public/private partnerships to face shared challenges.

Similar needs for collaborative information flow and dissemination have resulted in the development of data fusion centers, such as the Counterterrorism Communications Center at the Department of State and the NCTC at the Directorate of National Intelligence. NCTC also hosts a repository, NCTC Online, that serves as a library of information across the full range of intelligence, law enforcement, military, homeland security, and other federal organizations working on associated national security issues.

Increase Social and Cultural Understanding

The complexity of the challenges associated with strategic communication is increasing. Dramatic changes in information technology and media interface have enabled communities of interest to proactively use the mediasphere.

As a result of the advent of global internet connectivity with low barriers to participation, the prior communication model is transitioning from “top-down and one-to-many” to “bottom-up and many-to-many” in which one individual or small groups can truly shape opinion through their words and actions.

In light of the complexity associated with the successful management of U.S. government strategic communication today and in the future, many managers currently responsible for strategic communication have been working to develop comprehensive planning tools. In December 2006, the *Army and Marine Corps Counterinsurgency Field Manual* (FM3-24/MCMP3-33.5) highlighted the importance of deep cultural understanding. In June 2007 the *U.S. National Strategy for Public Diplomacy and Strategic Communication* called for a central repository of information and analysis of public opinion in different countries. Both of these documents highlighted the need for greater interagency exchange within the U.S. government and collaboration with external partners.

Collaborate with Outside Partners and Experts

The United States has an exceptional range and depth of expertise among its corporations, universities, nongovernmental organizations, and citizens. Many are world-class practitioners of Strategic Communication or have skills that are essential to its successful implementation in various cultural contexts. Others have long established track records of successful programmatic implementation on their own initiative or in partnership with USG. Their contributions to future USG efforts could both complement and supplement the capacities and resources of current USG staffs.

Partnering with the U.S. government to achieve shared goals can be a challenging bureaucratic process. Both USAID and the Department of State have created offices to facilitate the process.

USAID maintains a registry of U.S. private and voluntary organizations seeking to work with USAID. Through a competitive grant program administered by its Office of Private and Voluntary Cooperation, USAID provides direct support to efforts made by the U.S. private and voluntary organization community and by its partner nongovernmental organizations to address critical needs in developing countries and emerging democracies. Non-profit organizations based outside the United States work directly with USAID missions.

In 2006, the Office of Private Sector Outreach was established at the Department of State to facilitate partnerships between the U.S. government and companies, universities, foundations, and nongovernmental organizations. However, on an individual expert level, the U.S. government is not organized or resourced to readily identify, mobilize, and fund significant collaboration with outside individuals who possess expertise relevant to advancing U.S. government strategic communication objectives. This is a time-consuming process requiring a

depth of industry contacts that strategic communication practitioners cannot be expected to have the time to maintain or expand.

Listed here are just a few of the professional skill sets present in the U.S. population that have direct relevance to strategic communication:

- **Communications technologists** can provide insight toward methodologies that maximize utility of existing communication modalities as well as identify emerging technical capabilities.
- **Behavioral scientists and cultural anthropologists** provide deep understanding of human cultures, identities, attitudes and behaviors.
- **Educators** with knowledge of culturally relevant pedagogies offer valuable perspectives.
- **Historians** are versed in cultural perspectives and can act as interpreters of current and future events.
- **Economists** provide data models to understand and forecast financial events.
- **Religious** scholars and leaders offer insight into important dimensions of cultural life.
- **Linguists and translators** develop cultural sensitivities that are of great value in the selection of key words, messages and communication formats that resonate with intended audiences.
- **Political scientists** provide insights into power and influence in modern societies.
- **Librarians and researchers** provide expert information access and data management skills, have country- and culture-specific knowledge, contacts, and capabilities, and a proven track records of mission success.
- **Corporate business managers and entrepreneurs** have country and regional cultural experience, as well as ongoing relationships with international audiences, government leaders, and nongovernmental voluntary organizations.
- **Marketing managers** of products and services are accustomed to leading the complex and interdisciplinary management process associated with building and maintaining brand equity.

- **Market researchers** who advise U.S. global brand management teams have developed a wide range of measurement techniques to research and monitor international consumer interests, attitudes and preferences.
- **Advertising copywriters, art directors, and media planners** have proven abilities to transform copy and media strategies into compelling messages, events and programs as well as identify media vehicles that attract target audiences.
- **Producers and directors** of films, television programming, radio, video games, and advertising commercials are expert in crafting compelling and persuasive storylines and images.
- **Artists, authors, and musicians** live lives of demonstrated creativity that transcends national boundaries, and their personal stories and bodies of work offer windows into the American population.
- **Retired government officials** can provide historical perspective as well as program continuity.

Facilitate U.S. Government Strategic Communication Integration

As mandated in June 2007 by the *U.S. National Strategy for Public Diplomacy and Strategic Communication*, all U.S. government departments, agencies, and embassies are required to develop an agency-specific plan to implement the public diplomacy/strategic communication objectives of the national strategy.

This requirement represents an important step forward in the integration of strategic communication across the U.S. government. However, without the time to build leadership and staff awareness of the "best practices" and "tactics, techniques, and procedures" in the private sector and social sector with relevance to integrating strategic communication across the U.S. government, the forthcoming plans are likely to reflect existing programs and trends. U.S. government strategic communication would benefit from shared access to lessons learned and knowledge of outside sources of expertise.

With the recognition of the importance of integrated strategic communication in the *U.S. National Strategy for Public Diplomacy and Strategic Communication* and its contribution to successful achievement of the national security strategy, it becomes important to provide additional support to these interagency and intra-agency efforts.

Chapter 28. Conclusions and Recommendations

In light of the changing world and the significant impact new technology and media are having on information flow, effective, comprehensive, and coordinated strategic communication is vital to U.S. national security. Since the DSB last reported on this issue in 2004, positive changes were implemented in the DOD and Department of State. However, when compared to the private sector and civil sector enterprises, which have rapidly embraced the capabilities associated with integrated strategic communication, the U.S. government continues to have an underdeveloped strategic communication management process. As a result, much remains to be done to achieve an effective strategic communication approach, infrastructure, and operation.

In order to increase the effectiveness of the U.S. government strategic communication enterprise, this study makes seven recommendations:

1. Create a Center for Global Engagement.
2. Consolidate the nation's strategic communication leadership.
3. Investment in critical information science and technology (S&T) opportunities.
4. Significantly increase Department of State budget for public diplomacy and exchanges.
5. Review the Broadcasting Board of Governors missions, structure, funding, and performance.
6. Significantly increase DOD budget for strategic communication.
7. Take immediate actions that leverage existing budgets and programs to achieve near and medium term benefits.

Center for Global Engagement

In seeking ways to enhance government-private sector collaboration in support of strategic communication, the study examined roles, functions, and organizational structures. We concluded that direction, planning, coordination, and programmatic implementation is a government responsibility requiring

change at the White House and National Security Council (NSC) level. Further, America's interests would be well-served by creating a Congressionally mandated independent, non-profit, non-partisan Center for Global Engagement (CGE).

The center should be a hybrid organization modeled on FFRDCs, such as the Rand Corporation and the National Endowment for Democracy. The center should be a tax-exempt private 501(c)(3) corporation. Its authority should enable it to provide services to government departments on a cost-recovery basis and contract with academic, commercial, and government and non-government organizations.

The NSC's Deputy National Security Advisor for Strategic Communication and the members of the Strategic Communication Policy Coordinating Committee should provide program and project direction to the center. The Center for Global Engagement should be governed by an independent nonpartisan board of directors that would include distinguished Americans drawn from relevant professions and members of Congress appointed on a bipartisan basis. The NSC's Deputy National Security Advisor for Strategic Communication should be an *ex officio* member of the board. The board of directors should appoint the center's director and ensure mission coherence and quality of performance.

The center should be guided by three purposes:

1. Provide information and analysis on a regular basis to civilian and military decision-makers on issues vital to U.S. national security, including global public opinion; the role of culture, values, and religion in shaping human behavior; media trends and influences on audiences; information technologies; the implications of all source intelligence assessments; and non-departmental, non-political advice that will sharpen their judgment and provide a basis for informed choices.
2. Develop mandated and self-initiated plans, themes, products, and programs for the creation and implementation of U.S. communications strategies that embrace diplomatic opportunities and respond to national security threats.
3. Support government strategic communications through services provided on a cost recovery basis that mobilize non-governmental initiatives; foster cross-cultural exchanges of ideas, people, and information; maintain knowledge management systems, language and skills

inventories, and procedures to recruit private sector experts for short term assignments; and continually monitor and evaluate effectiveness.

The center would perform functions in six critical areas:

1. Perform audience polling and analysis including ethnographic, psychographic, demographic, behavioral and tracking research; hypothesis testing (focus groups); and other "listening" and assessment techniques used in political campaigns.
2. Perform cultural influence analysis including values, religion, entertainment, and education.
3. Analyze of media influences on audiences including content analysis, agendas, political/social tendencies, relevance and credibility, and media organization structure, ownership, and business models.
4. Foster cross-cultural exchanges of ideas, people, and information.
5. Work with the commercial and academic sectors for the development of a range of products and programs that communicate strategic themes and messages to appropriate target audiences. Broad themes and messages would include respect for human dignity and individual rights; individual education and economic opportunity; and personal freedom, safety, and mobility. Examples of products would be a children's TV series; video and interactive games; support for the distribution and production of selected foreign films; and web communications including BLOGs, chat rooms, and electronic journals. Programs might include training and exchanges of journalists, support for selected foreign television documentaries, maintenance of databases of third party validators and supporters for conferences, and the design and implementation of country and regional campaigns to support themes and messages and de-legitimize extremism and terrorism.
6. Continually monitor and evaluate effectiveness, efficiency, and message continuity to adapt themes, products, and programs as directed by the Chair of the Strategic Communications Policy Coordinating Committee and its members.

Program execution and operational implementation will continue to be a government responsibility.

The center should receive core funding that supports steady state operations through a new Congressional line item in the Department of State's annual appropriation. To initiate funding for the center, a new appropriation of $50 million should be included in fiscal year 2009. This core funding should grow to $150 million over a five-year period. The center's core funding would support basic operations (staff and administration), information and analysis (polling, media research, cultural studies), maintenance of databases and skills inventories, and self-initiated projects and programs.

The center would also develop additional funding for projects and programs provided through contracts and task orders from the Strategic Communication Policy Coordinating Committee's departments and agencies (e.g. DOD, AID). We estimate that the funds from other agencies and departments would be modest initially but would grow to about $100 million over five years as the CGE establishes its credibility. Total funding for the CGE is expected to exceed $250 million after five years.

The center's success will depend on its ability to serve as a central source of independent, objective expertise safeguarded from special pleadings of organizational interests. Structures and methods must:

- be agile, adaptable, and cutting edge
- are multi-disciplinary and fuse capabilities from a variety of sources
- respect past gains as they lay a strong foundation for the future

Regular critical feedback to key decision-makers based on polling and research, and longer-term independent analyses that help refocus and reassess policy and strategic communication initiatives, will be essential.

