Surprise Is Inevitable; Vulnerability Is Not

Improving the Defense Department's Readiness to Address Key Areas of Potential Surprise

A Report of the CSIS New Defense Approaches Project

PRINCIPAL AUTHORS
Maren Leed
Hilary Price
Tara Murphy

CONTRIBUTING AUTHOR
Becca Smith

June 2010

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Surprise Is Inevitable; Vulnerability Is Not

Improving the Defense Department's Readiness to Address Key Areas of Potential Surprise

A Report of the CSIS New Defense Approaches Project

PRINCIPAL AUTHORS
Maren Leed
Hilary Price
Tara Murphy

CONTRIBUTING AUTHOR
Becca Smith

June 2010

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

In an era of ever-changing global opportunities and challenges, the Center for Strategic and International Studies (CSIS) provides strategic insights and practical policy solutions to decisionmakers. CSIS conducts research and analysis and develops policy initiatives that look into the future and anticipate change.

Founded by David M. Abshire and Admiral Arleigh Burke at the height of the Cold War, CSIS was dedicated to the simple but urgent goal of finding ways for America to survive as a nation and prosper as a people. Since 1962, CSIS has grown to become one of the world's preeminent public policy institutions.

Today, CSIS is a bipartisan, nonprofit organization headquartered in Washington, D.C. More than 220 full-time staff and a large network of affiliated scholars focus their expertise on defense and security; on the world's regions and the unique challenges inherent to them; and on the issues that know no boundary in an increasingly connected world.

Former U.S. senator Sam Nunn became chairman of the CSIS Board of Trustees in 1999, and John J. Hamre has led CSIS as its president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed in this publication should be understood to be solely those of the author(s).

Center for Strategic and International Studies
1800 K Street, N.W., Washington, D.C. 20006
Tel: (202) 775-3119
Fax: (202) 775-3199
Web: www.csis.org

CONTENTS

Acknowledgments iv

Executive Summary v

Introduction 1

Study Methodology 1

1. Trends and Surprises 3

Summary of Trends and Surprises 3

Main Strategic Drivers in the Literature 4

Surprises in the Literature 6

Illustrative Scenarios 8

Summary 14

2. Capabilities and Gaps 15

Capability Gaps 16

Additional Areas of Interest 19

3. Mitigating or Preventing Surprises 22

Cross-cutting Options 22

Improving Readiness for Specific Gaps 23

Conclusion 26

Appendix A: Bibliography 27

Appendix B: Roundtable Participants 40

About the Authors 41

ACKNOWLEDGMENTS

The authors would like to thank a number of people who made this project possible. First and foremost, the team is indebted to its collaborators at the Office of the Under Secretary of Defense for Personnel and Readiness, led by Mr. Joe Angello. Within that office, Colonel Simon Goerger (U.S. Army) was an invaluable asset in the realization of this study.

A number of CSIS staff members were invaluable along the way, including Clark Murdock, Nathan Freier, Rick "Ozzie" Nelson, and several of the 2009–2010 CSIS Military Fellows. We owe a special thanks to several: Commander Douglas Fears (U.S. Coast Guard); Lieutenant Colonel Donald Dellinger (U.S. Army National Guard); Captain John Griffin (U.S. Navy); Lieutenant Colonel Glenn Guenther (U.S. Marine Corps); Lieutenant Colonel Ricky Rupp (U.S. Air Force); Major Lance Rosa-Miranda (U.S. Air Force); and Colonel Jeffery Vuono (U.S. Army). We also relied upon the expertise of CSIS colleagues Josh Hartman, Major Tom Hurley (U.S. Army), Margaret Taylor (Department of State), Jennifer Cooke, and Richard Downie, all of whom were generous with their time and knowledge. Craig Cohen was a patient and helpful resource who read multiple drafts of this document and vastly improved the final product. We owe a special word of thanks to the experts who attended our workshop in January 2010; they are listed in Appendix B. The few who are not currently involved in thinking through similar issues for a variety of organizations have spent substantial time doing so in past positions, and collectively they represented a wealth of experience and expertise. We also benefitted immensely from the thoughtful contributions of Captain Sean Buck (U.S. Navy) of U.S. Joint Forces Command and Brigadier General Robert "Woody" Nolan (U.S. Air Force) of U.S. Northern Command. Finally, interns Meg Giles, Raphael Marcus, and John Warden, who assisted in this project, were a tremendous help at every stage of the process.

EXECUTIVE SUMMARY

The Department of Defense's (DoD's) mission to protect the nation necessitates its leaders' concern about the military's readiness for a vast and expanding range of missions. These concerns are heightened in the midst of two ongoing campaigns in Iraq and Afghanistan and within the context of a world that is increasingly complex. To their credit, DoD leaders continue to seek insight from both inside and outside the department about areas of potential vulnerability; this study is one such effort.

In Fall 2009, the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD (P&R)) asked CSIS to undertake a six-month assessment of DoD vulnerabilities to events that might occur in the next 5 to 10 years. As described more fully below, the study team employed a three-step approach to meet this charter: (1) identify possible areas of surprise;[1] (2) estimate the types of military capabilities addressing such surprises might require; and (3) compare those demands to DoD's current capabilities to identify potential gaps. The report concludes with a broad discussion of those gaps and some considerations for DoD leaders going forward as they seek to address them.

As its conceptual starting point, the CSIS study team took the basic framework DoD uses in its "Trends and Shocks" process. Begun in 2006 in the Office of the Under Secretary of Defense for Policy (OUSD (P)), Trends and Shocks is essentially a horizon-scanning exercise that examines broad global trends (e.g., economics, demographics, and technological advances) and then seeks to identify the defense implications of shocks that might arise within a given trend or as multiple trends converge. Because organizations are frequently prone to bias (both conscious and unconscious), however, the study team began its effort with an independent assessment of potential near- to mid-term threats and challenges, as well as the broader trends underlying them.

This survey, drawn from a wide range of literature and interactions with experts, revealed dozens of postulated threats, described at varying levels of specificity. The study team synthesized these threats into broad categories and then applied three criteria to further refine a subset to be examined in greater depth. The first criterion was difference, or the degree to which the threats departed from those the subject matter experts involved in the study deemed already firmly ensconced in DoD planning processes. The second criterion was pervasiveness, or threats that were identified as significant by multiple experts. The third criterion was increasing likelihood. When the team examined the trends shaping the evolution of various threats, priority was given to the challenges that strategic drivers indicate are becoming more probable and thus worthy of addi-

1. As is explained more fully in chapter 1, the term "surprise" is used throughout this study to mean unanticipated events that are generally consistent with broader trends in governance, economics, demographics, etc. "Shocks," on the other hand, is used to describe events that result in major discontinuities along a trend line—for example, a major financial crisis that puts economic growth projections on a fundamentally different trajectory than had been expected.

tional attention. Application of these three filters resulted in six broad threat categories: (1) state collapse; (2) large-scale chemical, biological, radiological, or nuclear (CBRN) events, either within or outside the United States; (3) technological surprises; (4) unrestricted (i.e., primarily non-military) warfare; (5) cyber attacks; and (6) conflicts over increasingly scarce natural resources. These categories are not necessarily mutually exclusive. For example, while some experts envisioned military operations solely aimed at restoring order in a collapsed state, others foresaw DoD conducting such missions in a state that had suffered a chemical attack or that was experiencing widespread internal conflict over water supplies. Because each area reflects threats that have not been DoD's principal focus and are also becoming more likely, they represent potential surprises to the department worthy of further examination.

Within the six categories of potential surprise, the study team sought to identify areas where DoD might improve its readiness posture. This required envisioning, with some degree of fidelity, how specific missions might unfold. Using existing scholarship as a foundation, the team developed six representative scenarios, each incorporating one or more threat categories, as a means to identify capabilities DoD might require to successfully address potential surprises.

The scenarios were a necessary step to ground projections of potential DoD needs. The team was mindful, however, that positing the evolution of future conflicts inevitably involves some risk of implausibility that could undermine the overall credibility of the resulting analysis. Thus, the team sought to strike a difficult balance. On the one hand, the scenarios had to be detailed enough to support basic judgments about associated military needs. On the other, they had to be sufficiently general to avoid features that might strike experts as improbable and distract from the principal intent. Finding this "sweet spot" is an impossible task and one that the study team does not purport to have attained within any given scenario. The scenarios are sufficiently varied and realistic, however, that the resulting capability requirements are robust in the aggregate.

The team thus relied on the scenarios as a basis for framing the various capabilities DoD might demand for a range of surprises. Estimating the supply of those capabilities required detailed subject matter expertise and access to a variety of information sources not universally available to the public. Therefore, the CSIS team sought information about DoD's current capability levels from the study's sponsor. Using input from experts in each of the four military services, OUSD (P&R) provided an independent assessment of DoD's capabilities across a range of military missions that might be conducted in a variety of different physical environments (e.g., in space or in mountainous terrain). The study team then took these judgments about the "supply" of various capabilities and compared them to the "demands" suggested by the scenarios.

This comparison led to the identification of seven gaps in which DoD's current or planned capabilities may not be sufficient to address challenges that appear to be well within the realm of possibility in the next 5 to 10 years. The underlying trends suggest that these challenges are becoming increasingly likely, though to what degree is difficult to predict. Given this uncertainty, the study team prioritized the gaps relative to their probable consequences. Greatest concern was given to enemy actions that would likely produce large numbers of casualties. Second and tertiary priorities were given to actions that might result in widespread civil disruption or interference with the conduct of military operations. This logic produced the following list of capability gaps:

1. Insufficient ability to operate in contaminated environments;
2. Insufficient capacity to conduct computer network operations;

3. Inability to adequately anticipate or respond to attacks in space;
4. Shortfalls in the intelligence workforce;
5. Inability to achieve spectrum control;
6. Inability to definitively attribute enemy actions; and
7. Inadequate legal frameworks.

Not surprisingly given an increasingly interconnected world, none of these gaps represents challenges unique to the Defense Department. Nor is DoD likely to be solely responsible for (or even necessarily the lead agency in) addressing each of them. For many of the gaps, the most valuable capability improvements could likely be made by other elements of the U.S. government (USG). However, there are steps that DoD could consider that might further improve its capabilities in each area. These include updating personnel authorities, leveraging high-level games and exercises, relying more heavily on strategies aimed at redundancy in the space and cyber realms, continuing to encourage widespread collaboration by intelligence analysts, and ensuring organizational structures remain aligned with rapidly evolving warfighting environments.

Surprise is inevitable; perhaps even more so in a political and bureaucratic system designed to guard against decisive, far-reaching actions. And while the future cannot be known, policymakers must make some assumptions about its course in order to guide their actions and allocate resources. Deliberate attempts to understand areas of potential vulnerability can significantly improve the information available to those policymakers, and the purposeful inclusion of "outsiders" as a hedge against conscious and unconscious biases is likely to even further enhance the result. This study aims to contribute to this objective. Its findings seek to shore up DoD's capacity to shape or respond to potential surprises, thus enhancing the department's readiness for the future.

INTRODUCTION

As Danish physicist Niels Bohr reportedly said, prediction is very difficult, especially if it's about the future. Unfortunately, difficulty does not relieve policymakers of the task of taking daily decisions that are based, both implicitly and explicitly, on assumptions about how events will unfold. While there are countless methods used in both the private and public sectors that seek to better frame those decisions, one that the Department of Defense (DoD) has recently adopted involves a more deliberate review of strategic trends and the potential shocks that might affect those trends. Thus far, DoD's analytic process known as "Trends and Shocks" has provided useful insights into the defense implications of events that could have a sudden and disruptive impact on U.S. national security priorities, up to and including those events examined as part of the 2010 Quadrennial Defense Review (QDR). This study is an effort to complement and expand upon that work, focused on identifying potential areas of particular vulnerability where DoD's readiness might be enhanced.

Even a cursory review of many strategic trends clearly demonstrates that the potential for surprise is real and growing, increasing the premium on developing robust approaches to managing the associated risk. The amount of scholarship, reflection, and formal documentation on future threats to global and U.S. national security is prodigious. Feasibility constraints forced the CSIS study team[1] to make a number of decisions about this study's scope. Two are particularly worthy of note. First, the study focuses on events that may occur within the next 5 to 10 years. This period extends beyond the near future that tends to dominate policy debates, but it is still within the time frame covered by DoD resourcing processes. Second, our approach required some assessment of DoD's actual level of preparedness across a wide-ranging set of defense capabilities. The CSIS team lacked the resources to conduct such an assessment on our own; instead, our sponsor (the Office of the Under Secretary of Defense for Personnel and Readiness Division [OUSD(P&R)]) provided that assessment. We took those judgments at face value.