Therefore, we make the following recommendation:

RECOMMENDATION 1. THE CENTER FOR GLOBAL ENGAGEMENT

The President, Congressional leaders, and interested organizations outside government collaborate to create an independent, non-profit, and non-partisan Center for Global Engagement.

Three principles should guide the establishment and work of the center. First, that the direction, planning, and execution of the government's strategic communication instrument are government responsibilities. Second, government cannot succeed in carrying out its responsibilities without sustained, innovative, and high quality support from civil society. Third, the academic, research, business, and non-profit communities offer deep reservoirs of untapped knowledge, skills, credibility, and agility needed to strengthen strategic communication.

The Center for Global Engagement should be a:

- 501(c)(3) corporation with an independent director and board of directors
- means to motivate and attract civil society's best and brightest
- hub for innovation in cultural understanding, technology, and media
- repository of expertise
- magnet for innovative ideas
- means to institutionalize continuity and long-term memory
- focus for experimentation and project development

In addition to establishing the center, Congress needs to provide the Department of State with $500,000 to develop a charter that will define the mission, structure, and operations of the CGE. The department should award these funds through a competitive grant to an organization or group of organizations that will prepare and execute a business plan leading to the creation of the CGE as an independent corporate entity (one option could be to extend the mission of an existing FFRDC or 501(c)3 corporation).

Thereafter, Congress should provide sustained funding for the CGE through a line item in the Department of State's budget. This should be new money appropriated to the department. Congress should provide the CGE with an initial appropriation of $50 million in fiscal year 2009. The objective should be steady funding growth, consistent with performance and use by multiple government agencies, to $250 million during the first five years.

The CGE should:

- respond to multi-agency government taskings, coordinated through a National Security Council Deputies Committee for Strategic Communication

- provide deep understanding of cultures and cultural dynamics, core values of other societies, and media and technology trends
- provide core data, best practices, and an opinion research clearing house in support of government sponsored strategic communication programs
- assess the effectiveness of national strategic communication activities and programs
- collaborate with independent organizations that promote universal values, cultural understanding, and global engagement
- maintain a repository of strategic communication talent, skills, and capabilities
- attract fellows from the academic, non-profit, and business communities and from government

Strategic Communication Leadership

To ensure that gains made in the planning and conduct of the nation's strategic communication are maintained and built upon, it is crucial that the U.S. consolidate strategic communication leadership. We recommend that the NSC establish and coordinate a Deputies Committee for Strategic Communication. We also recommend that the position of Deputy National Security Advisor and Assistant to the President for Strategic Communication (DNA/SC) be established to provide a direct link between the leadership of strategic communication and the President.

We also recommend that the current position of Under Secretary of State for Public Diplomacy and Public Affairs be chair of the Policy Coordinating Committee for Strategic Communication.

We also recommend that the Office of Management and Budget create a position of Program Associate Director for Strategic Communication to allow effective coordination and advocacy for the overall government wide funding profile.

RECOMMENDATION 2. LEADERSHIP

Create a permanent strategic communication structure within the White House with these elements:

- Deputy National Security Advisor and Assistant to the President for Strategic Communication
- Deputies Committee for Strategic Communication
- Strategic Communication Policy Committee, chaired by the Deputy National Security Advisor and Assistant to the President for Strategic Communication, to include all departments and agencies with substantial strategic communication responsibilities
- Associate Director for Strategic Communication in the Office of Management and Budget
- legal and regulatory authorities as necessary for the Deputy National Security Advisor and Assistant to the President for Strategic Communication to:
  1. assign operational responsibilities, transfer funds, and concur in personnel appointments
  2. provide guidance on strategic communication to an independent CGE

Figure 7-28 establishes the relationships between the new leadership changes we have recommended and the CGE. The position of NSC Deputy for Strategic Communication and the new Deputies Committee for Strategic Communication will develop policy and advise the President and Principals Committee through the normal NSC process. The existing PCC for Strategic Communication should be strengthened and maintained with the Under Secretary of State for Public Diplomacy and Public Affairs as chair. The PCC will receive policy guidance from the Deputy NSC Advisor and the Deputies Committee for Strategic Communication and will work with the leadership of the CGE to reach out to industry, academia, nongovernmental organizations, and other think-tanks to provide the cultural and media analyses, establish focus groups on strategic communication, and develop programs and projects as directed by the PCC that support strategic communication objectives.

Figure 7-28. Organization for Strategic Communication

Critical Information S&T Opportunities

There are a number of scientific and technological tools and methodologies that can be applied to the understanding of today's complex information ecology. The Internet has created a vast universe of real-time and archival information and a Petri dish for experimentation that can be used and analyzed to better understand what the world is thinking and how this thinking can be influenced.

Social network analysis has matured in recent years and can be applied to Internet traffic to identify nodes of influence in the viral flow of information. Who are the change agents and opinion leaders in a particular culture, region, or topic? The hypothesis is that there are a small number of these influential nodes, which reduces the problem of achieving mass influence to the more tractable problem of influencing a few key people.

Machine translation is currently at a state at which it can be used to automatically analyze Internet content. It can also be used in the analysis of

content in printed media, and to a lesser degree, that in broadcast radio and television. From these translations it is possible to extract not only raw information and opinion, but indications and metrics about attitudes and feelings about important issues.

Sentiment analysis is a technique used to detect favorable and unfavorable opinions toward specific subjects within large numbers of documents. Using a syntactic parser and a "sentiment lexicon" it identifies the semantic relationships between the sentiment expressions and the subject of interest. Put simply, it tells us what the world (or some meaningful subset of the world) thinks about something.

While there is much that can be done with existing tools, strategic communication is a field that could greatly benefit from an expanded research program. Because of the revolutionary changes in the communications landscape in recent years, the field is fertile with new opportunities for the derivation and application of analytical techniques. This research program can be started immediately with existing mechanisms at the Defense Advanced Research Projects Agency (DARPA), the National Science Foundation, and within the Intelligence Community. We recommend an increase in funding for this area of $50 million.

Finally, it must be emphasized how important it is for the people and organizations involved in strategic communications to share both data and results across the entire community. While this should go without saying, too often sharing becomes the exception, rather than the rule.

RECOMMENDATION 3. CRITICAL S&T OPPORTUNITIES

The DOD needs to make greater use of existing tools and technologies to support strategic communication. For example, existing S&T capacity can be used to:

- identify nodes of influence through network analysis
- support communication and media analysis with machine translation
- understand viral information flows and influences
- utilize innovative evaluation/measurement methodologies (such as sentiment detection/analysis)

We recommend that $50 million a year be invested to advance knowledge in these areas and that this research budget be managed by the DARPA, the National Science Foundation, and the Intelligence Community. We recognize the current but disparate efforts in these areas and recommend vigorous engagement across the strategic communication community to share the existing knowledge base.

Significant Increase in Department of State Budget for Public Diplomacy and Exchanges

The current position of Under Secretary of State for Public Diplomacy and Public Affairs needs to be strengthened. The under secretary should have the authority and responsibility to review, coordinate, and certify to the Office of Management and Budget (OMB) agency budgets for strategic communication, including but not limited to State, Defense, USAID, Treasury, Commerce, and others. To accomplish this, it may be necessary to seek legislative changes to provide the DNA/SC authority to allocate, transfer, and reprogram strategic communication funds. The Under Secretary for Public Diplomacy and Public Affair should also have the authority to review and concur on key strategic communication/public diplomacy personnel assignments within the Department of State, as well as to control strategic communication resources and personnel currently lodged in State's regional and functional bureaus.

We recommend a substantial increase in the budget for public diplomacy programs and exchanges at the Department of State. Specifically, over a five-year period, beginning in fiscal year 2009, we recommend tripling the President's fiscal year 2008 request.

While we do not wish to prescribe specific allocations for these budgetary increases, we do suggest some specific areas of focus. For educational and cultural exchange programs, we believe substantial increases should go to the Fulbright; the International Visitor Leadership Program; youth exchanges; English language instruction; increased utilization of "cultural diplomats," such as American sports and entertainment figures; and programs to increase opportunities for Americans to study and conduct research abroad and to provide exchange and training opportunities for key foreign influences, including journalists, pundits, academics, and government officials.

For the diplomatic and consular programs/public diplomacy account, emphasis should be placed on the recruitment, training, and deployment overseas of public diplomacy positions, and in particular to make senior public diplomacy

Foreign Service officers available as advisors to combatant commanders. Increases should also be provided for opinion, attitude, and behavioral research and evaluation of and for public diplomacy programs. Other areas of emphasis include expanded Bureau of International Information Program activities (use of the Internet, foreign language websites, blogging, sms), as well as more "traditional" programs, such as book translation programs.

RECOMMENDATION 4. DEPARTMENT OF STATE

The Under Secretary of State for Public Diplomacy and Public Affairs should be given enhanced policy, budget, and personnel authorities.

We recommend a significant increase in the budget for the State Department's public diplomacy programs, including exchanges over a five-year period. The budget should be tripled and those additional funds be used in the following areas:

- exchanges (such as Fulbright, International Visitor Leadership Program, International Military Education and Training)
- Americans studying/conducting research abroad
- recruitment, training and deployment of additional public diplomacy positions
- support for strategic communication and public diplomacy activities of the U.S. military's combatant commands
- Internet, websites, blogging, Rapid Response Units, and Digital Outreach Teams
- opinion, attitude, and behavioral research and evaluation of/for public diplomacy programs
- book translation programs
- utilization of sports and entertainment figures as cultural diplomats
- training and partnerships with key civil society activists (journalists, local media, civic organizations)
- online English language programs focused on marginalized young Muslim populations
- public-private partnerships targeted at economic development and job creation in key strategic nations (Lebanon, Pakistan, Iraq, for example).

A senior State Department public diplomacy representative should be assigned to each combatant command.

Review of Broadcasting Board of Governors Mission, Structure, Funding, and Performance

The Broadcasting Board of Governors oversees an array of important, global media that reaches tens of millions of people in 57 languages. The context in which these media operate is in rapid transition. The traditional distinction between international broadcasting (HF and MW radio) and domestic broadcasting (AM/FM radio and terrestrial broadcast TV) is blurring, and both international and domestic broadcasters are increasingly being supplanted by transnational DBS-TV and a growing assortment of Internet-based media offerings.

Audience preferences and habits are changing and U.S. national strategic communication priorities are increasingly focused on reaching audiences in areas with significant Muslim populations. The entities that provide BBG broadcast services (VOA, RFE/RL, RFA, Radio and TV Marti, MBN) are responding to this shift in audience preference and national priorities. Radio continues to be the dominant distribution medium, but several services are accelerating a transition to TV distribution. This requires new investment in production facilities, training and distribution.

There is also increasing use of IP-based services (web sites, podcasts, etc.) Both VOA and REF/RL have achieved significant success with their web distribution.

RECOMMENDATION 5. BROADCASTING BOARD OF GOVERNORS

Conduct a review of the mission, structure, funding, and performance of the Broadcasting Board of Governors, as an integral element of the overall U.S. strategic communication capability.

The review should include the following:

- current media mix
- relationship among the U.S. international broadcasting services (e.g., VOA, RFE/RL, RFA)
- utilization of new communication media

- new models for utilization and funding of news and program services
- language priorities (currently 60 languages)
- audience research (market research, media usage, impact)
- management structures and relationships with the executive branch.

This study is pleased with the passage of Section 316 of the 9/11 bill that provides the President new authority to support requirements for surge broadcasting. We urge the administration and the Congress to implement procedures and funding measures to utilize this much-needed authority when a surge requirement is identified.

Significant Increase in the DOD Budget for Strategic Communication

The Department of Defense should create a permanent leadership position to coordinate all strategic communication activities within the Department and provide representation to the PCC for Strategic Communication. We believe this requires a new permanent policy office led by a deputy under secretary with representation from the offices of the Assistant Secretary of Defense for Public Affairs, the Joint Chiefs of Staff, and the Under Secretary of Defense for Intelligence. This new office would review and coordinate all strategic communication activities across public affairs, information operations, and the combatant command domains.

In addition, the Department should make the investments necessary to create an off-the-shelf capability to enable joint task force personnel, in coordination with host nation representatives, to communicate with affected publics. Significant deficiencies in this critical component of stability operations existed in both Afghanistan and Iraq, and would most likely be the case in many of the large ungoverned, or marginally governed, spaces that joint task force commanders could encounter. We also urge the Department to ensure that planning for such communication shortfalls be included in both Contingency Planning Guidance and Security Cooperation Guidance to the combatant commands.

Currently, DOD–funded FFRDCs such as RAND and the Institute for Defense Analyses, provide indirect support to the combatant commands by working through the Office of the Secretary of Defense, the Services, and supporting commands such as Joint Forces Command. Ongoing research programs on empowering moderate and countering extremist voices, for

example, could be developed on a regional basis for application in partnership with country teams and local authorities. Engagement strategies for regional media and other influence nodes could be developed and tailored for each combatant command.

We also identified more specific actions that could, if taken, provide direct support to security cooperation programs. Replicating the recent deployment of the *USNS Comfort* to Central and South America through activations of additional hospital ships would provide geographic combatant commands and country teams an opportunity to match words with actions about U.S. values, in partnership with local authorities and perhaps nongovernmental organizations (such as Doctors without Borders). Similarly, a cooperation program between the National Geospatial-Intelligence Agency and U.S. Strategic Command to provide unclassified reconnaissance products for regional and local environmental studies, crop management, and weather forecasting, for example, to country teams offers an opportunity to partner with local authorities.

There also appear to be opportunities to leverage IMET and DOD Regional Center programs toward improving interaction between the military and the private sector. At the National Defense University, the Industrial College of the Armed Forces has sought increasing industry representation across its annual future leaders class for several years. Eliminating current restrictions on DOD Regional Centers providing for the participation by both faculty and students whose origin and expertise fall outside the Security and Defense occupational fields (e.g. journalists, media executives and other opinion shapers). This would serve to significantly enrich a program that emphasizes educating the role of security in civilian societies, harmonizing views on common security challenges, de-legitimizing terrorist-driven extremism, and building support for moderate governments and societies.

Finally, the negative connotation people associate with the use of the term "PSYOP" (psychological operations) hinders the effective application of sound principles and doctrine. PSYOP activities that support military operations and training should be relabeled "Tactical Information Operations." PSYOP support to U.S. embassies and to geographic combatant commands in the context of security cooperation should also be renamed more appropriately, such as "military information support" or "public diplomacy support."

RECOMMENDATION 6. DEPARTMENT OF DEFENSE

Create a permanent Deputy Under Secretary of Defense for Strategic Communication, reporting to the Under Secretary of Defense for Policy.

This new office would include senior representatives from the Office of the Secretary of Defense for Public Affairs, the Joint Staff, and the Under Secretary of Defense for Intelligence. This new office would review and coordinate all activities across public affairs and information operation domains.

Significantly increase the strategic communication budgets of each combatant command. These budgets should be tripled within a separate budget for each combatant command. The additional funds should be used in the following activities:

- Support FFRDCs—such as the Institute for Defense Analysis and RAND—for cultural analysis and program development in each combatant commander's area of responsibility.
- Provide communications infrastructure in support of stability operations and disaster relief operations.
- Increase public affairs presence at combatant commands to support security cooperation.
- Increase collaborative planning and experimentation with nongovernmental organizations.

In addition, we recommend increasing engagements in support of strategic communication. For example:

- Increase hospital ship and crew activation to support security cooperation programs.
- Utilize Corps of Engineers capabilities to support programs for disaster relief, flood control, and infrastructure development (security cooperation).
- Release reconnaissance products for environmental studies, crop management, weather forecasting, food and water supply management, deforestation, and other similar activities.

- Create opportunities for civil sector participation (media, NGOs, academics) at the National Defense University, the military service colleges, and Centers for Regional Security Studies.

Finally, PSYOPs should be relabeled according to whether they are in support of military operations or other activities such as security cooperation and DOD support to public diplomacy.

Actions for Today

Many of the specific actions identified in the previous recommendations can be implemented immediately, and are organized here. The Departments of Defense and State should implement immediate actions such as the following:

- Establish and enhance combatant commander budgets for strategic communication to
  - fund FFRDCs to conduct cultural analysis and program developments in the area of responsibility
  - provide communications infrastructure in support of stability operations and disaster relief operations
- Increase DOD support for strategic communication through, for example:
  - increases in hospital ship and crew activation to support security cooperation programs
  - release of reconnaissance products for environmental studies, crop management, weather forecasting, food and water supply management, deforestation
  - creation of opportunities for civil sector participation at the National Defense University, the military service colleges, and Centers for Regional Security Studies
- Expand the Department of State's Strategic Communication funding and for activities such as:
  - online English language programs focused on marginalized young Muslim populations
  - Internet, websites, blogging, Rapid Response Units, and Digital Outreach Teams
  - public-private partnerships targeted at economic development and job creation in key strategic regions (such as Lebanon, Pakistan, Iraq).

Appendix VII-A. Executive Summary and Recommendations from the 2004 DSB Report on Strategic Communication

Below are the Executive Summary and the recommendations of the 2004 Defense Science Board Task Force on Strategic Communication[164].

The Defense Science Board Summer Study on the Transition to and from Hostilities was formed in early 2004 and culminated in the production of a final report and summary briefing in August of 2004. The DSB Task Force on Strategic Communication conducted its deliberations within the overall Summer Study schedule and revisited a topic that was addressed in October 2001.[165] The current Strategic Communication Task Force re-examined the purposes of strategic communication and the salience of recommendations in the earlier study. It then considered the following questions:

a. What are the consequences of changes in the strategic communication environment?

b. What Presidential direction and strategic communication means are required?

c. What should be done about public diplomacy and open military information operations?

The task force met with representatives from the National Security Council (NSC), White House Office of Global Communications, Department of State (DOS), Department of Defense (DOD), Broadcasting Board of Governors (BBG), and the private sector. Based on extensive interaction with a broad range of sectors in the government, commercial, and academic worlds, as well as a series of highly interactive internal debates, we have reached the following conclusions and recommendations.

---

164. http://www.acq.osd.mil/dsb/reports/2004-09-Strategic_Communication.pdf
165. Report of the Defense Science Board Task Force on Managed Information Dissemination, October 2001, http://www.acq.osd.mil/dsb/mid.pdf. The report was briefed to the Secretary of Defense, the Under Secretary of State for Public Diplomacy and Public Affairs, the Under Secretary of State for Management, and the National Security Council's Senior Advisor for Strategic Communications and Information and Senior Advisor for Democracy, Human Rights, and International Operations.

This task force concludes that U.S. strategic communication must be transformed.

America's negative image in world opinion and diminished ability to persuade are consequences of factors other than failure to implement communications strategies. Interests collide. Leadership counts. Policies matter. Mistakes dismay our friends and provide enemies with unintentional assistance. Strategic communication is not the problem, but it is a problem.

Understanding the problem. Strategic communication is a vital component of U.S. national security. It is in crisis, and it must be transformed with a strength of purpose that matches our commitment to diplomacy, defense, intelligence, law enforcement, and homeland security. Presidential leadership and the bipartisan political will of Congress are essential. Collaboration between government and the private sector on an unprecedented scale is imperative.

To succeed, we must understand the United States is engaged in a generational and global struggle about ideas, not a war between the West and Islam. It is more than a war against the tactic of terrorism. We must think in terms of global networks, both government and non-government. If we continue to concentrate primarily on states ("getting it right" in Iraq, managing the next state conflict better), we will fail. *Chapter 2 of this report examines the complex nature of this new paradigm and implications for sustained and imaginative action.*

Strategic communication requires a sophisticated method that maps perceptions and influence networks, identifies policy priorities, formulates objectives, focuses on "doable tasks," develops themes and messages, employs relevant channels, leverages new strategic and tactical dynamics, and monitors success. This approach will build on in depth knowledge of other cultures and factors that motivate human behavior. It will adapt techniques of skillful political campaigning, even as it avoids slogans, quick fixes, and mind sets of winners and losers. It will search out credible messengers and create message authority. It will seek to persuade within news cycles, weeks, and months. It will engage in a respectful dialogue of ideas that begins with listening and assumes decades of sustained effort. Just as importantly, through evaluation and feedback, it will enable political leaders and policymakers to make informed decisions on changes in strategy, policies, messages, and choices among instruments of statecraft. *Chapter 2 of this report addresses ways in which strategic communication can be generated and managed with effect.*

We need to move beyond outdated concepts, stale structural models, and institutionally based labels. Public diplomacy, public affairs, psychological operations (PSYOP) and open military information operations must be coordinated and energized. *Chapter 4 of this report recommends changes in the strategic communication functions and structures of the Departments of State and Defense, U.S. embassies and combatant commands.*

Leadership from the top. A unifying vision of strategic communication starts with Presidential direction. Only White House leadership, with support from cabinet secretaries and Congress, can bring about the sweeping reforms that are required. Nothing shapes U.S. policies and global perceptions of U.S. foreign and national security objectives more powerfully than the President's statements and actions, and those of senior officials. Interests, not public opinion, should drive policies. But opinions must be taken into account when policy options are considered and implemented. At a minimum, we should not be surprised by public reactions to policy choices. Policies will not succeed unless they are communicated to global and domestic audiences in ways that are credible and allow them to make informed, independent judgments. Words in tone and substance should avoid offence where possible; messages should seek to reduce, not increase, perceptions of arrogance, opportunism, and double standards. These objectives mean officials must take full advantage of powerful tools to measure attitudes, understand cultures, and assess influence structures—not occasionally but as an iterative process. *Policies and strategic communication cannot be separated.*

Swift and sustained Presidential direction is also required to connect strategy to structure.

In 1947, America confronted new threats and opportunities as well. The President with bipartisan support in Congress carried out policy and organizational initiatives that shaped U.S. national security for two generations. Today, we face challenges of similar magnitude, made more formidable by a world where geography, military power, and time to react are no longer sufficient to ensure our security. Strategic communication and other 21st century instruments of statecraft require changes different in kind but similar in scale to the National Security Act of 1947 and the Goldwater-Nichols Act of 1986.