Study Methodology

The fundamental aim of this study—to identify currently unforeseen or underappreciated events that could have a sudden and disruptive impact on U.S. national security—led the study team to focus on challenges that, for political, bureaucratic, cultural, or other reasons, have traditionally been underemphasized within DoD's normal planning processes. We relied on three primary information sources to inform this alternative view: a far-reaching literature review, an expert workshop, and a series of in-depth interviews.

1. Members of the team include Maren Leed, Clark Murdock, Hilary Price, Tara Murphy, Nathan Freier, David Sokolow, Becca Smith, and Meg Giles.

Initially, the study team conducted an extensive review of the business, economic, scientific, social science, and other literature addressing the prominent features of the future global environment. This review covered over 100 official government documents, books, articles, and monographs (see the bibliography in Appendix A for the full list of works included). In January 2010, shortly after the literature review and preliminary analysis were completed, the study team held a workshop with defense and planning experts. The primary purposes of the workshop were to vet the initial findings from the literature review and to refine the study methodology. Throughout the project, the CSIS study team held informal consultations with former senior national security officials, including Harold Brown, former secretary of defense; Zbigniew Brzezinski, former national security adviser; and Brent Scowcroft, former national security adviser. The team also relied on input from the 2009–2010 CSIS military fellows and military officers assigned to U.S. Joint Forces Command and U.S. Northern Command.

Drawing primarily from the literature review in the first phase of the analysis, the CSIS team derived broad categories of potential threats that the United States might face in the next decade; these were later refined into more specific military missions. The team also identified features of possible military operating environments that would have a substantial impact on the types of capabilities DoD might require (in terms of materiel, people, or authorities).

During the second phase of the project, the team further developed the missions and environmental features into scenarios in an effort to hone in more directly on specific capability needs. The scenarios represent a range of potential circumstances that highlight particular areas of possible vulnerability to DoD. In some cases this vulnerability may be the result of a deliberate decision about where to accept risk; in others it may reflect undervaluation or lack of appreciation of the risks involved.

The final phase of the analysis involved identifying the capabilities the Defense Department would require across the scenarios, which, when compared to DoD's assessment of what it in fact possesses, resulted in the identification of several critical gaps. The team then developed options for DoD to consider that might further enhance its readiness posture relative to those gaps.

The remainder of this report proceeds in three chapters. Chapter 1 summarizes the main threats or potential surprises identified from the literature and expert discussions; describes the scenarios developed to reflect those surprises; and examines the main trends driving them. Chapter 2 compares the military requirements from the scenarios to OUSD (P&R)'s estimation of DoD's capabilities on hand and derives the associated capability gaps. Chapter 3 discusses ongoing efforts within DoD that relate to the gap areas and offers suggestions that might further enhance the department's readiness in key capability areas.

1 TRENDS AND SURPRISES

The literature review, augmented by interviews and a roundtable with numerous experts, was the initial step in our analysis. The first section of this chapter describes the overarching themes and categories of potential surprises that emerged from that effort. The second section lays out the scenarios the study team developed based on those surprises. The last section provides an overview of the main strategic drivers behind them.

Summary of Trends and Surprises

The key objective of this study was to conduct an independent assessment of potential shocks or surprises, in order to present an additional and potentially contrasting view to ongoing processes within the U.S. government (USG). Our initial starting point was a comprehensive survey of the relevant literature, deliberately focused on areas that might normally fall outside of a defense-focused effort. The review was intended to help us better understand how different disciplines are viewing key trends and possible shocks, as well as to help us identify potential areas of surprise that could have implications for DoD. In this way, we sought to give equal or even greater attention to those security challenges considered nontraditional but that might place very real and significant future demands on the Defense Department. Therefore, in addition to surveying USG and DoD documents, our review spanned the worlds of business, natural science, and technology, as well as the work of a number of leading strategic thinkers and futurists. In order to ensure we had a firm understanding of how the broader national security and defense communities also view the same issues, we reviewed numerous key U.S. strategic documents, to include recent National Security, National Defense, and National Military Strategies; the National Intelligence Council's *Global Trends* studies; the 2001, 2006, and 2010 Quadrennial Defense Reviews; and the 2008 Joint Operating Environment. Our review also included multiple government-sponsored outside analyses, some of which were explicitly designed to seek international perspectives on these issues.

One general observation that emerged from our literature review was that there is far greater commonality in the trends and surprises across a wide range of disciplines than the study team had anticipated. There are a number of potential explanations for this finding. One is that, despite its complexity, there truly is a broad-based general consensus about the future. A second possibility is that this consensus results from some sort of collective "failure of imagination" or "groupthink" that could be caused by editorial or cultural bias or some other subconscious filter.

Secondly, as a general characterization, most of the materials we examined fell into one of two broad categories. Either they are relatively high-level or general discussions of one or more trends, or they are relatively narrowly focused on concrete manifestations of a given problem set as it relates to the military or DoD specifically. Few works we read spanned the full conceptual spectrum from trends to a range of potential outcomes and/or shocks or surprises and then to a defense-

relevant end. This suggests that there may be room for additional future analysis to help amplify the "middle ground" between one or more trends and concrete DoD implications.

Main Strategic Drivers in the Literature

Based on our analysis, four strategic drivers or trends are most directly salient to the missions DoD might be expected to conduct over the next 5 to 10 years. They are demographics, economics, governance, and science and technology. Each is briefly summarized below.

Demographics

The broad trends in birth rates, population age, and migration are inextricably intertwined with other key strategic drivers, particularly economics. Broadly speaking, the future portends a continued shift in population density and youth from the developed to the developing world.[1] According to December 2009 U.S. Census figures, virtually all population growth over the next 15 to 20 years is expected to occur in Asia, Africa, and Latin America, with India maintaining the lead.[2] Many of these regions already suffer from shortages in clean water and other basic resources, and these strains will likely increase.

Social welfare systems are also projected to come under increasing strain, both in developing states with much larger populations to support and in most Western, developed nations whose populations are projected to age significantly.[3] Migration patterns, which typically mirror economic opportunity, are expected to continue to exhibit a shift from rural to urban areas. Internationally, increasing economic opportunities in the developing world may result in fewer migrants to the West and more south-to-south movement. Youth bulges in many Middle Eastern countries, if not coupled with economic opportunities, may increase the impetus for migration.

Economics

While economic fortunes seem most vulnerable to permutation, most experts project an eastward shift in economic might over the next 15 to 20 years. Bolstered by an expanding middle class, China and India are expected to play increasingly dominant roles. Capitalizing on rising youth populations will require developing nations to invest in education and workforce development;[4] if they do, significant long-term growth could result. Even so, almost two-thirds of the world is projected to remain in poverty two decades hence.

At the national level, state control of businesses and assets is experiencing a global resurgence

1. Jack Goldstone, "The New Population Bomb: The Four Megatrends That Will Change the World," *Foreign Affairs* 89, no. 1 (2010).

2. National Intelligence Council, *Global Trends 2025: A Transformed World* (Washington, D.C.: U.S. Government Printing Office, 2008), vii, 19, http://www.dni.gov/nic/NIC_2025_project.html.

3. Populations are aging in virtually every country—though very gradually in youth bulge countries—but North America and Europe are expected to maintain the highest percentages of persons aged 65+ in 2030. See Table 2-5 and Figure 2-25 in Wan He, Manisha Sengupta, Victoria A. Velkoff, and Kimberly A. DeBarros, U.S. Bureau of the Census, *65+ in the United States: 2005*, Current Population Reports (Washington, D.C.: U.S. Government Printing Office, 2005), 23–209, http://www.census.gov/prod/2006pubs/p23-209.pdf.

4. National Intelligence Council, *Global Trends 2025*, 64.

in the form of state capitalism.[5] In the next two decades, states are expected to continue hybrid market policies to benefit national welfare and state (or ruling party) finances. China and other wealthy, energy-rich states, such as Russia, are using sovereign wealth funds to finance domestic and foreign investment. The ability of these nations to continue to exercise economic leverage, although subject to some variation in price, is likely to persist as current alternative energy technologies are insufficiently mature to supplant fossil fuels in the near term.[6] It remains possible that an alternative source, such as solar power or shale gas, could emerge more quickly. Most experts, however, believe fossil fuels will remain the dominant energy source for at least the next 15 years. Unless such a breakthrough dramatically reduces U.S. exposure to international energy markets, the United States is increasingly likely to face adversaries able, through economic influence and might, to effectively undermine U.S. military advantages.

Governance

As the world has become more connected, the declining salience of the state has become a much-noted casualty. Expanding power for individuals and groups has come at the expense of the state and, in turn, the international system built upon a state construct. The degree to which national structures are challenged varies from state to state, but at least one clear implication for U.S. armed forces is the challenge of dealing with power sources outside of existing legal and organizational mechanisms. The multiplicity of players, many with separate objectives and values, vastly complicates almost every military mission. The same is true for the U.S. government as a whole, which must confront expanding sources of conflict with an architecture designed for a much more simplistic era. Outdated legal and political structures, both nationally and globally, are particularly problematic for Western nations grounded in law and federalism.

Science and Technology

Trends in science and technology continue to reflect the double-edged sword of opportunity and vulnerability. Advances in information technology (IT) and communications, space, and medicine are perhaps most directly relevant to national security, though in different ways. The United States has been able to exploit the advantages of IT and space capabilities for decades, but as those technologies have become more powerful, less expensive, and more accessible, the United States' relative advantage has decreased. At the same time, many U.S. military capabilities are increasingly reliant on these technologies, resulting in greater vulnerability. Recent years have also seen the development of numerous medical advances that have the potential to positively affect workforce productivity and life expectancy. The potential social and military implications are profound, but whether societies fully embrace them and the challenges they pose socially and ethically may serve as the most significant determinant of their ultimate impact.

As an example of the potential impacts of technology, one of the most influential vehicles for this trend in the next two decades will likely be the smartphone and the technology that builds on it. American Heritage's *Invention & Technology* magazine calls camera phones "the world's

5. Ian Bremmer, "State Capitalism Comes of Age: The End of the Free Market?" *Foreign Affairs* 88, no. 3 (2009): 40–45.

6. National Intelligence Council, *Global Trends 2025*, 44.

best-selling gadgets" and "the most ubiquitous device in history."[7] Smartphones with photo and video capability are likely to remain popular for the foreseeable future, in the developed world and increasingly in the developing world as well. The political, economic, cultural, and military implications of these types of technologies will be dramatic. Amateur cell-phone photos and videos have made headlines in recent years, capturing events such as the hanging of Saddam Hussein, the shootings at Virginia Tech,[8] and the post-2009 election riots in Iran. Camera-phone technology has converged with social-networking and video-sharing Web sites to create a powerful new communication tool accessible even to individuals in more repressive societies. The inclusion of global positioning system (GPS) technology in personal devices has added yet another dimension to this phenomenon.[9] On the positive side, the devices increase the U.S. military's ability to protect and rescue. They may also offer an avenue to target enemies more accurately. And over the long term, they may assist repressed societies toward more open systems of government. On the negative side, analysts and policymakers will be ever more challenged to identify enemies amidst the chatter, protect sensitive information, and disseminate official explanations of U.S. actions and intentions.

Trend Summary

The brief descriptions above capture a small portion of vast literature on the strategic drivers, whose encompassed trends are shaping the future. All are subject to variation, some of which could be extreme. For example, while birthrates suggest a future age profile, illness, natural disaster, or war can dramatically alter those projections. Despite this uncertainty, the trends are typically characterized more by constancy than disruption. We therefore grounded our assessments of potential surprise in a review of the trends that have the most direct impact on the likely missions for U.S. military forces over the next decade.

Surprises in the Literature

While some experts address both trends and more specific threats that might emanate from them, many sources focus on one or the other. There is substantial discussion of potential threats facing the United States and the international community throughout the literature, ranging from the very broad to the specific. Upon further examination, the team observed that almost all of the potential events that authors and experts described were cast as surprises rather than shocks. The distinction is somewhat artificial, but the two terms as used here represent concepts that do differ—and that ultimately describe one of the important parameters of this study. Because most of what we gleaned from our research related to surprise, we focused the remainder of our analysis in that area and did not further examine potential shocks.