These changes will occur only with sustained, enthusiastic, and deeply committed Presidential leadership—and the collaborative and bipartisan support of the Foreign Relations and Armed Services Committees of Congress.

Government-private sector partnership. Finding new ways to harness strategic communication to the flexibility and creative imagination of the private sector will be central to successful strategic communication in the 21st century. The commercial sector has a dominant competitive edge in multi-media production, opinion and media surveys, information technologies, program evaluation, and measuring the influence of communications. Academic and research communities offer vast untapped resources for education, training, area and language expertise, planning and consultative services.

Effective sharing between government and society in the conduct of strategic communication is not new. Government grants to private organizations have long been a way to carry out international educational and cultural exchanges, foreign opinion polling, democratization and media training programs, and much of U.S. international broadcasting. Grants extend the reach of government programs and capitalize on the expertise and flexibility of non-government partner organizations.

Recent study groups, including the October 2001 Defense Science Board Task Force, have recommended more extensive collaboration. These observers see value not only in leveraging private sector competencies but in new structures and a *degree of distance* that attracts credible messengers with non-government resumes, creative thinkers and talented communicators uncomfortable working with government agencies, and skilled, language qualified professionals available for temporary crisis deployment.

Collaboration between government and the many benefits of private sector thinking and skills should be strongly encouraged. The complexity of strategic communication problems calls for balanced coordination of effort. Independent analysis is required in a wide range of fields: cultures and values, international intellectual engagement, communications studies, and applied science. Teamwork among civilian agencies and military services will be necessary to draw effectively on the seminars of universities, professional skills of non-governmental organizations (NGOs), and imagination of the media production industry. Appropriate controls and risk assessment will be needed. For all their strengths, private organizations represent particular interests. Investments in strategic communication must be grounded in the public interest as determined by appropriate executive branch and Congressional authorities.

Election cycles and episodic commitment have shaped implementation of U.S. strategic communication for more than half a century. New thinking and

new collaborative structures hold promise of a transformed and continuous strategic communication capability that serves America's interests.

The task force has made a set of recommendations listed below which we believe will make a significant difference. The time line and scale of their impact is difficult to quantify but we will not succeed in revitalizing Strategic Communication if we tinker around the edges. Given the enormous challenges we face, we can succeed only if we use all the instruments of national power. We should expect to see some progress within a year but we are dealing with at least a decade to have a significant impact. US public diplomacy efforts in the Cold War, the creation of the Peace Corps and the launch of a new brand or product within the private sector in a highly competitive environment are examples of efforts that have required comparable time scales and the challenges we face today are potentially more complex. We must begin and maintain our intensity and focus until we succeed.

Recommendation 1

The task force recommends that the President issue a directive to:

- Strengthen the U.S. Government's ability to understand global public opinion, advise on the strategic implications of policymaking, and communicate with global audiences;
- Coordinate all components of strategic communication including public diplomacy, public affairs, international broadcasting, and military information operations; and
- Provide a foundation for new legislation on the planning, coordination, conduct, and funding of strategic communication.

Recommendation 2

The task force recommends that the President should establish a permanent strategic communication structure within the NSC and work with Congress to create legislation and funding for a:

- Deputy National Security Advisor for Strategic Communication;
- Strategic Communication Committee within the NSC; and an
- Independent, non-profit, non-partisan Center for Strategic Communication

The Deputy National Security Advisor for Strategic Communication should chair a Strategic Communication Committee. Its members should have the equivalent of under secretary rank and be designated by the Secretaries of State, Defense and Homeland Security; the Attorney General; the Chief of Staff to the President; the Director of the Office of Management and Budget; the White House Communications Director; the Director of Central Intelligence; the Chairman of the Joint Chiefs of Staff; the Director of the Agency for International Development; and the Chairman of the Broadcasting Board of Governors. Unlike previous coordinating mechanisms with nominal authority, this Strategic Communication Committee should have authority to assign responsibilities and plan the work of departments and agencies in the areas of public diplomacy, public affairs, and military information operations; concur in strategic communication personnel choices; shape strategic communication budget priorities; and provide program and project direction to a new Center for Strategic Communication.

Recommendation 3

The task force recommends that the President work with Congress to create legislation and funding for an independent, non-profit and non-partisan Center for Strategic Communication to support the NSC and the departments and organizations represented on its Strategic Communication Committee. The Center should be a hybrid organization modeled on federally funded research and development centers (FFRDCs), such as the Rand Corporation, and the National Endowment for Democracy. It should be a tax-exempt private 501(c)(3) corporation that would receive an annual appropriation approved by Congress as part of the Department of State budget. The NSC's Deputy National Security Advisor for Strategic Communication and the members of the Strategic Communication Committee should provide program and project direction to the Center. The Center for Strategic Communication should be governed by an independent nonpartisan Board of Directors that would include distinguished Americans drawn from relevant professions and members of Congress appointed on a bipartisan basis. The NSC's Deputy National Security Advisor for Strategic Communication should be an ex-officio member of the Board. The Board of Directors should appoint the Center's Director and ensure mission coherence and quality of performance.

The Center should be guided by three purposes:

- Provide information and analysis on a regular basis to civilian and military decision makers on issues vital to U.S. national security including global public opinion; the role of culture, values, and religion in shaping human behavior; media trends and influences on audiences, information technologies, the implications of all source intelligence assessments, and non-departmental, non-political advice that will sharpen their judgment and provide a basis for informed choices.
- Develop mandated and self-initiated plans, themes, products and programs for the creation and implementation of U.S. communications strategies that embrace diplomatic opportunities and respond to national security threats.
- Support government strategic communications through services provided on a cost recovery basis that mobilize non-governmental initiatives; foster cross-cultural exchanges of ideas, people, and information; maintain knowledge management systems, language and skills inventories, and procedures to recruit private sector experts for short term assignments, deploy temporary communications teams; augment planning, recruitment, and training; and continually monitor and evaluate effectiveness.

Recommendation 4

The task force recommends that the Secretary of State redefine the role and responsibility of the Under Secretary of State for Public Diplomacy and Public Affairs to be both policy advisor and manager for public diplomacy. The Under Secretary should serve as the Department's principal on the NSC's Strategic Communication Committee; have adequate staff for policy advice, program direction, and evaluation; direct the Department's foreign opinion and media research activities; approve senior public diplomacy assignments; and review the performance ratings of public diplomacy office director and embassy public affairs officers. All foreign policy initiatives and directives should have a public diplomacy component approved by the Under Secretary. The Department's current resources (personnel & funding) for public diplomacy should be tripled from current levels and placed under the control of the Under Secretary. The Department should provide a core funding grant to the Center for Strategic Communication in the amount of an annual appropriation in the Department's budget.

Recommendation 5

The task force recommends that public diplomacy office directors in the Department of State should be at the level of deputy assistant secretary or senior advisor to the Assistant Secretary. Officers promoted to Chief of Mission positions or the Senior Foreign Service should have served at least one tour in a public diplomacy assignment in the Department or in an interagency assignment relevant to public diplomacy. The Bureau of International Information Programs should be directed by an Assistant Secretary.

Recommendation 6

The task force recommends that the Under Secretary of Defense for Policy should act as the DOD focal point for strategic communication and serve as the Department's principal on the NSC's Strategic Communication Coordinating Committee. The Under Secretary for Policy should coordinate strategic communication activities with the Assistant Secretary of Defense for Public Affairs and the Under Secretary of Defense for Intelligence. The Under Secretary of Defense for Policy should extend the role and responsibility of the Assistant Secretary of Defense for International Security Affairs to act as the Department's focal point for military support of public diplomacy and create a new Deputy Assistant Secretary for International Security Affairs to coordinate all activities associated with military support for public diplomacy; and provide adequate staff for policy advice, program direction, and evaluation.

Recommendation 7

The task force recommends that the Under Secretary of Defense for Policy and the Joint Chiefs of Staff ensure that all military plans and operations have appropriate strategic communication components, ensure collaboration with the Department of State's diplomatic missions and with theater security cooperation plans; and extend U.S. STRATCOM's and U.S. SOCOM's Information Operations responsibilities to include DOD support for public diplomacy. The Department should triple current resources (personnel & funding) available to combatant commanders for DOD support to public diplomacy and reallocate Information Operations funding within U.S. STRATCOM for expanded support for strategic communication programs.

Appendix VII-B. Recommendations from the 2001 DSB Report on Managed Information Dissemination

Below are the recommendations of the 2001 Defense Science Board Task Force on Managed Information Dissemination[166].

Recommendation 1

The task force recommends that the President issue a National Security Presidential Directive (NSPD) on international information dissemination to

1. Strengthen the U.S. Government's ability to communicate with foreign audiences and thereby shape understanding of and support for U.S. national security policies, and
2. Coordinate public diplomacy, public affairs, and overt international military information.

The directive should require all regional and functional National Security Council (NSC) Policy Coordinating Committees to

1. Assess the potential impact of foreign public opinion when national security options are considered and
2. Recommend or develop strategies for public information dissemination strategies before or in concert with policy implementation.

Recommendation 2

The task force recommends that the NSPD establish an NSC Policy Coordinating Committee (PCC) on International Information Dissemination. The committee should be chaired by a person of Under Secretary rank designated by the Secretary of State. The chair will be assisted by a deputy designated by the Assistant to the President for National Security Affairs. Members of senior rank should be designated by the Secretaries of Defense, Treasury, and Commerce; the Attorney General; the Chairman of the Joint

166. See http://www.acq.osd.mil/dsb/reports/mid.pdf

Chiefs of Staff; the Director of Central Intelligence; the Director of the U.S. Agency for International Development; and the Chairman of the Broadcasting Board of Governors.

Recommendation 3

The task force recommends that the NSPD delegate to the Policy Coordinating Committee and its Secretariat adequate authority to coordinate timely public diplomacy, public affairs, and open military information planning and dissemination activities, including the authority to require

- Analysis of foreign public opinion and influence structures,
- Development of strategic themes and messages for long-term and crisis response communications,
- Identify appropriate media channels, and
- Produce information products.

Recommendation 4

The task force recommends that the Secretary of State support the Policy Coordinating Committee on International Information Dissemination through a dedicated and expanded Secretariat in the Department of State consisting of the current interagency working group on international public information augmented by an expanded staff and budget and an executive secretary from the NSC staff. A robust, expanded, and multi-agency PCC Secretariat support staff, drawing upon expertise from DOS, DOD, the Joint Staff, 4th PSYOP Group, CIA, and commercial media and communications entities must be established to facilitate audience research and to develop channels and information products.

Recommendation 5

The task force recommends that the Secretary of State strengthen the Department of State's International Information Bureau under the leadership of an Assistant Secretary; substantially increase funding for Bureau activities intended to understand and influence foreign publics, with much of the increase for contracted products and services; and make these assets available to support U.S. strategic policy objectives at the direction of the Policy Coordinating Committee's Secretariat.