To clarify, shocks and surprises both refer to unforeseen events.[10] The fundamental difference is that surprises are events that are generally consistent with current trends, while shocks represent

7. Stewart Wolpin, "The Decade's Top 10 Trends," *Invention & Technology* 24, no. 4 (Winter 2010): 19, http://www.americanheritage.com/articles/magazine/it/2010/4/2010_4_16.shtml.

8. Ibid., 19.

9. Ibid., 27.

10. In a recent report, the Defense Science Board further delineates surprises into two types: "known surprises," or events that are anticipated but which, for a variety of reasons, decisionmakers have chosen not to address; and "surprising surprises," or those events that are truly unexpected. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Capability Surprise: Volume 1: Main Report*,

major departures from or breaks in those projections. As a general rule, the two tend to be described at different levels of abstraction. Surprises, because they are posited within the broad strategic framework that already exists, are more readily amenable to detailed descriptions and require fewer flights of imagination. Shocks, on the other hand, manifest themselves as events with such impact that the slope of a given trend line or lines is altered, requiring greater conceptual openness. Taking the global financial crisis as a recent example, conventional wisdom failed to envision a shock so widespread and dramatic that it would result in significantly lower growth projections for most of the world's economies.

This is just one illustration of how difficult it is to hypothesize about potential shocks in a way that generates broad acceptance. While most people could likely accept the possibility of additional terrorist attacks in the United States (a surprise that would be consistent with a number of observable and broadly appreciated trends), fewer are likely to see as probable, for example, the widespread introduction of a nanotechnology that results in significantly longer life expectancy and the concomitant effects it might have on social and economic structures (shocks). To the extent that shocks *are* imagined, most find it easier to conceive of and discuss them (e.g., a large drop in birthrates or a diplomatic breakdown that results in the implosion of the United Nations) absent a narrative that explains how they emerge. Because this study was shaped by the literature and expert views, and those inputs largely reflected surprises rather than shocks, the analysis that follows shares that same focus. The attention to surprise is not an indication that DoD can or should pay less attention to potential shocks; to the contrary, it may in fact suggest that a detailed investigation of shocks could produce a number of insights obscured by much of the existing literature on this subject. DoD must ultimately concern itself with both surprise and shock; unfortunately, time did not permit an examination of both as part of this effort.

Within the range of events that we did consider, numerous categories of potential surprises emerged. Given the short duration of this study, however, we could not consider them all. The study team thus decided to focus on those threats that met three conditions. The first criterion was difference, or the degree to which the threats being studied depart from those already firmly ensconced in DoD planning processes. Not surprisingly, there were a substantial number that dealt with the poles of the current defense debate about the appropriate balance between major conventional conflicts and counterinsurgency (or irregular warfare). Because both poles are the subject of such intense scrutiny and analysis within DoD, the study team determined that the marginal impact of additional recommendations in these areas was likely to be low. Therefore, we did not include them going forward in the analysis. The same logic applied to terrorism; while it clearly remains a threat and DoD can likely take some steps to improve its readiness to prevent or respond to terrorist events, the topic already enjoys significant attention, and the impact of additional recommendations here was deemed likely to be limited.

The next filter we applied was pervasiveness. While there were some interesting potential challenges raised by just one or two authors, most involved scenarios that were likely to fall outside of our 5- to 10-year time frame or were judged to be so radical that decisionmakers would find them difficult to address. Therefore, the team further limited the types of threats under consideration to those that were mentioned, though possibly in widely varying forms, by multiple authors or experts. The majority fell into six broad categories: state collapse; large-scale chemical, biological,

---

Report of the Defense Science Board 2008 Summer Study (Washington, D.C.: Defense Science Board, September 2009), http://www.acq.osd.mil/dsb/reports/ADA506396.pdf.

radiological, or nuclear (CBRN) events (either within or outside the United States); the introduction of new, unanticipated technologies; unrestricted (i.e., primarily nonmilitary) warfare; cyber attacks; and conflicts over increasingly scarce natural resources. These categories are not mutually exclusive; authors and experts frequently foresaw combinations (e.g., cyber attacks against the financial system as part of an unrestricted warfare campaign, or technological innovations used in a campaign initiated because of conflicts over rare minerals). However, because in theory each of these threats could be manifest in a "pure" form, the team categorized them individually.

There were a few other types of threats that also were raised repeatedly. However, based on an examination of the principal drivers behind various types of threats, the team determined that the six categories above were both the most pressing for DoD and the most likely over the next 5 to 10 years. These six types of surprises, therefore, became the basis for the subsequent phases of our analysis.

Illustrative Scenarios

After identifying the areas of potential surprise, the team then faced the challenge of translating the threats into implied requirements for DoD. This necessitated describing each threat area in sufficient detail to allow the study team to identify the capabilities a DoD response would require. Of course, every mission is different and DoD's role is dynamic, shaped by factors ranging from domestic and international political climates to available lines of communication to enemy behavior and capabilities, all of which also evolve over time. That said, estimates of requirements must be grounded in some approximation of realistic circumstances, which are described in each particular scenario. The study team thus developed six scenarios encompassing the threat categories above.

Positing the evolution of future conflicts inevitably involves some risk of implausibility that could undermine the overall credibility of the resulting analysis. Therefore, we sought to strike a difficult balance between providing enough detail to support basic judgments about associated military needs and making them sufficiently general to avoid features that might strike experts as improbable and distract from the principal intent. Finding this "sweet spot" is an impossible task and one that we do not purport to have tackled successfully in any given scenario. The study team believes, however, that the capability requirements resulting from the scenarios are at a minimum robust in the aggregate.

The scenarios are not intended to be definitive or exhaustive; instead, they are representative of a number of different types of missions and/or circumstances that have been postulated as probable over the next decade and that highlight areas that appear to be underemphasized or oversimplified in traditional defense planning. Basic themes guiding scenario content, and in some cases more detailed specifics, were drawn from the literature review and interviews. For example, many experts raised the possibility of a technological surprise; judgments may differ about the likelihood of the specific surprise incorporated into the scenario (or the country that develops the cited technology), but the probability of a surprise of some nature remains high and—given technological advances, increased information sharing, and economic trends—may be on the rise.[11] The scenarios do not include specific information about locations or particular actors. Such details

11. Many experts focus on particular types of technology when discussing the possibility of surprise. This perspective tends to assume that the capacity to surprise is inherent to the technology itself. However,

are necessary for highly refined estimates of military requirements but were not necessary for the level of analysis in this report. Including them, further, posed the risk of drawing undue attention toward the individual political-military situations in particular countries or regions. While this is an important part of more detailed planning, the aim of this analysis was to explore broad areas of potential vulnerability that DoD could then explore in greater (and likely classified) detail.

The six scenarios below range from pandemics to unrestricted warfare to collapse of a nuclear state. Each scenario describes a basic set of circumstances that leads to an initial commitment of DoD capabilities; further requirements could evolve in a variety of different ways in each particular case. Because of the vast range of potential evolutions, the study team did not attempt to carry the scenarios through to their conclusions; thus, the associated required capabilities are likely to be conservative estimates.

Scenario One: Pandemic

An antibiotic-resistant strain of the plague originates in the slums of a large city and produces a massive and uncontained pandemic.[12] Widespread chaos ensues as the central government is unable to contain the quickly spreading disease. Fear drives tens of thousands to flee toward the borders, bringing the highly infectious disease with them. Within days, the illness has spread to the United States, which is also facing a large influx of refugees at its borders. Border authorities and hospitals are soon overwhelmed. International transportation is shut down or severely restricted across the globe, to include the United States, and domestic forces in multiple nations are employed to prevent unauthorized air and sea access into home countries.

Initially, governors in U.S. border states call upon National Guard forces to assist in managing and containing the health and security challenges associated with the pandemic. The crisis rapidly overwhelms these capabilities, however, and the president, through authorities under the Insurrection Act of 1807, authorizes the use of active component forces to provide border security, logistics, and public health assistance (including the setup of mass quarantine centers and field hospitals), as well as maintenance of order throughout the United States. Despite the relatively quick reaction, however, millions fall critically ill and tens of thousands of Americans die.

As the pandemic continues along its destructive path, overseas criminal networks begin to view the resulting social and governmental chaos as a threat to their operations. Therefore, large-scale drug networks begin shifting production and distribution into the United States. As a result, drug- and gang-related violence skyrockets in a few major U.S. cities, compounding the security challenges for U.S. authorities. To stem the influx of drug producers, the military is charged with conducting offensive counternarcotics operations in the cartels' havens overseas and with providing direct support to state and local agencies combating the networks inside the United States. Air and maritime assets are deployed in support of multiagency counternarcotics detection and monitoring operations.

---

an alternative perspective is that this capacity is *relative* rather than *absolute*. The implications of this difference are discussed in greater detail in the section on technology surprise at the end of chapter 2.

12. This scenario assumes that the disease is transmitted from person to person. It is equally, if not more, plausible that a possible pathogen could be transmitted in other ways, such as through the food or water supplies. The implications for DoD of other transmission methods would likely be significantly different, both in quality and quantity. A more fulsome examination of possible scenarios with disparate transmission methods could therefore be useful as a follow-on effort to this analysis.

At the request of crippled allies, the USG, primarily with military forces, provides humanitarian assistance in the form of medicine, food, and clean water and leads the reconstruction of health care facilities and basic infrastructure as other governments seek to contain the illness and preserve essential services.

Scenario Two: Global Bioterrorist Attacks

Over the course of one week, three bioterrorist attacks take place in major cities around the globe. Artillery rockets loaded with a virus for which there is no vaccine or specific treatment are launched into city centers, causing the outbreak of viral hemorrhagic fever and resulting in tens of thousands of deaths as well as widespread illness. Worldwide panic ensues. The next day a terrorist extremist group claims credit for the attacks and posts the blueprint for weaponizing the virus on multiple Web sites.

U.S. intelligence analysis soon emerges that strongly, but not definitively, suggests that the source of the virus is likely to be a foreign organized crime group that stole the pathogen from a now-closed facility abroad and subsequently sold it on the black market. Without incontrovertible evidence, some governments refuse to take decisive action, and the international response is largely confined to the provision of humanitarian and technical assistance to the affected states. Intense international intelligence efforts are initiated, and the United States deploys special operations forces to locate and secure any remaining biological stockpiles the terrorists might possess. Sensitive missions targeting the implicated criminal organizations are also initiated.

Several days after the initial attacks a large U.S. city suffers a viral outbreak, with similar symptoms and effects. Panic erupts throughout the United States as no one is sure who is responsible. Local and regional agencies move quickly to impose quarantines. Governors in several states deploy National Guard forces to assist domestic agencies with the increasing public health and public safety challenge. The Department of Homeland Security raises the national threat level to "severe," and several steps are taken to increase protection inside the United States. Border security is significantly enhanced, and security forces at all international airports and seaports are augmented with state and federal forces to increase the ability to scrutinize passengers and cargo without severely affecting throughput.

Public hysteria rises to levels that necessitate a U.S. response. U.S. Navy and Air Force aircraft launch precision strikes against additional terrorist sites, and special operations forces conduct assaults on known supporters of the group and its key logistics nodes. After the strikes, forensic analysis indicates that the pathogen used in the United States is from a different strain of the virus than was used in the three previous attacks. The Centers for Disease Control acknowledge that the origin of the U.S. strain was an American university research laboratory.

Scenario Three: Resource Competition

A tenuous cease-fire with insurgent groups in a foreign nation unravels as the central government fails to deliver on promises of job retraining for former members of armed resistance groups and regional development. Disgruntled youth again take up arms, organized by their former leaders, who—angered by the failure of amnesty—have become more militant than ever. A variety of militias within the country unify to launch an orchestrated campaign of attacks on oil installations, sabotage of oil pipelines, and kidnappings of foreign oil workers. The armed groups are able to

restock their armories with heavy weaponry funded by kidnap ransom payments and oil "bunkering," or theft of oil from pipelines. Violent turf battles erupt over control of the lucrative bunkering trade, and scores of people are murdered in the crossfire.

In the absence of any authority with the capacity to reestablish order, and under pressure from the international oil companies to take action, the federal government sends in a national military force to restore order. The national force comes under sustained attacks by heavily armed militia groups and suffers heavy losses. It responds with indiscriminate force, destroying villages accused of sheltering militants and killing and raping civilians. Enraged by the state force's actions, militants armed with rocket-propelled grenades and heavy machine guns stage a coordinated assault on an offshore oil platform, killing a dozen foreign workers, and forcing the remaining workforce to be evacuated. At the same time, a second group attacks an onshore oil storage facility and blows up the pipelines that feed it, causing an enormous oil spill that releases millions of gallons of oil into neighboring waters.