Recommendation 6

The task force recommends that the Secretary of State modernize and diversify the products and services of the Department of State's International Information Bureau to include significantly expanded use of

- Internet Web sites, streaming audio and video, and leased emerging satellite TV and FM radio broadcast channels;
- American Embassy TV and radio and Washington File print services for both direct distribution and distribution through foreign media channels;
- The Foreign Press Center by U.S. policymakers and military leaders to communicate with foreign publics though foreign press and media channels;
- Interactive information networks (and the associated databases) containing key foreign audiences and influence structures;
- Joint State-DOD training and increased interagency assignments; and
- A reserve cadre of retired, language-qualified State and DOD officers available for crisis response deployment.

Recommendation 7

The task force recommends that the Secretary of Defense establish an International Public Information Committee within DOD under OASD (SO/LIC) to coordinate all DOD open information programs carried out under the authority of the Policy Coordinating Committee on International Information Dissemination. DOD membership should include senior Public Affairs, Civil Affairs, PSYOP and Joint Staff representatives.

Recommendation 8

The task force recommends that the Secretary of Defense implement DOD's draft OASD(SO/LIC) guidelines to

- Increase coordination between PSYOP forces and the CINC/JFC staff,
- Revitalize the CINCs' Theater Engagement Plans,
- Strengthen PYSOP capability to support the U.S. Government's strategic information programs, and

Recommendation 9

The task force recommends that the Secretary of Defense enhance DOD's information dissemination capabilities worldwide in support of the regional CINCs' Theater Engagement Plans and in anticipation of crisis response requirements. In addition, the Secretary should make these capabilities available to support U.S. strategic policy objectives at the direction of the Policy Coordinating Committee on International Information Dissemination. Enhancements include

- Expanded use of direct satellite FM radio and TV,
- Additional use of regional magazines such as Forum and Dialogue,
- Expanding use of regional Internet Web sites; and
- Establishment of a public diplomacy office within the Office of the Secretary of Defense.

Recommendation 10

The task force recommends that the President and his senior national security advisors strengthen U.S. international information dissemination by

- Insisting that civilian and military information capabilities be harnessed to the Internet revolution,
- Taking full advantage of commercial media production methods, and
- Significantly increasing foreign opinion research and studies of foreign media environments and influence structures.

Appendix VII-C. Government and Independent Organization Studies of Strategic Communication and Public Diplomacy, September 2001–October 2007

Advisory Group on Public Diplomacy for the Arab and Muslim World, *Changing Minds, Winning Peace: A New Strategic Direction for U.S. Public Diplomacy,* October 2003.
http://www.state.gov/documents/organization/24882.pdf

Advisory Committee on Cultural Diplomacy, *Cultural Diplomacy: The Linchpin of Public Diplomacy,* U.S. Department of State, September 2005.
http://www.publicdiplomacywatch.com/091505Cultural-Diplomacy-Report.pdf

The Aspen Institute, *The Rise of Netpolitik: How the Internet is Changing International Politics and Diplomacy,* Eleventh Annual Aspen Instititue Roundtable on Information Technology, 2003.
http://www.aspeninstitute.org/atf/cf/{DEB6F227-659B-4EC8-8F84-8DF23CA704F5}/netpolitik.pdf

The Brookings Institution, *The Need to Communicate: How to Improve U.S. Public Diplomacy with the Islamic World,* Analysis Paper #6, January 2004.
http://www.brookings.edu/fp/saban/analysis/amr20040101.htm

Center for the Study of the Presidency, *Strengthening U.S.-Muslim Communications,* July 2003.
http://www.thepresidency.org/pubs/US-MuslimCommunications.pdf

Congressional Research Service, *Public Diplomacy: A Review of Past Recommendations,* Library of Congress, September 5, 2005.
http://www.opencrs.com/rpts/RL33062_20050902.pdf

Consortium for Strategic Communication, A 21st Century Model for Communication in the Global War of Ideas: From Simplistic Influence to Pragmatic Complexity, Report #0701, Arizona State University, April 3, 2007.
http://comops.org/publications/CSC_report_0701-pragmatic_complexity.pdf

Council on Foreign Relations Independent Task Force on Public Diplomacy, *Public Diplomacy a Strategy for Reform,* July 2002.
http://129.11.188.64/papers/pmt/exhibits/579/Task-force_final2-19.pdf

Council on Foreign Relations Independent Task Force on Public Diplomacy, *Finding America's Voice: A Strategy for Reinvigorating Public Diplomacy,* September 2003.
http://www.cfr.org/content/publications/attachments/public_diplomacy.pdf

The Heritage Foundation, *Strengthening U.S. Public Diplomacy Requires Organization, Coordination, and Strategy,* Backgrounder No. 1875, August 5, 2005.
http://www.heritage.org/Research/PublicDiplomacy/bg1875.cfm

The Heritage Foundation, *Reclaiming America's Voice Overseas,* May 2003.
http://www.heritage.org/Research/NationalSecurity/wm273.cfm

The Heritage Foundation, *How to Reinvigorate U.S. Public Diplomacy,* April 2003.
http://www.heritage.org/Research/PublicDiplomacy/bg1645.cfm

Defense Science Board Task Force on Strategic Communication, *Strategic Communication,* September 2004.
http://www.acq.osd.mil/dsb/reports/2004-09-StrategicCommunication.pdf

Defense Science Board Task Force Sponsored by the Department of Defense and Department of State, *Managed Information Dissemination,* September 2001.
http://www.acq.osd.mil/dsb/reports/mid.pdf

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. July 22, 2004.
http://www.gpoaccess.gov/911/index.html

Public Diplomacy Council. *Call for Action on Public Diplomacy,* January 2005.
http://pdi.gwu.edu/merlin-cgi/p/downloadFile/d/7536/n/off/other/1/name/ACAL%20LFORACTIONONPUBLICDIPLOMACY01-2005prin

Public Diplomacy Council, Transformation Not Restoration," Statement of Dissent to *Call for Action on Public Diplomacy,* January 2005.
http://pdi.gwu.edu/merlin-cgi/p/downloadFile/d/7537/n/off/other/1/name/Dissent%20_12-21-04pdf/

RAND National Defense Research Institute, *Enlisting Madison Avenue: The Marketing Approach to Earning Popular Support in Theaters of Operation,* Washington, DC, 2007.
http://www.rand.org/pubs/monographs/2007/RAND_MG607.pdf

United States Advisory Commission on Public Diplomacy. *2004 Report of the United States Advisory Commission on Public Diplomacy,* September 2004.
http://www.state.gov/r/adcompd/rls/36275.htm

U.S. Advisory Commission on Public Diplomacy, *The New Diplomacy: Utilizing Innovative Communication Concepts That Recognize Resource Constraints,* July 2003.
http://www.state.gov/r/adcompd/rls/22818.htm

U.S. Advisory Commission on Public Diplomacy, *Building Public Diplomacy Through a Reformed Structure and Additional Resources,* 2002.
http://www.state.gov/documents/organization/13622.pdf

U.S. General Accountability Office, *Actions Needed to Improve Strategic Use and Coordination of Research,* July 2007.
http://www.gao.gov/new.items/d07904.pdf

U.S. General Accountability Office, *US Public Diplomacy: Strategic Planning Efforts Have Improved, But Agencies Face Significant Implementation Challenges,* Statement before the House Subcommittee on International Organizations, Human Rights, and Oversight, April 26, 2007.
http://www.gao.gov/new.items/d07795t.pdf

U.S. General Accountability Office, *Foreign Assistance: Actions Needed to Better Assess the Impact of Agencies' Marking and Publicizing Efforts,* GAO-07-277, March 2007.
http://www.gao.gov/new.items/d06535.pdf

U.S. General Accountability Office, *U.S. International Broadcasting: Management of Middle East Broadcasting Services Could Be Improved,* GAO-06-762, August 2006.
http://www.gao.gov/new.items/d06762.pdf

U.S. General Accountability Office, *Department of State: Staffing and Foreign Language Shortfalls Persist Despite Initiatives to Address Gaps.* GAO-06-894, August 2006.
http://www.gao.gov/new.items/d06894.pdf

U.S. General Accountability Office, *U.S. Public Diplomacy: State Department Efforts to Engage Muslim Audiences Lack Certain Communication Elements and Face Significant Challenges,* GAO-06-535, May 2006.
http://www.gao.gov/new.items/d06535.pdf

U.S. General Accountability Office. *Information on U.S. Agencies' Efforts to Address Islamic Extremism,* GAO-05-852, September 2005.
http://www.gao.gov/new.items/d05852.pdf

U.S. General Accountability Office, *U.S. Public Diplomacy: State Department and Broadcasting Board of Governors Expand Post- 9/11 Efforts but Challenges Remain.* GAO-04-1061T, August 2004.
http://www.gao.gov/new.items/d041061t.pdf

U.S. General Accountability Office, *U.S. Public Diplomacy: Interagency Coordination Efforts Hampered by the Lack of a National Communication Strategy,* GAO-05-323, April 2005.
http://www.gao.gov/new.items/d05323.pdf

U.S. General Accountability Office, *U.S. International Broadcasting: Challenges Facing the Broadcasting Board of Governors,* Testimony before the U.S. Senate Subcommittee on International Operations and Terrorism, April 29, 2004.
http://www.senate.gov/~foreign/testimony/2004/FordTestimony040429.pdf

U.S. General Accountability Office, *U.S. International Broadcasting: Enhanced Measure of Local Media Conditions Would Facilitate Decisions to Terminate Language Services,* February 2004.
http://www.gao.gov/new.items/d04374.pdf

U.S. General Accountability Office, *U.S. Public Diplomacy: State Department and Broadcasting Board of Governors Expand Efforts in the Middle East but Face Significant Challenges,* GAO-04-435T, February 2004.
http://www.gao.gov/new.items/d04435t.pdf

U.S. General Accountability Office, *U.S. Public Diplomacy: State Department Expands Efforts But Faces Significant Challenges,* GAO-04-435T, September 2003
http://www.gao.gov/new.items/d03951.pdf

U.S. General Accountability Office, *U.S. International Broadcasting: New Strategic Approach Focuses on Reaching Large Audiences but Lacks Measurable Program Objectives,* GAO-03-772, July 2003.
http://www.gao.gov/new.items/d03772.pdf

U.S. National Strategy for Public Diplomacy and Strategic Communication, Strategic Communication and Public Diplomacy Policy Coordinating Committee (PCC), June 2007.
http://www.state.gov/documents/organization/87427.pdf

Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

FEB 0 2 2007

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

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

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

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

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

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

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

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

Specifically the Summer Study should:

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

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

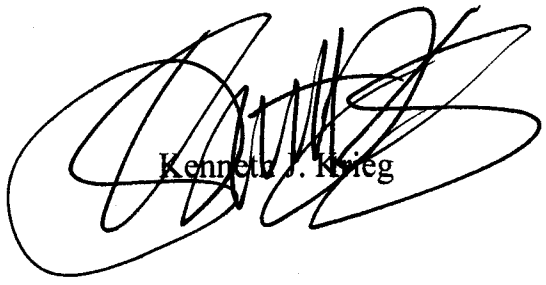
(3) Assess capability gaps;

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

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

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

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



Study Participants

CHAIRMEN

Name	Affiliation
Dr. Craig Fields	Private Consultant
Mr. Richard Haver	Northrop Grumman Corporation

EXECUTIVE SECRETARY

Todd Lowery	OSD(P)/SOLICIC

FUTURE OF WAR PANEL

Chairs	
GEN Bill Hartzog	Burdeshaw
Dr. Joe Markowitz	Private Consultant
Members	
Paul Davis	RAND
Bert Fowler	CA Fowler Associates
Dr. Ted Gold	Private Consultant
MG Kenneth Israel USAF (Ret.)	Lockheed Martin Aero
Bob Mikelskas	MITRE
Bill Murray	Alphom, LLC
MG Rich O'Lear	Lockheed Martin
Dr. Joe Rosen	Dartmouth-Hitchcock Medical Center
MG Robert Scales	Private Consultant
Dr. James Wade	Defense Group
Mike Wheeler	DTRA
Government Advisors	
LTC Kirklin Bateman	Army G-35, DAMO-SSP
COL Jeff Bearor	USMC
Peter Bechtel	HQDA DCS G-3/5/7
Thomas Behling	OSD/OUSDI
Maj Trudy Caldwell	Bechtel's Staff (HQDA DCS G-3/5/7)
Dr. James Forest	West Point (USMA)

Dr. Ellen Klein	OSD/GSA--Detainee Affairs
COL Daniel Klippstein	HQDA DCS G-3/5/7
MAJ John Livingstone	HQDA, G-3/5/7
Col Louis Michael USA (Ret.)	Defense Group Inc
Dr. Mac Owens	Naval War College (1D)
Charles Swett	OSD Policy
Robert Vickers	ODNI

TECHNOLOGY ASSESSMENT PANEL

Chairs	
Larry Lynn	Private Consultant
Bob Stein	Private Consultant
Members	
Dr. Larry Brandt	Sandia National Laboratories
Dr. Regina Dugan	RedXDefense
Dr. Kevin Fall	Intel Corporation
Dr. Milton Finger	Lawrence Livermore National Laboratory
Mr. Jim Gosler	Sandia National Laboratories
Dr. Bernadette Johnson	MIT Lincoln Laboratory
Dr. Duane Lindner	Sandia National Laboratories
Mr. Walter Morrow	MIT Lincoln Laboratory
Mr. Jim Shields	Draper Laboratory
Dr. Wayne Shotts	Lawrence Livermore National Laboratory
Dr. Ann Marie Skalka	Fox Chase Cancer Center
Dr. James Tour	Rice University
Dr. Rich Wagner	Los Alamos National Laboratory
Dr. Bruce Wald	Private Consultant
Mr. Larry Wright	BAH
Dr. Gerry Yonas	Sandia National Laboratories
Government Advisors	
Dr. Jon Calomiris	United States Army Nuclear and Chemical Agency
Mr. Christina Filarowski-Sheaks	Office of the Secretary of Defense

Dr. Stephen Morse	National Center for Preparedness, Detection, and Control of Infectious Diseases Coordinating Center, Centers for Disease Control
Ms. Cecilia Phan	The Joint Staff, Directorate for Command, Control, Communications, and Computer Systems
Dr. Lisa Rotz	National Center for Preparedness, Detection, and Control of Infectious Diseases Coordinating Center, Centers for Disease Control
David Thomen	Army G-3/5/7

NUCLEAR PROLIFERATION PANEL

Chair	
Dr. Brad Roberts	Institute for Defense Analyses
Members	
Dr. Dan Chiu	Institute for Defense Analyses Joint Advanced Warfighting Program
Dr. Lewis Dunn	SAIC
John Hinton	Sandia National Laboratory
Douglas Lawson	OATSD(NCB/NM)
Dr. James Miller	Center For a New American Security
Jim Thomas	Applied Minds, Inc.
Dr. Victor Utgoff	Institute for Defense Analyses
Major Stephanie Vaughn	US Army Nuclear and Combating WMD Agency
Government Advisors	
Larry Brant	Sandia National Laboratories
Melanie Elder	ODNI/National Couterproliferation Center
Ms. Rebecca Hersman	National Defense University
Col Chuck Lutes USAF	National Defense University
Mike Wheeler	DTRA

DEFENDING AGAINST DOMESTIC CATASTROPHE IN WAR TIME PANEL

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

ENSURING DEPLOYMENT AND SUPPLY PANEL

Chairs	
Dr. Miriam John	Private Consultant
Dr. Ronald Kerber	Private Consultant
Members	
Dr. John Cummings	Sandia National Laboratories
Maj Gen John Fenimore V, USAF (Ret)	J.H. Fenimore & Assoc, LLC
LtGen Rick Kelly USMC (Ret.)	LMI
Dr. Duane Lindner	Sandia National Laboratories
VADM Keith Lippert, USN (Ret.)	Accenture National Security Service, LLC
Ms. Nancy Suski	Lawrence Livermore National Laboratory
LTG David Teal USAF (Ret.)	Accenture National Security Services
Ms. Nancy Wilson	Association of American RR
Government Advisors	
COL Joe Bassani, USA	NORTHCOM
Mr. Bill Bryan	OSD(P)/ASD/HD
Mr. James Caverly	DHS
Mr. G. Gurvais Grigg	FBI
Mr. Lacey Hughes	HQDA DCS G-4
Mr. John Humpton	Department of the Army, G3

WHAT WE KNOW AND DON'T KNOW: INTELLIGENCE PANEL

Chair	
ADM Bill Studeman	Private Consultant
Members	
Joan Dempsey	Booz Allen Hamilton
Marty Faga	MITRE
Carol Haave	
Jeffrey Harris	LMCO
Jake Jacoby VADM, USN, (Ret.)	CACI, Inc.
Peter Marino	Private Consultant
Joseph Mazzafro	EMC2
Dave McMunn	McMunn Associates, Inc.
Barbara McNamara	CACI International
Rocky Roccanova	Rock & Nova
Earl Sheck	NGC
Dick Szafranski	Toffler Associates
Jim Woolsey	BAH
Mike Wheeler	DTRA
Government Advisors	
RC Porter	OSD
Michelle Van Cleave	National Defense University

FIGHTING THROUGH ASYMMETRIC COUNTERFORCE PANEL

Chair	
GEN Jim McCarthy, USAF (Ret.)	U.S. Air Force Academy
Members	
Russ Barber	Raytheon
LT GEN David Deptula	AF/A2
VADM Dave Frost USN (Ret.)	Frost & Associates, Inc.
Greg Gardner	Oracle Corporation
Dr. Ted Gold	Private Consultant
GEN Richard Hearney USMC (Ret.)	Private Consultant
Dr. Bob Hermann	Private Consultant

Richard Ivanetich	Institute for Defense Analyses
ADM Greg Johnson USN (Ret.)	
Jim Kurtz	Institute for Defense Analyses
Jim Kuzmick	Private Consultant
Zachary Lemnios	MIT Lincoln Lab
Maj. Gen Tim Lowenberg	Washington Army and Air National Guard
Dr. Jerry McGinn	Northrop Grumman Corporation
Dawn Meyerriecks	Private Consultant
RADM Norm Saunders USCG (Ret.)	SAIC
GEN Eric Shinseki	USA
Government Advisors	
Col Ronald Banks	USAF A9L
LTC Alan Eckersley	Army G-3/5/7
BG David Fadok	HAF
Darrin Gilchrist	
COL Clay Hicks	HQDA, G-33, Army Asymmetric Warfare Office, DAMO-ODA-P
BGen Jan-Marc Jouas	AF ISR Agency/CV
COL Doug King	USMC
CAPT Forbes MacVane	USN JFCC-NW J9
Ed Martin	Contractor, The Wexford Group International G3/5/7
Tim Moore	US Army Nuclear and Chemical Agency
John Plant	Contractor, The Wexford Group G3/5/7
LTC Dirk Plante	ARMY
Douglas Richardson	USSOCOM
Jeffrey Sawyer	DTRA
LTC Richard Voegtly	G3/5/7

STRATEGIC COMMUNICATION PANEL

Chair	
Mr. Vincent Vitto	Private Consultant
Members	
Mr. Robert Coonrod	Private Consultant
Dr. Barry Fulton	Private Consultant
Prof. Bruce Gregory	George Washington University
Prof. Anita Jones*	University of Virginia
Dr. Robert Lucky*	Private Consultant
Dr. Mark Maybury	The MITRE Corporation
Ms. Leigh Warner	Private Consultant
Government Advisors	
Amb. Brian Carlson	State Department and OSD Policy
BG Mari Eder	Deputy Chief of Public Affairs, US Army
Mr. Morris Jacobs	U.S. State Department
Mr. John Matheny	OSD Policy
Mr. John Mills	OASD NII / CIO
RDML Frank Thorp	Joint Communications and SCIG, OSD

ADDITIONAL GOVERNMENT ADVISORS

Maj Russell Buttram	USMC
COL Igor Gardner USAF	ISR Plans and Resources DCS, Intelligence
COL Brian Groft	DDUSA Nuclear and Combating WMD Agency
Dave Helvey	OSD Policy
Frank Hoffman	Marine Corps Warfighting Lab
COL Jonathan Jaffin	U.S. Army Medical Research and Material Command
CAPT Andrew King	Chief of Naval Operations (N81)
Dr. George Ludwig	U.S. Army Medical Research and Material Command
Terry Pudas	OUSDP
LTC Bryan Sparling	US Southern Command
Shawn Spencer	STRATCOM G-8

COL Jeffrey Springman	JCS J5
Captain Gene Wynne	USMC

DSB REPRESENTATIVES

Brian Hughes	DSB Office Executive Director
Andrew Chappell	DSB Office, USA
Maj Charles Lominac	DSB Office, USAF
Clifton Phillips	DSB Office, USN

STAFF

Barbara Bicksler	Strategic Analysis, Inc.
Sarah Canna	Strategic Analysis, Inc.
Julie Evans	Strategic Analysis, Inc.
Kelly Frere	Strategic Analysis, Inc.
Jennifer Howell	Strategic Analysis, Inc.
Anthony Johnson	Strategic Analysis, Inc.
Brian Keller	Private Consultant
Carla King	Strategic Analysis, Inc.
Philippe Loustaunau	Vista Consulting LLC
Toni Marechaux	Strategic Analysis, Inc.
Adam Savery	Strategic Analysis, Inc.
Ted Stump	Strategic Analysis, Inc.