Alarmed by the spike in violence, international oil companies operating in the country announce the temporary closure of their operations and withdraw all foreign workers from the area. Oil production is shut down, causing a sudden rise in petroleum prices on the world market and intensifying pressure on the government to act. The oil spill spreads, causing an environmental catastrophe, and the government's inaction further fuels the rebellion. At the same time, the heavy losses incurred by the national force spark an army revolt. Units refuse to follow orders, and rumors of an impending coup by junior officers begin to surface. Overwhelmed by the multiple crises, the federal government reluctantly calls for international help in restoring order and stopping the environmental damage, which is now threatening neighboring countries.

A UN task force led by the United States is deployed into the region to establish order, stanch the spread of the oil spill, and provide food, water, and medical assistance to the population. UN troops assist host nation forces to secure the borders and limit the uncontrolled movement of displaced persons into neighboring countries, reduce the inflow of arms, and prevent a humanitarian crisis. Shortly after the arrival of military and humanitarian aid, however, U.S.-provided systems are found to be causing interference with civilian cell-phone networks, which are heavily used by both the population and nongovernmental organizations involved in relief efforts. Insurgent groups quickly seek to turn this interference to their advantage, fueling popular discontent by claiming the United States is acting purposefully to monitor and shut down civilians' communications in support of the corrupt and incompetent government. In an effort to avoid further interference, host nation forces adjust their equipment, causing interoperability problems with UN forces that culminate in six casualties due to friendly fire. Insurgents use commercial technologies to further interfere with UN force communications while publicly blaming the resulting challenges on the United States.

Scenario Four: Technology Surprise

The year is 2018. Increased oil and gas exports and the discovery of new reserves of natural resources have enriched a number of foreign nations, some of whom begin investing significant amounts of revenue into high-technology research and development. The United States, on the other hand, has still not fully recovered from the economic crisis of 2007–2009; this and other fiscal pressures have led to significant declining investment in a number of technical domains. Further, dramatic decreases across the board in U.S. defense spending followed the withdrawal of

military forces from Iraq and Afghanistan. As a result, the United States is no longer the world's preeminent leader in defense technology and has a force structure in need of modernization.

Growing budget pressures have increased the premium for the United States to establish basing arrangements around the globe, as the strain of supporting very long lines of communication severely taxes strategic lift capabilities that are fewer in number and have aged. Negotiations over the establishment of a particular base spark a political crisis between the prospective host nation and a resource-rich state with which it has long-standing historic and cultural ties. The crisis quickly escalates, and the larger nation sends military forces into the smaller one as a show of force, claiming the action has been taken at the request of dissident groups whose rights are being violated.

In response, the United States hastily leads the establishment of a coalition force and assumes responsibility for the preponderance of military commitments. Coalition troops meet with initial successes, but operations soon encounter severe complications when communication systems stop functioning, positioning data is inaccurate, and imagery is degraded or delayed. Exploiting the delay, the enemy conducts airstrikes and then moves in ground troops to solidify control over key cities. As coalition forces fight to regain the momentum, U.S. leaders discover that more than half of U.S. and allied satellites have been destroyed or severely damaged. After some analysis, U.S. leaders conclude the scale and nature of the disruptions could only have been intentional, and logic suggests antisatellite (ASAT) microsatellites are responsible, although conclusive evidence is lacking. The United States lacks the ability to quickly regenerate all of its space capabilities and is thus forced to rely on spared commercial satellites and highly unsecure high-frequency radio for communications and intelligence. The United States responds to the attacks in space by elevating its levels of network protection and cyber defenses and by declaring that any further disruption of satellite capabilities will be met with a forceful and unequivocal response.

Scenario Five: Unrestricted Warfare

An unexpected win by a fringe candidate in a nation's presidential election raises strong international suspicions of outside interference. These suspicions heighten as the newly elected president tightens economic ties with his suspected patron government and increases his anti-Western rhetoric. Within the country, protests and large demonstrations break out, with opposition leaders calling loudly for U.S. and international intervention. Pressure on the international community to challenge the election's validity rises as democracy advocates charge that a U.S. failure to do so is a clear demonstration of the erosion of American influence.

To demonstrate commitment to its traditional ally, as well as its continued relevance in the region's affairs, the United States sends aircraft to a neighboring nation and repositions a naval strike group in closer proximity. Major powers in the region make no outward response to the increased and highly visible U.S. military presence. DoD augments this perceived success by launching an information campaign in surrounding countries that carries a message underscoring U.S. interests and its intent to remain present in the region. Public affairs officials in the beleaguered country are successful in surging outreach to journalists before the anti-U.S. leadership clamps down on media.

Over the course of the following month, American attention shifts inward as a series of alarming events occur. These incidents begin with unexpected, repeated, and significant drops in the stock market, which spur fears of another recession. In addition, there are numerous technical fail-

ures and multiple accidents, seemingly inexplicable, on subway systems in multiple cities. Finally, U.S. government leaders publicly acknowledge a notable surge in the number of cyber intrusions and attacks against government networks. Government agencies heighten their cyber defenses and restrict employee access to outside networks. Public frustration and fear is further exacerbated by officials' inability to authoritatively attribute responsibility for these events or even definitively state whether they are related.

As international and U.S. media outlets increase their coverage of the rising tribulations, the American public's faith in government dramatically declines. Executive branch and congressional approval ratings plummet as the media coverage fixates on the government's inability to defend the nation and its allies, let alone uphold its long-stated commitment to the democratic process. Continual stories fuel public anger over taxpayer money being spent to move military forces across the globe while the daily lives of Americans are in disarray. Public debate over the appropriate responses to the foreign election, the events at home, and the broader role the United States should play in the world becomes increasingly polarized and inflammatory. A growing segment of the American public believes, despite the lack of government confirmation, that a foreign power is behind the events taking place domestically. This leads to growing calls for the United States to return all of its deployed forces to the homeland; an equally powerful argument emerges advocating debilitating strikes against the alleged hidden hand overseas. As pressure to take some action rises, the government is consumed by a parallel and equally heated debate over the evidentiary standards required to justify retaliatory cyber attacks or other measures.

Scenario Six: Collapse of a Nuclear State[13]

Increasing tensions within the military and parliament, severe economic instability, and a rising insurgency threaten the already weak civilian government leading one of the world's nuclear powers. Long-standing antagonistic relations between that state and its neighbor add to the pressure. In a seemingly unprompted display of military might, the neighboring country conducts extensive and highly publicized air force drills not far from the shared border. Several days later, coordinated suicide attacks are carried out in the neighboring country's capital, resulting in massive casualties. Violence along the border intensifies as both sides rush forces to the area. Three weeks later, militants attack nuclear facilities within the weak nation. Although they are not successful, the attacks result in the widespread perception, including in the United States, that the nuclear infrastructure is much less secure than previously thought.

U.S. intelligence sources indicate that several high-ranking officers are plotting to take over the weak nation's government. At the same time, elements within the parliament are advocating steps to remove the president from power. U.S. officials hold emergency meetings with Western allies, foreign military elites, and others in the region to determine the best immediate course of action to ensure that U.S.-supported elements within the nuclear nation can reassert control and safeguard the nuclear stockpile. Special operations forces are deployed to assist with securing vulnerable nuclear facilities, but the foreign government insists no additional support is required.

Several weeks of relative calm pass before militants attack and gain entry to a civilian nuclear facility where the weak state's army had recently transported several nuclear weapons components

13. This scenario is based in part on currently unpublished work being conducted by Nathan Freier, senior fellow at CSIS, in support of the Peacekeeping and Stability Operations Institute of the U.S. Army War College.

for assembly in case of war. Ten days later, a 15-kiloton nuclear weapon is detonated in one of the country's major cities, which houses the armed forces headquarters. Tens of thousands of casualties result, to include much of the senior military leadership, and devastation is widespread. The government is overwhelmed and, facing riots and disruption in many other areas of the country as a result, requests immediate assistance from the United States to aid in cleanup and humanitarian assistance. The power vacuum within the nation's army sparks devolution into local factions amidst contests for power between mid-level commanders.

One of the few remaining senior army commanders threatens to launch a retaliatory nuclear attack on the militants' stronghold in the country's north, and the nation descends into a full-scale civil war. In a state of panic over the lack of nuclear command and control, the neighboring government launches several preemptive airstrikes on several auxiliary nuclear facilities, leaving the warheads intact and sparing the people from additional radiological fallout. The United States and its Western allies suspect that weapons proliferation outside the country is highly probable if the situation continues to spiral out of control.

The United States launches multiple airstrikes on suspected militant and terrorist strongholds and sends large numbers of special operations forces to seize control of sensitive sites. In response to informal requests, the United States also sends large shipments of small arms and other weapons, as well as provides air support to remaining domestic forces fighting for control of the capital. A decision on sending in large numbers of ground troops continues to be delayed as the United States seeks to assemble a broad-based coalition of sufficient size and capability to restore stability in a nuclear-contaminated environment.

Summary

While details within the scenarios above may strike some readers as implausible, global trends suggest that, as a whole, the scenarios' key features are becoming more likely. Increasing numbers of treatment-resistant microbes that have mutated in response to the growing availability of antibiotics suggest that large-scale pandemics are more likely to emerge from benign or malicious origins. The threat is compounded when viewed in concert with the rise in massive slums around many major cities as well as the preponderance of global air travel. The spread of advanced scientific knowledge and materials around the globe, coupled with the potential convergence of ideological and criminal networks, makes global bioterrorist attacks, potentially by multiple perpetrators, a growing possibility.

The intersection of governance challenges, information availability, and either increasingly valuable natural resources or highly prized CBRN materials can also pose serious and growing risks to international order. Finally, while the sunset of American power has often been falsely predicted, rising regional challenges are almost inevitable given shifts in demographic and economic weight. That these challenges will increasingly manifest themselves in nonmilitary ways, at least for the foreseeable future, while the United States maintains advantages in most domains, is a logical expectation. The scenarios are not intended to be predictions of how actual events would unfold; instead, they are designed to be representative of the types of threats the United States could reasonably face in the next decade. These threats are becoming more likely given the current trajectory of major trends, a fact that may be receiving less attention than the growing threats warrant in DoD's traditional planning and resourcing processes.

2 CAPABILITIES AND GAPS

A key criterion the study team used to justify its focus on the six threat areas described in chapter 1 was that those areas have received less attention than many others in traditional DoD planning. One test of the validity of this hypothesis is whether a comparison of the types of capabilities needed to address new areas of potential surprise with existing capabilities reveals major gaps. Discontinuities would reinforce this contention, while the finding that DoD is generally well prepared to meet such challenges would refute it.

As the next step in its analysis the study team undertook such an examination, which first involved deriving broad types of capabilities that would be needed in the illustrative scenarios described in the previous chapter. Relying primarily on the subject matter expertise of team members and CSIS military fellows, as well as assessments contained in scenarios with similar elements in the broader literature, the team developed broad estimates of amounts and types of intelligence, combat and logistical forces, equipment, and organizations that each of the scenarios suggested, as well as the legal authorities they might require.[1]

Concurrently, the team asked the study's sponsor, the Office of the Under Secretary of Defense (Personnel and Readiness), to provide an assessment of DoD's capabilities across a range of missions and physical environmental conditions. These judgments were formed independently of the scenarios described above and were intended to reflect broad-based assessments of DoD's capacity. Relying on inputs from subject matter experts from each of the services, the sponsor provided the CSIS team with judgments about the levels of current and planned capabilities for each mission and environment. These two inputs—the demand for DoD capabilities as derived from the scenarios and the projected supply of those capabilities as independently estimated by OUSD (P&R)—provided the basis for the comparison that identified a number of capability gaps.

Before reviewing the gaps in more detail, some additional context is required about how gaps arise and how the ones specifically identified in this analysis should be viewed. Gaps can result from a variety of one or more causes. One is the simple reality that leaders must make tradeoffs within bureaucratic and/or budgetary constraints. This may mean that a gap is fully recognized and appreciated but that, when weighed against all of the other responsibilities and challenges faced by DoD or the expected effort to fix it, a deliberate decision to accept some risk is taken. Another possibility is that a gap is appreciated but that a technical solution to ameliorate it is not yet available. A third possible cause is that the problem is not recognized at all or is fully appreciated only within a community unable to raise it to a level where action might be taken to address it. Determining the basis (or bases) of the gaps we identified here was beyond the scope of this effort.