Presentations to the Study

Name	Topic

Plenary Sessions

JANUARY 24, 2007

Ms. Judy Kim	DOD General Counsel Briefing
Mr. John J. Hamre Center for Strategic and International Studies	Discussion
Dr. Stephen A. Cambone Former Under Secretary of Defense for Intelligence	Discussion
Mr. Ryan Henry Principal Deputy Under Secretary of Defense for Policy	Discussion

FEBRUARY 21, 2007

Aaron Friedberg Princeton University Dan Blumenthal, AEI Roy Kamphausen National Bureau of Asian Research	China
Mr. Richard Lawless Deputy Under Secretary of Defense for Asia and Pacific Affairs	Discussion
COL Joseph A. Bassani, USA U.S. Northern Command	Preparing for Domestic Catastrophes: Plans and Exercises
General James E. Cartwright Commander, U.S. Strategic Command	Discussion

MARCH 21, 2007

Mike Vickers Director, Strategic Studies, CSBA	Strategic Competition and Conflict with Near-Peer Competitors
Dr. Richard Danzig	Biowarfare
MG John Landry	Discussion
RADM Kenneth Deutsch Director, Warfare Integration (N6F)	Discussion

APRIL 25, 2007

Mr. William Neugent MITRE	Countering Sophisticated Cyber Threats
Mr. Peter Bechtel Director for the US Army Nuclear and Combating WMD Agency	Discussion
COL Jonathan Jaffin Acting Commander, U.S. Army Medical Research and Materiel Command	Future Army Medical Challenges

JUNE 20, 2007

Lt. Gen. David A. Deptula Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance	Discussion

Future of War Panel

MARCH 20, 2007

Jim Thomas, Applied Minds, Inc.	Discussion on QDR (Secret)
Patrick Garrett, Bill Miles, & Joel Sepulveda, CIA	Chinese ASAT Launch (TS/SCI)
Charles Swett, OSD	QDR Scenarios
Joseph Rosen, Dartmouth-Hitchcock Medical Center and War Panel Member	Theory and Practice of War: Adversaries, Weapons, and Recommendations

APRIL 24, 2007

Maj Gen Rich O'Lear, Lockheed Martin & War Panel Member	Red Team Perspectives and Tasks (FOUO)
Jason M.K. Lyall Assistant Professor of Politics & International Affairs, Princeton University LTC Isaiah Wilson, West Point	"Rage Against the Machines: Mechanization and the Determinants of Victory in Counterinsurgency Warfare"
Andy Marshall, Director, Office of Net Assessment, OSD	Past War Gaming (Secret)
Mackubin Thomas Owens Associate Dean of Academics and Professor of National Security Affairs, US Naval War College	The Logic of Future Force Planning

MAY 22, 2007

Dan Flynn, Office of the Director of National Intelligence	NIC Assessment (Secret/NOFORN)

JULY 17, 2007

Robert O. Work Vice President, Strategic Studies, CBSA	Thinking About Future Warfare
Roy Evans Director of National Security Analysis Group, MITRE Corporation	Future of War (Secret)

Technology Assessment Panel

FEBRUARY 20, 2007

Norman Kahn, Program Manager Intelligence Technology Innovation Center	Biological Defense Research in the Intelligence Community

APRIL 6, 2007

Roundtable Discussion Kirtland, Air Force Base	Directed Energy Weapons

APRIL 24, 2007

Len Connell Sandia National Laboratories	Radiological Weapons Update
Dr. Jason Lyall, Princeton University LTC Isaiah Wilson, West Point	Analysis of Asymmetrical Conflicts
Lawrence Gershwin, National Intelligence Council	Cyber threat technologies and Biotechnology Issues

MAY 24, 2007

Michael R. Rooney, Defense Threat Reduction Agency	Understanding High-Altitude Electromagnetic Pulse (HEMP) Effects and Uncertainties

JUNE 21, 2007

Brett Giroir, Director, Defense Sciences Office, Defense Advanced Research Projects Agency	Progress on Relevant Research at DARPA

JULY 17, 2007

John Vitko Jr, Chemical and Biological Division, Department of Homeland Security	An Overview of DHS/S&T Chem and Bio Programs
John MacKinney, National Homeland Security Research Center, US Environmental Protection Agency	RDD Threat and Technology Needs

Nuclear Proliferation Panel

MARCH 22, 2007

Dr. Melanie Elder (chair) National Counterproliferation Center Mr. Vann H. Van Diepen, National Intelligence Officer for WMD and Proliferation Ms. Marybeth Davis, Deputy Director for Strategy and Evaluation, National Counterproliferation Center Mr. Joseph Pritchard, Deputy Director for Interdiction and Networks, National Counterproliferation Center	Proliferation Pathway Analysis
Ms. Rebecca Hersman, National Defense University	Future Nuclear Landscape: 2006–2011
Hon. Mr. Ryan Henry, Principal Deputy Under Secretary of Defense for Policy	Life in a Highly Proliferated World

APRIL 17-18, 2007

Dr. Vic Ugtoff, Institute for Defense Analysis	Extended Deterrence

MAY 22, 2007

Chuck Lutes, National Defense University	Pathways and Alternative Futures
Jim Thomas, Applied Minds, Inc.	From Scenarios to Requirements
Daniel Chiu, Institute for Defense Analysis	Implications for the Nuclear Deterrent

JUNE 19–20, 2007

Mr. Greg Hulcher Office of the Secretary of Defense (Acquisition, Technology &Logistics) Mr. Tom Scheber National Institute of Public Policy	"New Triad Implementation" (SECRET)

JULY 10, 2007

Mr. Greg Hulcher Office of the Secretary of Defense (Acquisition, Technology &Logistics) Mr. Dennis Even Office of the Secretary of Defense – Program Analysis & Evaluation	The New Triad Program of Record (SECRET)
COL Pat Sharon Joint Staff (J-8)	Combating WMD Program of Record (SECRET)
Dr. John Hinton Sandia National Laboratories Dr. Jim Miller Center for a New American Security	Defining the Needed Nuclear Posture

JULY 17, 2007

Ms. Rebecca Hersman, National Defense University	Means to Inhibit Future Cascades

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

FEBRUARY 9, 2007

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

MARCH 20, 2007

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

APRIL 24, 2007

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

MAY 24, 2007

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

JUNE 11, 2007

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

JUNE 12, 2007

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

JUNE 19, 2007

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

JULY 17, 2007

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

Know / Don't Know: Intelligence Panel

FEBRUARY 27, 2007

Tom Behling, DUSD (I)	How "Persistent Surveillance" Will Work in the Future

MARCH 7, 2007

Larry Gershwin, NIO for S&T	Unfolding S&T Based Challenges Confronting the military through 2025
Mary Margret Graham, Deputy Director of National Intelligence for Collection	DNI Collection Priorities for the Near Future
Vann H. Van Diepen National Intelligence Office for Weapons of Mass Destruction and Proliferation ODNI/National Intelligence Council	WMD capabilities of all the known and aspiring nuclear (also chem/bio) States

APRIL 19, 2007

LTG William Boykin, DUSD Intelligence and Warfighting Support Mr. John W. Perkins, Chief, Special Activities Division at CIA. MG Thomas Csmko, USA Special Forces Command LTG Michael Maples, Dir. DIA	Panel Discussion: "How SOF, HUMINT, and CA Interact to Generate and Use Good Intel"

MAY 11, 2007

Ken Knight, NIO for Warning	National Intelligence Warning System
Mr. Patrick Gorman, ADDNI for Strategy, Plans, and Policy	Results of the QICR (the IC Quadrennial Review)
Don Burke, CIA/DS&T Sean Dennehy, CIA/DI	Intelipedia

JUNE 12, 2007

Phil Midland	Insight on China from a Different Perspective
Hank Messick, Bill Miles, & Joe Sepulveda, CIA	Chinese ASAT Launch
Dave Cattler / Josh Kerbel	Navy Deep Red Intel
Dan DeMots/ CDR George Capen	Asia Net Assessment

Fighting Through Asymmetric Counterforce Panel

FEBRUARY 14, 2007

GEN Paul Gorman, USA (Ret.)	Military Intelligence Review

MARCH 20, 2007

COL Clay Hicks, USA	Army Asymmetric Warfare

APRIL 26, 2007

CAPT Sam Neill, USCG	Coast Guard Evergreen Project
LTC Alan Eckersley, USA	Army Irregular Warfare
BG Robin P. Swann, USA	Army Capabilities Integration Center (ARCIC)

MAY 24, 2007

Mr. John Plant	Army Asymmetric Warfare
CAPT Mark Mullins, USN	Navy Irregular Warfare / Asymmetric Perspective
Lt Col Tom Dobbs, USAF	Irregular Warfare: Implications for the U.S. Air Force
Mr. Frank Hoffman	Future Warfare: Competing for Influence
Col King, USMC (Ret.)	USMC Perspective: Irregular Warfare Cross-Functional Team

JUNE 21, 2007

Maj Gen William Shelton, USAF	AFSPACE, JFCC SPACE, USSTATCOM Brief
Dr. James A. Tegnalia	DTRA Perspective on 21st Century Warfare
Director James Rabon, JIEDDO	Network Centric ISR Fusion Capabilities in Support of Offensive Counterterrorist Operations
RADM Elizabeth Hight, USN	JTF-GNO Brief

CAPT Forbes O. MacVane, USN	Joint Functional Component Command - Network Warfare: Fighting Cyber Adversaries
Dr. Lani Kass	USAF Systems and Connectivity Perspective

JULY 21, 2007

Mr. Anthony Bargar	GIG Mission Assurance
Mr. David Aland	Assessment of IA Aspects of COCOM Exercises
Col Steve Luxion, USAF	Q&A USAF Cyber Command
Mr. James Richberg	National Cyber Study Group

Strategic Communication Panel

MARCH 1, 2007

Mr. Alberto Fernandez, Director, Middle-East, U.S. Department of State Mr. Thomas Skipper, Director, East Asia and Pacific, U.S. Department of State	Views from the Regional Bureaus
Ms. Gretchen Welch, PPR Director, U.S. Department of State	Policy Plans and Resources (PPR)
Mr. Jeremy Curtin, IIP Coordinator, U.S. Department of State	International Information Programs (IIP)
Mr. Thomas Farrell, Deputy Assistant Secretary for Academic Programs, U.S. Department of State Ms. Chris Miner, Managing Director for Professional and Cultural Exchanges Programs, U.S. Department of State	Educational and Cultural Affairs (ECA)

MARCH 23, 2007

Mr. Robert Giesler, USD (Intelligence) Col Glen Ayers, J-39	IO and PSYOPS
RDML Frank Thorp, Director, OASD (Public Affairs) Ms. Alisa Stack-O'Conner, USD (Policy)	Public Affairs and Public Diplomacy
Hon. Ryan Henry, PUSD (Policy) Hon Dorrance Smith, ASD (PA) LTG Walter (Skip) Sharp, DJS JCS	Roundtable Discussion
Mr. Michael Pease, IDA Dr. Caroline Ziemke, IDA	Discussion

APRIL 13, 2007

Dr. Jon B. Alterman, Director of the Middle East Program at the Center for Strategic and International Studies (CSIS)	The Lexus Hits an Olive Tree
Mr. David Brugger, CEO of Brugger Consulting & Brugger Global Media, former President, Association of America's Public Television Stations (APTS) William Siemering, President, Developing Radio Partners	Community-Based Media
Mr. Kenneth Y. Tomlinson, chairman of U.S. Broadcasting Board of Governors (BBG)	BBG Perspective
Mr. Gary Knell, President and CEO, Sesame Workshop	Sesame Perspective
Mr. Joe Norris, Senior Analyst/Transnational Issues Terrorism/Near East Program, DNI Open Source Center Dr. William C. Hannas, Senior Officer for East Asia S&T, DNI Open Source Center	The Current State of the Arab Media & The China RDA Metadata Mapping Project
Dr. Adam Powell, Director, Integrated Media Systems Center, USC Viterbi School of Engineering	International Broadcasting: Future Trends and Techniques