1. The team is especially grateful to Margaret Taylor and Major Tom Hurley, visiting fellows at CSIS, for their legal expertise in support of this effort. Ms. Taylor is a Council on Foreign Relations International Affairs Fellow from the Legal Office at the Department of State; Major Hurley is a Judge Advocate General officer in the U.S. Army.

However, the fact that most of areas highlighted have been addressed elsewhere indicates that the gaps are known, at least within some elements of the defense community.

As with the scenarios, the gaps raised here are not intended to be exhaustive. Instead they aim to highlight a few areas that are particularly pressing and of interest to OUSD (P&R) and should be viewed in concert with the results of other analyses, especially those that employed different methodologies. In addition, this analysis was conducted at a fairly high degree of generality; each gap could be explored in greater depth and detail in simulations, exercises, and similar efforts. For the purposes here, however, the team aimed to identify broad areas where DoD might usefully take additional steps to increase its resilience relative to particular challenges.

Capability Gaps

The comparative process described above revealed seven major gaps in DoD's capabilities. Some became apparent in specific missions or environments, while others are overarching and resulted in strains evident across multiple scenarios. None is the sole, or even necessarily the primary, purview of the Defense Department. Nor are all of them of equal import. The analysis was constructed to examine challenges that are becoming increasingly likely, though determining by how much was beyond the scope of this effort. Therefore the team relied on judgments about the likely consequence of a successful enemy attack in each area, using a three-stage framework. Highest priority was given to gaps that, if leveraged by an opponent, would likely result in casualties and deaths (the higher the expected number, the higher the priority). Second priority was given to gaps that, if exploited, would likely lead to widespread disruption in the lives of U.S. citizens, some of which could in turn lead to deaths or casualties. Such disruptions might include power outages, manipulation of the financial markets, interruptions of fuel, food, or water supplies, etc. Third priority was given to gaps that, if taken advantage of, would likely have serious consequences for the conduct of U.S. military operations or broader national security interests. These might include actions such as scrambling positioning data, interruptions of logistics flows, rendering certain U.S. military capabilities inoperable, etc. The three consequence categories are not necessarily mutually exclusive (i.e., if an enemy were to disable a key military satellite constellation, for example, the most immediate effect might be on military missions (a priority three concern), but secondary and tertiary effects might extend to serious losses of life (a priority one concern). While such combinations are possible and potentially more likely than not, the study team categorized the gaps according the most obvious direct impact an enemy action might be expected to have. Based on this framework, the resulting capability gaps are as follows:

1. **Contaminated environments:** The scenarios indicated high demand for training and equipment for operations in biological- or nuclear-contaminated environments that likely exceed current DoD capacity. In addition to shortfalls in the *amounts* of such equipment, there may also be gaps in the *types* of gear required to operate in contaminated environments. Because the scenarios were fairly general and the analysis is unclassified, this study cannot speak to that possibility. Notwithstanding this possibility, it is likely that the shortfalls highlighted here extend to chemical- and radiological-contaminated operating environments as well, although they were not explicitly included in this analysis.

   Because of compounding requirements, CBRN (chemical, biological, radiological and nuclear) training and equipment shortfalls are particularly acute in situations where DoD might be

called upon to support other USG agencies, foreign governments, or other organizations in addition to protecting its own forces. There is a set of circumstances for which it is easily imaginable that a DoD response would be an imperative. These include attacks within the United States or, as posited in our scenarios, in locations where potentially even larger threats might emerge if an event is not contained. If the U.S. military must respond, but lacks sufficient equipment to adequately protect the force and/or others critical to the response effort, large numbers of deaths or injuries could result.

2. **Computer network operations:** The mission-specific gap most prominent in our comparison of requirements to DoD's capability levels is in the services' ability to conduct computer network operations (CNO).[2] This gap is one that has been recognized at both the DoD and national levels, and the Defense Department has taken numerous steps in the last few years to remediate it. These actions range from the creation of new organizations (most prominently, U.S. Cyber Command), to adding substantial numbers of new cyber specialists, to drafting cyber doctrine. At the same time, DoD leaders continue to acknowledge that the policy and doctrine to guide CNO capability development continue to lag behind the technology. Developing a full appreciation for the capability needs, let alone setting aside the resources to acquire them, therefore, is unlikely until broader questions about deterrence in cyberspace, thresholds that might constitute an attack, the range of appropriate responses under international law, etc., are answered. Determining the risk associated with our present state, however, is difficult. The shortfalls in the USG's ability to respond to cyber attacks, and DoD's responsibilities as part of that larger effort, would not necessarily lead to casualties. Yet, if large-scale cyber attacks were to occur, they have the very real potential of causing massive civil disruption and certainly could have deleterious effects on the ability of the U.S. military to conduct operations as designed and desired.

3. **Space:** Our analysis clearly identifies shortfalls relating to potential operations in space. As noted above, international authorities governing actions in space are outdated; for example, despite significant technological advances, the primary treaty that continues to govern space conduct today was enacted over 40 ago. Violations of international norms in space carry significant consequences for the United States overall and DoD in particular, given the heavy U.S. reliance on satellites. The increasing dependence of American society, to include the military, on space-enabled communications and data flows leaves the United States vulnerable to enemy actions that could have many of the same effects expected from possible cyber attacks. Should current norms constraining international aggression in space break down, already-acknowledged capability and capacity shortfalls over the next 5 to 10 years would be further compounded.[3] However, developing robust space defenses is also problematic, both technically and politically. Finally, the technical challenges associated with understanding what has occurred in space are substantial and further complicate U.S. policy options. The potential consequences of an attack in space are wide ranging and include major disruptions to critical infrastructure and/or to military command, control, and communications. One factor that might mitigate the impact of space attacks is the possible availability of commercial satellite capacity, which, although it could not fully replicate the loss of military capabilities, could likely fill some of the gap. Given

2. These include computer network attack, defense, and exploitation.

3. General Kevin P. Chilton, commander, U.S. Strategic Command, statement before the House Armed Services Committee, Subcommittee on Strategic Forces, March 16, 2010, http://armedservices.house.gov/pdfs/StratForces031610/Chilton_Testimony.pdf.

this possibility, the study team judged that attacks in space could have more limited effects than similarly aimed cyber efforts.

4. **Intelligence sufficiency:** When viewed in the aggregate, the scenarios suggest that there are likely to be significant strains on both intelligence collection and analysis when DoD forces are engaged in multiple simultaneous and—in particular—dissimilar missions. These challenges are compounded when events occur without much warning and under circumstances where the perpetrators are not clear. Providing strategically and operationally relevant information to national and defense leaders under conditions with multiple actors, when forced to look both forward and backward in time, is likely to require large numbers of highly diverse analysts who are informed by wide-ranging and multisource collection. While DoD should be lauded for ramping up its recruiting efforts to increase its intelligence workforce, whose size was significantly reduced during the 1990s, a notable gap in mid-level personnel exists.[4] The mid-level career workforce is a key contributor to the depth of knowledge within an organization, and its absence in DoD intelligence agencies presents an area of concern.

   The expected effects of this gap and the three that follow are extremely difficult to predict in any general sense; depending on the specific circumstances, the consequences could be relatively limited or fairly severe. Given the range of uncertainty, however, the study team judged that the most obvious and unavoidable effects would principally relate to the conduct of military operations. Using that as the basic premise, challenges in sufficient depth and breadth in the intelligence community were deemed most pressing. This is because such shortfalls were assumed to have the effect of failing to give decisionmakers enough information to make well-informed decisions. This could in turn lead to mission failure, vulnerability to attack from unforeseen avenues, or both, any of which could result in casualties and/or societal disruption, but almost certainly would have a negative impact on U.S. military operations.

5. **Contested or congested spectrum environments:** Another area of concern suggested by our analysis is ensuring that U.S. and coalition forces are able to exert control over the electromagnetic spectrum. This requires ensuring that friendly spectrum use is secure and maintains its integrity while precluding deliberate or commercial interference that might deny, disrupt, or distort information flows. Although not a major feature of our scenarios, DoD's relatively limited and potentially diminishing capabilities in this area[5] suggest the gap here could potentially grow. DoD has recognized the need to take additional action in this area, but if and until those efforts bear fruit, shortfalls in spectrum-related organization, personnel, training, and equipment are likely to continue to present an area of substantial vulnerability for U.S. forces. The most immediate effects of DoD shortfalls in controlling and managing a given frequency environment may not become apparent until military operations commence. Once underway, however, more systemic failures in ensuring adequate spectrum for operations or in "designing out" interoperability problems or system vulnerabilities could lead to increased casualties. Such

4. Former intelligence community chief human capital officer Ronald P. Sanders has discussed the effects that the pre-9/11 hiring freeze have had on the character of the workforce, as well as the demand to reconstitute the workforce that events of the past decade have created. Joe Davidson, "Intelligence community's chief human capital officer to retire," *Washington Post,* January 15, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/14/AR2010011404133.html.

5. These include inventory reductions in various electronic warfare platforms (the more serious consequence of which will be the retirement of the personnel who operated them and the subject matter expertise they possess).

failure could also leave U.S. forces susceptible to either high- or low-end disruptive technologies such as improvised explosive devices (IEDs). As the ongoing conflicts in Iraq and Afghanistan have illustrated, these vulnerabilities can pose tactical, operational, and strategic risks to U.S. objectives and thus could have far-reaching effects.

6. **Attribution:** One of the most troubling consequences of the trends driving globalization and technological advances is the ability of a widening range of actors to mask their activities. This issue of attribution is particularly pronounced in—but not unique to—the cyber domain. As multiple scenarios illustrate, the inability to unequivocally identify who has taken adverse action directly undercuts one area in which U.S. forces have traditionally enjoyed great advantage: speed of response. Further, the United States, as a law-based society, relies on legal structures that assume a relatively high degree of certitude. Meeting that standard is becoming increasingly problematic. Thus, the challenges associated with correctly attributing CBRN, cyber, space, or other types of attacks reflect an area of great vulnerability to surprise. Attribution challenges can be expected to most directly affect the conduct of military operations in at least two ways. First, lack of clear evidence about responsibility would presumably result in longer deliberations and decision timelines about responses at both the domestic and international levels. (The latter is most important in instances where U.S. leaders place a high priority on having potential U.S. actions viewed as legitimate by the majority of the international community.) Second, the absence of certainty (or near certainty) might also affect decisionmakers' risk tolerance and thus restrict the number of response options under consideration. While circumstances could again vary widely, both time delays and restraints on response to enemy actions could have potentially devastating effects on mission success.

7. **Legal authorities:** As noted above, some of the scenarios highlighted areas where international law governing issues such as what constitutes an act of war are inchoate or outdated, especially in the cyber and space domains. Additional domestic legal challenges exist, particularly where U.S. law has failed to keep pace with technical advances, information-based infrastructures, and the increasing overlap of threats such as crime, narcotics, and traditional defense missions. Finally, it is not clear that law and policy fully account for possible frictions between national and state leaders in the particular case of the use of the National Guard. The Defense Department, for example, generally assumes that governors will voluntarily relinquish control of National Guard forces for national missions; this may not always be the case.[6] While these gaps create seams that adversaries have sought and will likely to continue to seek to exploit, in the short term it may be that the implications can be overcome. This is largely based on the assumption that, under the most extreme set of circumstances, U.S. leaders would forgo legal niceties to take whatever actions might seem necessary to prevent major casualties or significant disruptions. This assumption may be faulty, however, and is important enough to deserve further examination, perhaps through historical case studies or in war games.

Additional Areas of Interest

While not a direct result of the team's comparative approach, there were two other areas that emerged during this research that merit particular consideration: the possibility of technology

6. Fran Townsend, former homeland security adviser, "Defending the Homeland" panel discussion, Military Strategy Forum, CSIS, Washington, D.C., June 16, 2009, http://csis.org/event/defending-homeland.

surprise and the increasing probability of conflict in the Arctic. These issues were not included as a formal part of the analysis for a few reasons. In the case of technology surprise, while numerous scholars and experts have posited a huge range of technological "surprises," each is specific enough to preclude the development of a general scenario that would capture broad-based capability requirements. The same challenge exists in attempting to assess DoD's capacity to respond to technology surprise: it depends on the specific technologies in question. These problems are further compounded by the unclassified nature of this analysis. With respect to the Arctic, while the economic, physical, and political dynamic in the region is a topic of increasing attention, again the challenges are specific to that area and not "generalizeable" like the others for which we were able to develop semi-generic scenarios and high-level assessments of DoD capacity. Thus neither issue fits well into the structure of the overall study. However, they both represent areas that DoD may wish to consider further as it thinks about surprise.

1. **Technology surprise:** As noted above, various experts have postulated specific areas of technological advancement that could pose particular asymmetric challenges to U.S. forces;[7] we incorporated one such example (microsatellites) into one of our scenarios. The accelerating pace of technological innovation, coupled with broader trends in globalization, demographics, economics, and commercialization, indicate that the United States will certainly face such asymmetric challenges going forward, though there is much less consensus about the particular form they might take. Considerable attention is given in the literature to potential disruptive technologies emerging in the fields of information technology, biotechnology, and nanotechnology.[8] Yet, it would be shortsighted—and potentially self-defeating—to limit our attention to advancements in these fields alone. The diversity and speed with which individuals and organizations across the globe are developing entirely new technologies or are adapting existing ones for new purposes has created a significant signal-to-noise problem in this area. As the number and type of actors who can acquire or field advanced technology and the availability and scope of dual-use technology with advanced applications, increase, so too does the challenge that the United States faces in avoiding technological surprise. While the pursuit of specific capabilities to counter developments in a given field is necessary, a more systematic approach might also be warranted. Specifically, one author has suggested that the element of surprise is not inherent to a given technology but instead is a *relative* characteristic. That is, U.S. forces are vulnerable to challenge, whether from new technological capabilities or adaptations of old or outdated ones, in areas that they conceive of as secondary or tertiary to their primary missions.[9] Thus the bureaucracy will foster innovation in areas it values but can be caught unprepared in areas it disdains or undervalues. If true, this theory suggests that DoD ought to have at least one component that specifically views areas of vulnerability not through our enemies' eyes but through our own, paying particular attention to those areas that are seen as of lesser import.
2. **Developments in the Arctic:** Driven primarily by climate change and increasing competition for natural resources, all indications suggest that the Arctic will play an increasingly important

7. Some areas from which technology surprise could emerge include biotechnology and genetics, nanotechnology, micro-electromechanical systems, and directed energy.

8. Committee on Defense Intelligence Agency Technology Forecasts and Reviews, National Resource Council, *Avoiding Surprise in an Era of Global Technology Advances* (Washington, D.C.: National Academies Press, 2005), 15.

9. Guatam Makunda, "We Cannot Go On: Disruptive Innovation and the First World War Royal Navy, *Security Studies* 19, no. 1 (January 2010).

role in geopolitics and have significant implications for U.S. national security in the twenty-first century. Receding summertime ice has opened previously impenetrable water channels, offering new opportunities for commercial shipping and fishing, resource extraction, and tourism. Scientists predict that Arctic summers may be ice free by the 2030s,[10] allowing for easier exploitation of the region's rich natural resources, estimated to include around 90 billion barrels of oil.[11] However, increasing competition for access to these resources and passageways is simultaneously heightening tensions in the region. International disagreements on navigational rights to Russia's Northern Sea Route and Canada's Northwest Passage remain unresolved, and an intensification of Russian military activity in disputed areas of the Arctic has elicited sharp criticism from other bordering states.[12] Although risk of direct military confrontation in the region remains low, environmental conditions in the Arctic pose unique technical challenges for many types of DoD equipment. Therefore, if armed conflict of any significant scale were to arise, it might quickly strain DoD's capacity to respond. As DoD and its agency counterparts pay increasing heed to developments in the far north, careful analysis of system vulnerabilities and specialty equipment deserves continued attention.

The judgments above reflect the study team's best estimates about areas of potential surprise. The next and final chapter discusses potential actions DoD might take in order to lower the probability those gaps might be exploited and/or improve its ability to respond if they are.

10. Lance M. Bacon, "Time is now to prep for ice-free Arctic," *Navy Times*, February 2, 2010, http://www.navytimes.com/news/2010/01/navy_arctic_main_013110w/.

11. U.S. Geological Survey, "Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle," USGS Fact Sheet 2008-3049, http://pubs.usgs.gov/fs/2008/3049/fs2008-3049.pdf.

12. Rob Huebert, "Polar frontiers," *Armed Forces Journal*, March 2010, http://www.armedforcesjournal.com/2010/03/4500480.

3 MITIGATING OR PREVENTING SURPRISES

Chapter 2 identified seven areas where DoD may be vulnerable to future surprises. Mitigating or preventing surprises is a highly complex effort that relies on intelligence, equipment, and training, among other things. The study team did not have access to the full range of investments DoD has made or is planning to make in each area and consequently cannot recommend specific steps DoD might take to augment its preparedness. The team has therefore sought only to capture a few thoughts that DoD leaders may wish to consider, in concert with other actions, as they seek to bolster U.S. defenses against widely varying and unpredictable threats. This chapter begins with a discussion of potential changes to policy and investment that might enhance readiness across a number of gap areas; it then turns to alternatives that relate more directly to one specific gap.

Cross-cutting Options

One of DoD's most significant challenges is the need to develop and manage its personnel such that they collectively possess an astounding and growing range of breadth, but also depth, of expertise. The military operating environment is increasingly shaped by rapidly advancing commercial developments that have significant implications for the military's ability to leverage opportunities and defend U.S. interests in spectrum, cyber, space, and intelligence in particular. Bridging the gap between the relatively rigid personnel systems for both military members and defense civilians and the rapidly evolving knowledge in the private sector is likely to become an increasing strain. DoD has sought and been granted authority to launch a number of pilot programs to experiment with allowing service members to take sabbaticals from service, for example. These types of enhanced tools—options that permit greater ease of movement between Active and Reserve and military and civilian status, for example—are an important recognition of the changes not only in the operating environment that the military is likely to face in the future but also of evolving demographic and economic realities for Americans who wish to serve. More flexible policies governing service members' working conditions may increase the amounts and types of expertise DoD can draw upon at short notice, greatly enhancing its overall resiliency. Additional steps in this direction will require close consultation with Congress and careful analysis to avoid unintended consequences, but continued progress could have a profoundly positive impact on the shape and nature of the U.S. military going forward.

At the same time that DoD can take steps to enhance its own capabilities, the probability that it will be acting on its own is diminishing. The scenarios discussed earlier in this report involving space and cyber attack, in addition to those requiring military action within the United States, all serve as illustrations of a national and international legal structure designed for a bygone era. All of these problems involve other U.S. government agencies, at a minimum, and potentially the broader international community. DoD cannot resolve these shortfalls on its own and must

therefore focus its efforts on spurring others to action. As others have noted, interagency and international training and exercises can make important contributions in this area. Not only do they help develop relationships and individual expertise, but they can also serve as a low-risk means for more precisely estimating the range of needs in areas such as medical response or protective gear.

As or more importantly, however, additional senior-level wargames and simulations can serve to highlight major shortcomings in interagency planning, policy, and authority.[1] DoD's ability to affect progress on interagency coordination and cooperation is strongest in areas where it has primary responsibility, but DoD has important equities that extend well beyond those bounds. Exercises can be an effective tool for vividly illustrating the consequences of vagueness in policy or planning and may be one of the most powerful ways for DoD to indirectly generate momentum in areas critical to national security generally, as well as their military-specific components. Organizational theory suggests that the bureaucracy in other agencies may resist prompting by DoD leaders for advances in crucial areas such as cyber, intelligence, CBRN response, and homeland security. If DoD is willing to play a supporting role, but also provide funding and planning expertise for enhanced training opportunities, it may be possible to overcome some of that resistance.

High-level exercises may also be one of the few hedging actions available to address the difficulties surrounding attribution. Although additional tools to forensically determine the origins of CBRN, space, spectrum, or cyber attacks are being pursued, the reality is that this problem is unlikely to ever be fully resolved. Some level of ambiguity is almost certain to exist for at least some types of future attacks. Opportunities for senior leaders to experience that ambiguity in simulations and exercises can help increase their comfort with decisionmaking under such conditions.

Improving Readiness for Specific Gaps

The preceding analysis suggested that DoD could be called upon to provide additional support to other government and/or nongovernment organizations in the case of a CBRN event. While DoD is neither responsible nor resourced for such circumstances, DoD leaders may wish to consider revisiting these constraints. Even if expanding inventories to cover a greater-than-expected military need as a more robust hedge against such possibilities is not possible, at a minimum DoD may wish to determine how rapidly its suppliers could respond if there were a dramatic and sudden increase in the requirement for CBRN equipment.[2] Workforce expertise may represent another opportunity for DoD to shore up its CBRN response capacity. Over time, DoD has become increasingly reliant on contractors to provide CBRN expertise.[3] The significant potential consequences of operating in a dirty environment, coupled with the increasing likelihood that DoD will be called upon to do so, suggests that the Defense Department may wish to consider bringing additional CBRN capacity "in house" as part of its broader effort to "in-source" previously contracted activities.

---

1. For example, while the administration recently released the *National Strategy for Countering Biological Threats*, it does not assign specific responsibilities to federal departments and agencies. Bob Graham and Jim Talent, *Prevention of WMD Proliferation and Terrorism Report Card* (Washington, D.C.: Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, 2010), 6, http://www.preventwmd.gov/static/docs/report-card.pdf.

2. U.S. Government Accountability Office, *Defense Logistics: Lack of Key Information May Impede DOD's Ability to Improve Supply Chain Management*, GAO-09-150 (Washington, D.C.: GAO, January 2009), http://www.gao.gov/new.items/d09150.pdf.

3. Ibid.

In the cyber realm, although DoD has taken multiple steps to address emerging cyber challenges, most agree that still more can be done. DoD has recognized the need to expand cyber expertise[4] and is investing in this expansion. Expanded and more flexible personnel authorities, such as those discussed above, if implemented, would likely add to the effectiveness of these new hires. At the strategic level, however, DoD's efforts remain constrained by a lack of clarity about public expectations. The historical compact between the American citizenry and its government (to include the Defense Department) is ill-suited to cyber realities, and a new understanding about the desired balance between privacy and protection in cyberspace must be forged. To the extent that DoD can contribute to advancing this debate as part of a larger U.S. government effort, it may help bring about greater fidelity about the department' responsibilities in this rapidly evolving domain.

Like cyber, the space domain also is characterized by an accelerating pace of change. Increasing competition in space from both the military and civilian realms is eroding the relative advantage the United States has long enjoyed. While a significant stigma against offensive space action remains, how long this will hold is unknown. This putative restraint becomes even more tenuous as technologies are developed that can mask the identities of possible perpetrators of offensive actions. DoD is pursuing a variety of programs aimed at enhancing and protecting space situational awareness, to include a Space-Based Surveillance System and Tactical Component Network. Continued and stable investment in these types of activities is crucial, but so too is a strategy of resiliency. The short-lived relevance of technologies aimed at denial and advantage necessitates that DoD continue to examine alternative approaches should space be compromised. The most effective space defense may be the ability to rapidly reconstitute in the wake of an attack. While immensely useful in its own right, such a capability may also serve as a deterrent, dissuading potential attackers who perceive diminishing effects of such a challenge.

Redundancy is not likely to be available at prices government can afford, however, which DoD has recognized as it seeks to increase its reliance on commercial satellites. Recalibrating this balance is in turn necessitating a cultural shift away from maximum protection to one of studied and measured risk; for example, it may mean military forces have to consider time as a factor when judging communications security requirements. Security need not always be absolute; if an enemy intercepts communications five minutes after the information is relevant to U.S. operations (rather than never), this may be an acceptable trade for increased speed or alternative pathways. A more nuanced space portfolio, then, will ultimately rest on both more sophisticated consumers and a mix of defense and private-sector assets.

Thinking about surprise can ultimately be reduced almost completely to an intelligence problem. Beyond this strategic concern, this study focused more directly on operational concerns, specifically the stresses associated with providing sufficient information to senior leaders to support decisions on accelerated timelines and relating to multiple missions and/or adversaries. Similar strains have been observed in today's operations: one recent report quoted a senior military commander as saying that the president and other national leaders "are not getting the right information [from the defense intelligence community] to make decisions with."[5] That report attributed the shortcomings not to a lack of information, but to intelligence community attitudes and culture.

---

4. U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C.: U.S. Department of Defense, February 2010), 28, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

5. Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, D.C.: Center for a New American Security, January 2010), 9, http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf.

One means to bridge the gap between intelligence consumers and producers is to conduct additional exercises along the lines of those described above. As intelligence officials have the opportunity to systematically review the types of demands national leaders place on the system in a constructed rather than real-time environment, this understanding may help better align analysis with need.