MAY 4, 2007

Ms. Mary Lou Jepsen, MIT Media Lab	One Laptop per Child
Mr. Robert Gehorsam, CEO, Forterra Systems Inc.	On Line Gaming
Mr. Ben Gross, Social Technologies Group, UC Berkeley, and UI Urbana-Champaign	Social Technologies
Ms. Susan Gigli, Chief Operating Officer, InterMedia Dr. Haleh Vaziri, Regional Research Manager for Middle East/North Africa, InterMedia	InterMedia
Mr. Mike Pease, IDA	Enemy Use of Immersive Computer Game Technology

MAY 18, 2005

Mr. Kevin Klose, President, NPR	NPR Perspective
Ms. Jody Olsen, Deputy Director, Peace Corps	Peace Corps Perspective
Mr. James Dobbins, Director, International Security and Defense Policy Center, RAND	Discussion
Professor Jarol B. Manheim, School of Media and Public Affairs, GWU	Social Network Analysis
Mr. Bruce Sherman, BBG Mr. Brian Conniff, BBG	BBG 2008-2013 strategy Radio Sawa & AlHurra TV

Interviews with Senior Officials

Mr. Peter Bechtel	Strategy, Plans, and Policy Directorate, U.S. Army
Lt. Gen. James L. Campbell	Director of the Army Staff
General James E. Cartwright	Commander, U.S. Strategic Command
General James T. Conway	Commandant, U.S. Marine Corps
Lt Gen David A. Deptula	Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, Headquarters U.S. Air Force
Honorable Eric Edelman	Under Secretary of Defense for Policy
BG Mari K. Eder	Deputy Chief of Public Affairs, U.S. Army
VADM Mark J. Edwards	Deputy Chief of Naval Operations for Communication Networks
Honorable Gordon England	Deputy Secretary of Defense
Admiral Edmund Giambastiani Jr.	Vice Chairman, Joint Chiefs of Staff
Honorable John G. Grimes	Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer
Honorable Francis Harvey	Secretary of the Army
Honorable Ryan Henry	Principal Deputy Under Secretary of Defense for Policy
Dr. Tom Hopkins	Acting Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs
ADM Timothy J. Keating	Commander, U.S. Northern Command
Honorable Ken Krieg	Under Secretary of Defense for Acquisition, Technology, and Logistics
VADM Eric T. Olson	Deputy Commander, U.S. Special Operations Command
Lt.Gen. John F. Sattler	Director for Strategic Plans and Policy, Joint Staff
MG Eric Schoomaker	U.S. Army Medical Research and Materiel Command
General Peter Schoomaker	Chief of Staff, U.S. Army
ADM James Stavridis	Commander, U.S. Southern Command
Dr. James A. Tegnelia	Director, Defense Threat Reduction Agency
Mr. Peter Verga	Assistant Secretary of Defense for Homeland Defense
Honorable Donald Winter	Secretary of the Navy
Honorable Michael Wynne	Secretary of the Air Force
Honorable John Young	Director, Defense Research and Engineering

Glossary

AESA	active electronically scanned array
APOD	airport of debarkation
ASAT	anti-satellite
ASCM	anti-sub/ship cruise missile
ASD	Assistant Secretary of Defense
ASD/HD&ASA	Assistant Secretary of Defense for Homeland Defense and America's Security Affairs
ASD/ISP	Assistant Secretary of Defense for International Security Policy
ASD/NII	Assistant Secretary of Defense for Networks and Information Integration
AWI	Asymmetric Warfare Initiative
BG	battle group
C3	command, control, and communications
C4	command, control, computing, and communications
CBG	carrier battle group
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-explosive
CDRG	Catastrophic Disaster Response Group
CENTCOM	U.S. Central Command
CEO	Chief Executive Officer
CI	counterintelligence
C3I	command, control, communications, and intelligence
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CI/KR	critical infrastructure/key resources
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Advisory Council
C2ISR	command, control, intelligence, surveillance, and reconnaissance
C4ISR	command, control, communications, computing, intelligence, surveillance, and reconnaissance
CIW	complex irregular warfare

CJCS	Chairman, Joint Chiefs of Staff
CJTFEx	Combined Joint Task Force Exercise
COCOM	Combatant Command
COIN	counter-insurgency
CONOPs	concepts of operation
CONPLAN	Concept of Operations Plan
CONUS	continental United States
COTS	commercial off-the-shelf
CSRT	Combatant Status Review Tribunal
CWID	Coalition Warrior Interoperability Demonstrations
DARPA	Defense Advance Research Projects Agency
DCA	defense critical asset
DCIP	Defense Critical Infrastructure Program
DCR	DOTMLPF Change Recommendations
DDS	distributed denial of service
DE	directed energy
DHS	Department of Homeland Security
DHS/EPR	Department of Homeland Security, Emergency Preparedness and Response Directorate
DHS/IAIP/NCS	Department of Homeland Security, Information Analysis and Infrastructure Protection Directorate, National Communications System
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DIME	diplomatic, information, military, and economic
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DMAT	Disaster Medical Assistance Team
DNI	Director of National Intelligence
DOC	Department of Commerce
DOD	Department of Defense
DOD/USACE	Department of Defense/U.S. Army Corps of Engineers
DOE	Department of Energy

DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel and facilities
DOT&E	Director, Operational Test and Evaluation
DSA	Defense Security Agency
DSB	Defense Science Board
DT&E	developmental test and evaluation
DTRA	Defense Threat Reduction Agency
ED	U.S. Department of Education
EEI	elements of information
EFP	explosively formed penetrators
EMAC	Emergency Management Assistance Compact
EMP	electromagnetic pulse
EMT	emergency medical technician
ENC	electronic navigation charts
EOD	explosive ordnance disposal
EUCOM	United States European Command
FBI	Federal Bureau of Investigation
FDCE	Federated Development and Certification Environment
FEDOS	Federation of Systems
FEMA	Federal Emergency Management Agency
FID	p 77 chap 6
GCC	Government Coordinating Council
GIG	Global Information Grid
GPS	global positioning system
GWOT	global war on terrorism
HAE-UAV	high-altitude, long-endurance unmanned aerial vehicle
HANE	high altitude nuclear explosion
HAZMAT	hazardous materials

HE	high explosives
HHS	Department of Health and Human Services
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HN	host nation
HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSPD	Homeland Secretary Presidential Directive
HUD	Department of Housing and Urban Development
HVAC	heating, ventilation, and air conditioning
IAEA	International Atomic Energy Association
IA&I	Information Assurance & Interoperability
IC	intelligence community
ICP	Incident Command Post
ICS	Incident Command System
IED	improvised explosive device
IEMS	Integrated Energy Management System
IIWG	Interagency Infrastructure Working Group
IMU	inertial measurement unit
ISAC	Information Sharing and Analysis Center
ISR	intelligence, surveillance, and reconnaissance
JCIDS	Joint Capabilities Integration and Development System
JIATF	Joint Interagency Task Force
JIC	Joint Integrating Concept
JFC	Joint Forces Commander
JFCC-NW	Joint Functional Component Communications for Network Warfare
JFCOM	Joint Forces Command
JFO	joint field office
JFT-GNO	Joint Task Force-Global Network Operations
JNTC	Joint National Training Capability
JOpsC	Joint Operations Concepts
JPEO	Joint Program Executive Office

JWID	Joint Warrior Interoperability Demonstration
LEO	lower earth orbit
LIDAR	light detection and ranging
LRASCM	long-range anti-sub/ship criuse missile
LRSAM	long-range surface-to-air missile
LTA-UAV	lighter-than-air unmanned aerial vehicle
MANPAD	man-portable air defense system
MCA	Military Commissions Act
MCP	mobile command post
MEFEx	Middle East Force Exercise
MOPP	mission oriented protective posture
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NCCC	National Communications and Coordination Capability
NCO	non-commissioned officer
NCPC	National Counterproliferation Center
NDMS	National Disaster Medical System
NetWarCom	Naval Network Warfare Command
NIC	National Intelligence Council
NIMS	National Incident Management System
NIPC	National Infrastructure Protection Center
NIPP	National Infrastructure Protection Plan
NORTHCOM	Northern Command
NNBIS	National Narcotics Border Interdiction System
NRP	National Response Plan
NSA	National Security Agency
NSC	National Security Council
NT-ISR	non-traditional intelligence surveillance and reconnaissance
NYPD	New York Police Department
OCONUS	outside continental U.S.
ODUSD (LM&R)	Office of Deputy Under Secretary of Defense for Logistics and Materiel Readiness

OEF/OIF	Operation Enduring Freedom/Operation Iraqi Freedom
OJCS	Organization of the Joint Chiefs of Staff
ORS	operationally responsive space
OSD	Office of the Secretary of Defense
OTA	Operational Test Agency
OT&E	operational test and evaluation
OTH	over the horizon
OUSD (AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology & Logistics
PACOM	Pacific Command
PLA	People's Liberation Army (China)
QDR	Quadrennial Defense Review
RAIDRS	Rapid Attack Identification Detection Reporting System
RDD	radiation dispersal devices
RF	radio frequency
RSOI	reception, staging, onward-movement and integration
SAG	Studies and Analysis Group
SAM	surface-to-air missile
SCADA	supervisory control and data acquisition
SCC	Sector Coordinating Council
SCC-WMD	Strategic Command Center for Combating WMD
SLOC	strategic lanes of communication
SOF	special operations forces
SOUTHCOM	Southern Command
SPOD	sea port of debarkation
SSA	sector-specific agency
SSN	Space Surveillance Network
SSP	sector-specific plan
STRATCOM	United States Strategic Command
SWET	sewer, water, electricity, and trash
TCA	Task Critical Asset
TERCOM	terrain contour matching

TIC	toxic industrial chemicals
TRANSCOM	Transportation Command
TSA	Transportation Security Administration
UAS	unmanned aerial system
UFAC	Underground Facility Analysis Center
USA	United States Army
USAF	United States Air Force
USCG	United States Coast Guard
USDA	United States Department of Agriculture
USDA/FS	United States Department of Agriculture Forest Service
USD (AT&L)	Under Secretary for Defense for Acquisition, Technology and Logistics
USD (I)	Under Secretary for Defense for Intelligence
USD (P)	Under Secretary for Defense for Policy
USD (P&R)	Under Secretary for Defense for Personnel and Readiness
USMC	United States Marine Corps
USN	United States Navy
WMD	weapons of mass destruction
WTRAC	WMD Threat Research and Analysis Center

Future of War

Technology

Nuclear Proliferation

Domestic Catastrophe

Deployment and Resupply

Intelligence

Asymmetric Counterforce

Strategic Communication