Despite a number of efforts specifically targeted at reducing the insularity of the intelligence community, this too remains a barrier to more relevant analysis.[6] As Major General Michael Flynn, current intelligence chief for the NATO mission in Afghanistan, recently wrote, intelligence analysts "must open their doors to anyone who is willing to exchange information."[7] This exhortation holds true not only in the villages of Paktia province but in the suburbs of Virginia as well, and while the community has made an effort to increase inputs from open sources, these interactions are rarely systematically integrated into the analytic process.[8] DoD and the broader intelligence community are exploring a range of collaboration tools and other incentives to help break down cultural barriers to broader cooperation. To the extent that they have not already done so, leaders may wish to consider injecting specific collaboration criteria into performance evaluations, as well as the establishment of bonuses or awards for demonstrated collaborative behavior.

Finally, like space, the electromagnetic spectrum is increasingly congested and contested. These twin pressures, one from commercial interests and one from adversaries able to employ a growing array of tools against friendly forces, foretell a rise in frequency of fratricide, confusion, and constraint. The challenges to spectrum extend beyond space and cyber to all of the warfighting domains; thus, failure to take decisive action in this area has the potential to seriously impede defense capabilities over the next decade and beyond. Internal DoD analyses have recognized shortcomings in this area,[9] and studies are underway to examine and resolve complex questions on the boundaries between many overlapping areas and how DoD should best organize to resolve them. These include an analysis of how the military should organize to address joint spectrum concerns, of the boundaries between spectrum and cyber and the appropriate resulting organizational relationships, and of the functions and purpose of information operations. As the Defense Department seeks to clarify these issues, it should include assessments of whether the structures to provide civilian oversight of these activities should also be revised in order to ensure maximum effectiveness and efficiency going forward. And finally, because of the broad implications and widely dispersed bureaucratic equities in cyber, space, and spectrum, the deputy secretary of defense may also wish to consider whether his staff should include some expertise dedicated specifically to those issues in particular.

6. Ibid.

7. Ibid., 23.

8. Monitor 360, *Practical Steps for Improving Intelligence Analysis: Perspectives from Monitor 360* (San Francisco: Monitor 360, March 2009), 5, http://www.360.monitor.com/downloads/ImprovingAnalysisMonitor360.pdf.

9. General Kevin Chilton recently testified that DoD's electronic warfare (EW) Initial Capabilities Document "emphasized the need for focused leadership in the EW area." See General Kevin Chilton, commander, U.S. Strategic Command, statement before the House Armed Services Committee, Subcommittee on Strategic Forces, March 16, 2010.

Conclusion

Predicting the future is an impossible but inescapable task for decisionmakers. For those who support them, continuous evaluation of methods for improving the quality of available information is a basic responsibility. As the world becomes ever more complex, the value of seeking multiple perspectives, including from outsiders, is only increased.

This study, while not definitive or exhaustive, represents one such perspective on areas in which DoD might be vulnerable to surprise over the next decade. Through the use of six scenarios representing a range of threats that are becoming increasingly likely, the study team identified gaps in DoD's capabilities. None of these gaps is novel; all have been previously imagined, and DoD is taking action to address all of them in a variety of ways. That said, there may be additional steps DoD can take to increase its readiness, particularly when they do not require significant additional investment. The suggestions above are not panaceas, and one certainty is that other surprises will emerge. Despite that reality, as DoD considers its activities, the suggestions above are intended to highlight some areas in which DoD might further enhance its overall readiness in the years to come.

APPENDIX A
BIBLIOGRAPHY

Alexandrov, Oleg. "Labyrinths of the Arctic Policy." *Russia in Global Affairs* 3 (July–September 2009). http://eng.globalaffairs.ru/numbers/28/1300.html.

American Enterprise Institute for Public Policy Research. "Gulf of Aden Security Review—February 26, 2010." *Critical Threats* (February 26, 2010). http://www.criticalthreats.org/gulf-aden-security-review/gulf-aden-security-review-february-16-2010

Anderson, Mark T., and Matthew K. McLaughlin. "Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Consequence Management Response Force: The Title 10 Initial Entry Force." *Maneuver Support Magazine* (Summer 2009). http://www.wood.army.mil/engrmag/Maneuver%20Support%20Magazine/PDFs%20for%20Summer%202009/Anderson-McLaughlin.pdf.

Anthes, Emily. "What a Pest: Why the Black Death still won't die." *Foreign Policy*, November/December 2009). http://www.foreignpolicy.com/articles/2009/10/19/what_a_pest?page=full.

Army Environmental Policy Institute. "Climate Change and Army Sustainability." *Army Foresight: Searching for Sustainability* 4.1 (July 2007). http://www.aepi.army.mil/foresight/jul07-ccas.pdf.

———. "Emerging Ecosystem Services and Markets." *Army Foresight: Searching for Sustainability* 3.1 (March 2007). http://www.aepi.army.mil/foresight/mar07-eesm.pdf.

———. "Stability Operations Plans." *Army Foresight: Searching for Sustainability* 2 (August 2006). http://www.aepi.army.mil/foresight/aug06-sop.pdf.

Arnas, Neyla, ed. *Fighting Chance: Global Trends and Shocks in the National Security Environment*. Washington, D.C.: National Defense University Press, 2009.

Axe, David. "War is Boring: Mixed Signals from China Point to Security Dilemma." *World Politics Review* (February 17, 2010). http://www.worldpoliticsreview.com/article.aspx?id=5132.

Bacon, Lance M. "Ice breaker." *Armed Forces Journal* (March 2010). http://www.afji.com/2010/03/4437078.

———. "Time is now to prep for ice-free Arctic," *Navy Times*, February 2, 2010. http://www.navytimes.com/news/2010/01/navy_arctic_main_013110w/.

Barrett, Scott. "Regulating the Global Commons—Part 1." *YaleGlobal* (March 26, 2008). http://yaleglobal.yale.edu/content/regulating-global-commons-%E2%80%93-part-i.

Bert, Melissa, and Mark Schlakman. "Ratifying the Law of the Sea." *Boston Globe*, March 16, 2009. http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2009/03/16/ratifying_the_law_of_the_sea/.

Boot, Max. "China's stealth war on the U.S." *Los Angeles Times*, July 20, 2005. http://articles.latimes.com/2005/jul/20/opinion/oe-boot20.

Bowie, Christopher J., Robert P. Haffa Jr. and Robert E. Mullins. *Future War: What Trends in America's Post–Cold War Military Conflicts Tell Us About Early 21st Century Warfare*. Arlington, Va.: Northrop Grumman Analysis Center, 2003. http://www.northropgrumman.com/analysis-center/paper/assets/future_war.pdf.

Bremmer, Ian. "State Capitalism Comes of Age: The End of the Free Market?" *Foreign Affairs* 88, no. 3 (May/June 2009). http://www.foreignaffairs.com/articles/64948/ian-bremmer/state-capitalism-comes-of-age.

Brewer, Chris. "Maritime Security & Counter-Piracy: Strategic Adaptations and Technological Options." *Journal of Energy Security* (April 23, 2009). http://www.ensec.org/index.php?option=com_content&view=article&id=188:maritime-security-aamp-counter-piracy-stragegic-adaptation-and-technological-options&catid=94:0409content&Itemid=342.

Browne, Marjorie Ann. "The Law of the Sea Convention and U.S. Policy." CRS Issue Brief for Congress. Washington, D.C.: Congressional Research Service, February 10, 2005. http://www.fas.org/sgp/crs/row/IB95010.pdf.

Bueno de Mesquita, Bruce. "Recipe for Failure." *Foreign Policy*, November/December 2009. http://www.foreignpolicy.com/articles/2009/10/16/recipe_for_failure.

Butler, Amy. "2011 Funding Request includes New Sat System." *Aviation Week*, February 11, 2010. http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=defense&id=news/awst/2010/02/08/AW_02_08_2010_p27-202005.xml&headline=2011%20Funding%20Request%20Includes%20New%20Sat%20System.

Carafano, James. "Debating QDR Recommendations for Northern Command." *Security Debrief*, April 2, 2010. http://securitydebrief.adfero.com/2010/04/02/debating-qdr-recommendations-for-northern-command/.

Castelli, Christopher J. "McHale, Lieberman Slam Plan To Shrink Certain Homeland Defense Forces." *Inside the Pentagon* 26, no. 13 (April 2010).

Chabrow, Eric. "Collective Cyber Defense: Int'l Synergy a Must," *GovInfoSecurity.com*, February 15, 2010. http://www.govinfosecurity.com/articles.php?art_id=2201.

Chairman of the Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations (U)*. Washington, D.C.: Joint Chiefs of Staff, 2006. http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf.

———. *National Military Strategy to Combat Weapons of Mass Destruction*. Washington, D.C.: Joint Chiefs of Staff, 2006. http://www.defense.gov/pdf/NMS-CWMD2006.pdf.

Coll, Steve. "The Unthinkable: Can the United States be made safe from nuclear terrorism?" *New Yorker*, March 12, 2007.

Combined Maritime Forces Public Affairs. "New Counter-Piracy Task Force Established." *NAVY.mil*, January 8, 2009. http://www.navy.mil/Search/display.asp?story_id=41687.

Committee on Defense Intelligence Agency Technology Forecasts and Reviews, National Resource Council. *Avoiding Surprise in an Era of Global Technology Advances*. Washington, D.C.: National Academies Press, 2005.

Cook, Robin. "Plague: A New Thriller of the Coming Pandemic." *Foreign Policy*, November/December 2009. http://www.foreignpolicy.com/articles/2009/10/15/plague_a_new_thriller_of_the_coming_pandemic.

Council on Foreign Relations. *Public Opinion on Global Issues: A Web-based Digest of Polling from Around the World*. New York: Council on Foreign Relations, 2009. http://www.cfr.org/think-tank/iigg/pop/.

Courtney, Hugh. *20/20 Foresight: Crafting Strategy in an Uncertain World*. Boston, Mass.: Harvard Business School Press, 2001.

Cronin, Patrick M., ed. *Global Strategic Assessment 2009: America's Security Role in a Changing World*. Washington, D.C.: Institute for National Strategic Studies, National Defense University, 2009. http://www.ndu.edu/inss/index.cfm?type=section&secid=8&pageid=126.

Danzig, Richard. "New Priorities in Bioterrorism: Recommendations for the New Administration." Address for the *Analytic Services Distinguished Speaker Series*, Analytic Services, Arlington, Va., December 1, 2009.

———. *The Big Three: Our Greatest Security Risks and How to Address Them*. New York: Center for International Political Economy, 1999.

Davidson, Joe. "Intelligence community's chief human capital officer to retire." *Washington Post,* January 15, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/01/14/AR2010011404133.html.

Davis, Jacquelyn K., and Michael J. Sweeney. *Strategic Paradigm 2025: U.S. Security Planning for a New Era*. Dulles, Va.: Brassey's, 1999.

Denmark, Abraham M., and James Mulvenon. *CNAS Capstone—Contested Commons: The Future of American Power in a Multipolar World.* Washington, D.C.: Center for a New American Security, 2010.

Dewar, James A. *Assumption-Based Planning: A Tool for Reducing Avoidable Surprises.* New York: Cambridge University Press, 2002.

Dombrowski, Peter. "Alternative Futures in War and Conflict: Implications for U.S. National Security in the Next Century." Occasional Paper. Newport, R.I.: Center for Naval Warfare Studies, April 2000. http://www.au.af.mil/au/awc/awcgate/navy/alt_futures.htm.

Doyle, Jennifer. "Lack of EMS Focus at the National Level Impedes Local Preparedness." *JEMS.com*, March 26, 2010. http://www.jems.com/news_and_articles/articles/us_gets_an_f_in_bioterror_readiness.html.

Economist. "Nuclear's Next Generation," December 10, 2009.

———. "Who runs the world? Wrestling for influence," July 3, 2008.

Editorial. "Obama must pay heed to al-Qaeda's quest for biological weapons." *Washington Post*, February 3, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/02/AR2010020203390.html.

Eggen, Dan, Karen DeYoung and Spencer S. Hsu. "Plane suspect was listed in terror database after father alerted U.S. officials." *Washington Post*, December 27, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/12/25/AR2009122501355.html.

Emke, Jerry. "Trends and Shocks, and the Impact to the Acquisition Community." *Defense AT&L Magazine* 37, no. 1 (2008).

Engelbrecht, Joseph A., Jr., et al. *Alternative Futures for 2025: Security Planning to Avoid Surprise*. Maxwell Air Force Base, Ala.: Air University Press, 1996. http://csat.au.af.mil/2025/a_f.pdf.

Eunjung Cha, Ariana, and Ellen Nakashima. "Google China cyberattack part of vast espionage campaign, experts say." *Washington Post*, January 14, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

Fine Maron, Dina. "Canada Will Use Robot Subs to Map Arctic Sea Floor, Boost Territorial Claims." *New York Times*, February 10, 2010. http://www.nytimes.com/gwire/2010/02/10/10greenwire-canada-will-use-robot-subs-to-map-arctic-sea-f-45098.html.

Fleshman, Michael. "At last, signs of progress on AIDS." *Africa Renewal,* January 2010. http://www.un.org/ecosocdev/geninfo/afrec/vol23no4/progress-on-aids.html.

Flournoy, Michèle. "Rebalancing the Force: Major Issues for QDR 2010." Remarks to the Center for Strategic and International Studies, Washington, D.C., April 27, 2009. http://policy.defense.gov/sections/public_statements/speeches/usdp/flournoy/2009/April_27_2009.pdf.

Flournoy, Michèle, and Shawn Brimley. "The Contested Commons." *Proceedings Magazine* 135 (July 2009). http://www.usni.org/magazines/proceedings/story.asp?STORY_ID=1950.

Flynn, Michael T., Matt Pottinger, and Paul D. Batchelor. *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*. Washington, D.C.: Center for a New American Security, 2010. http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf.

Freeman, Bob. "Conference Addresses Navy's Role in a Changing Arctic." *NAVY.mil*, October 4, 2009. http://www.navy.mil/search/display.asp?story_id=48533.

Freier, Nathan. "Hybrid Threats and Challenges: Describe…Don't Define." *Small Wars Journal*, 2009. http://smallwarsjournal.com/blog/journal/docs-temp/343-freier.pdf.

———. *Known Unknowns: Unconventional "Strategic Shocks" in Defense Strategy Development*. Carlisle, Penn.: Strategic Studies Institute, U.S. Army War College, 2008.

Friedman, George. *The Next 100 Years: A Forecast for the 21st Century.* New York: Doubleday, 2009.

Fukuyama, Francis. *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*. Washington, D.C.: Brookings Institution Press, 2007.

Gates, Robert M. Remarks to Air War College, Maxwell-Gunter Air Force Base, Ala., April 21, 2008. http://www.defense.gov/speeches/speech.aspx?speechid=1231.

———. Remarks to the International Institute for Strategic Studies, Singapore, May 31, 2008. http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1253.

———. Defense Budget/QDR Announcement, Arlington, Va., February 1, 2010. http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1416.

———. "A Balanced Strategy: Reprogramming the Pentagon for a New Age." *Foreign Affairs* 88, no. 1 (January/February 2009). http://www.foreignaffairs.com/articles/63717/robert-m-gates/a-balanced-strategy.

Gettleman, Jeffrey. "Africa's Forever Wars." *Foreign Policy*, March/April 2010. http://www.foreignpolicy.com/articles/2010/02/22/africas_forever_wars.

Gill, Bates, and Martin Kleiber. "China's Space Odyssey: What the Antisatellite Test Reveals about Decision-Making in Beijing." *Foreign Affairs* 86, no. 3 (May/June 2007). http://www.foreignaffairs.com/articles/62602/bates-gill-and-martin-kleiber/chinas-space-odyssey-what-the-antisatellite-test-reveals-about-d.

Goldstone, Jack A. "The New Population Bomb: The Four Megatrends That Will Change the World." *Foreign Affairs* 89, no. 1 (January/February 2010). http://www.foreignaffairs.com/articles/65735/jack-a-goldstone/the-new-population-bomb.

Governmentattic.org. "Reports prepared by US Northern Command (USNORTHCOM) for Congress, 2007 –2009." http://www.governmentattic.org/2docs/NorthcomCongRepts_2007-2009.pdf.

Graham, Bob, and Jim Talent. "H1N1 response shows need for better medical emergency plans." *Washington Post*, January 4, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/01/03/AR2010010301812.html.

———. *Prevention of WMD Proliferation and Terrorism Report Card*. Washington, D.C.: Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, January 2010. http://www.preventwmd.gov/static/docs/report-card.pdf.

Gregory, Shaun. "The Terrorist Threat to Pakistan's Nuclear Weapons." *CTC Sentinel* 2, no. 7 (July 2009). http://www.ctc.usma.edu/sentinel/CTCSentinel-Vol2Iss7.pdf.

Grossman, Elaine M. "Talk of U.S. Plans to Secure Pakistani Nuclear Weapons Called 'Wildly Hypothetical.'" *Global Security Newswire*, June 10, 2009. http://www.globalsecuritynewswire.org/gsn/nw_20090610_2476.php.

Grossman, Marc. "Global Trends for the Coming Decade and the Formulation of U.S. Foreign Policy." Remarks to the National Newspaper Association, Columbia, Mo., March 21, 2002.

Hamilton, John. "Storms in Space Disrupt Travel on Earth." National Public Radio, February 1, 2010. http://www.npr.org/templates/story/story.php?storyId=123111882.

Hammond, Allen. *Which World? Scenarios for the 21st Century*. Washington, D.C.: Island Press, 1998.

Hardin, Garrett. "The Tragedy of the Commons." *Science* 162 (1968).

Hays, Peter L., and Charles D. Lutes. "Towards a theory of spacepower." *Space Policy* 23, no. 4 (November 2007).

He, Wan, Manisha Sengupta, Victoria A. Velkoff, and Kimberly A. DeBarros, U.S. Bureau of the Census. *65+ in the United States: 2005*. Current Population Reports. Washington, D.C.: U.S. Government Printing Office, 2005.

Hersh, Seymour M. "Defending the Arsenal." *New Yorker*, November 16, 2009. http://www.newyorker.com/reporting/2009/11/16/091116fa_fact_hersh.

Hsu, Spencer S. "National disaster exercises, called too costly and scripted, may be scaled back." *Washington Post*, April 2, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/04/01/AR2010040103746.html.

Huebert, Rob. "Polar frontiers." *Armed Forces Journal* (March 2010). http://www.afji.com/2010/03/4500480.

Intergovernmental Panel on Climate Change (IPCC). *Climate Change 2007: Synthesis Report*. Geneva, 2007. http://www.ipcc.ch/pdf/assessment-report/ar4/syr/ar4_syr.pdf.

Javers, Eamon. "Whodunit? Sneak attack on the U.S. dollar." *POLITICO*, October 8, 2009. http://www.politico.com/news/stories/1009/28091.html.

Johnson, Dana J. Remarks at the Air Education and Training Command Symposium, "Policies for a Contested Space Environment," San Antonio, Texas, January 14, 2010. http://spacepolicyonline.com/pages/images/stories/Johnson_-_AETC_Symposium_Remarks_14_Jan_2010_FINAL.pdf.

Joint Chiefs of Staff. *The National Military Strategy of the United States: A Strategy for Today, a Vision for Tomorrow*. Washington, D.C.: Joint Chiefs of Staff, 2004.

Jones, Willie. "Researchers to Report on Nanotechnology Advances." *IEEE*, November 2009. http://www.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute_level1_article&TheCat=2203&article=tionline/legacy/inst2009/nov09/conference.xml&.

Kagan, Frederick W., and Michael O'Hanlon. "Pakistan's Collapse, Our Problem." *New York Times*, November 18, 2007. http://www.nytimes.com/2007/11/18/opinion/18kagan.html.

Kaplan, Sid. "Project Horizon—A new approach to interagency planning." *Federal Times*, February 13, 2006. http://www.epa.gov/OSP/futures/ProjectHorizon.pdf.

Khalilzad, Zalmay, and Ian O. Lesser, eds. *Sources of Conflict in the 21st Century: Regional Futures and U.S. Strategy*. Santa Monica, Calif.: RAND Corporation, 1998.

Korb, Larry, and Michael Kraig. *Strategies for US National Security: Winning the Peace in the 21st Century: A Task Force Report*. Muscatine, Iowa: Stanley Foundation, October 2003. http://www.stanleyfoundation.org/publications/archive/SNS03.pdf.

Knight, Matthew. "Briefing: Oil." CNN, June 26, 2008. http://www.cnn.com/2008/TECH/science/05/13/Oilbriefing/index.html.

Kraska, James. "How the United States Lost the Naval War of 2015." *Orbis* (Winter 2010). http://www.fpri.org/orbis/5401/kraska.navalwar2015.pdf.

Krepinevich, Andrew F., Jr. *7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century.* New York: Bantam Dell, 2009.

———. *The Conflict Environment of 2016: A Scenario-Based Approach*. Washington, D.C.: Center for Strategic and Budgetary Assessments, 1996. http://www.csbaonline.org/4Publications/PubLibrary/R.19961001.The_Conflict_Envir/R.19961001.The_Conflict_Envir.pdf.

Li, Nan. "Unrestricted Warfare and Chinese Military Strategy." *RISS Commentaries/IDSS Commentaries*, no. 22. October 3, 2002. http://www3.ntu.edu.sg/rsis/publications/Perspective/IDSS222002.pdf.

Lundesgaard, Amund. "Will US navy Arctic roadmap increase tension?" GeoPolitics in the High North, December 15, 2009. http://www.geopoliticsnorth.org/index.php?option=com_content&view=article&id=96:will-us-navy-arctic-roadmap-increase-tension-in-the-arctic.

MacLeod, Ian. "U.S. navy plots Arctic push." *Ottawa Citizen*, November 28, 2009. http://www.ottawacitizen.com/technology/navy+plots+Arctic+push/2278324/story.html.

Mahnken, Thomas. "Irregular Warfare Challenges." In *Proceedings on Combating the Unrestricted Warfare Threat: Integrative Strategy, Analysis, and Technology*, edited by Ronald R. Luman. Laurel, Md.: Applied Physics Laboratory and School of Advanced International Studies, Johns Hopkins University, March 2008. http://www.jhuapl.edu/urw_symposium/Proceedings/2008/chapters/URW2008Book.pdf.

Manwaring, Max G. *The Inescapable Global Security Arena*. Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, 2002. http://www.strategicstudiesinstitute.army.mil/pdffiles/pub292.pdf.

Marine Corps Combat Development Command. *Marine Corps Operating Concepts for a Changing Security Environment*. Quantico, Va.: Marine Corps Combat Development Command, 2006.

Marine Technology Reporter. "Oceanographer of the Navy Addresses Climate Change." *Seadiscovery.com*, January 4, 2010. http://www.seadiscovery.com/mtStories.aspx?ShowStory=1034432072.

Markoff, John, David E. Sanger, and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *New York Times*, January 26, 2010. http://www.nytimes.com/2010/01/26/world/26cyber.html.

Maynard, Micheline, and Liz Robbins. "New Restrictions Quickly Added for Air Passengers." *New York Times*, December 27, 2009. http://www.nytimes.com/2009/12/27/us/27security.html.

Metz, Steven, and Raymond A. Millen. *Future War/Future Battlespace: The Strategic Role of American Landpower*. Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, 2003. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=214.

Monitor 360. *Practical Steps for Improving Intelligence Analysis: Perspectives from Monitor 360*. San Francisco: Monitor 360, March 2009. http://www.360.monitor.com/downloads/ImprovingAnalysisMonitor360.pdf.

National Defense Panel. *Transforming Defense: National Security in the 21st Century*. Washington, D.C.: National Defense Panel, 1997. http://www.dod.gov/pubs/foi/reading_room/902.pdf.

National Intelligence Council. *Global Trends 2015: A Dialogue about the Future with Nongovernment Experts*. Langley, Va.: National Intelligence Council, 2000. http://www.dni.gov/nic/PDF_GIF_global/globaltrend2015.pdf

———. *Global Trends 2025: A Transformed World*. Washington, D.C.: U.S. Government Printing Office, 2008.

———. *Mapping the Global Future: Report of the National Intelligence Council's 2020 Project*. Washington, D.C.: U.S. Government Printing Office, 2004.

Naval Postgraduate School Transformation Chair. "Forces Transformation Chairs Meeting: Visions of Transformation 2025—Shocks and Trends." Executive Summary presented at *Visions of Transformation 2005* conference, Monterey, California, February 12–13, 2007.

Nuclear Threat Initiative. "India Conducts Military Drill Close to Pakistan Border." *Global Security Newswire*, March 2, 2010. http://gsn.nti.org/gsn/nw_20100301_7761.php.

Nuclear Threat Initiative. "Toxin Found in Botox Could Pose Bioterrorism Threat." *Global Security Newswire*, January 25, 2010. http://gsn.nti.org/gsn/nw_20100125_2898.php.

O'Neil, William D., and Caitlin Talmadge. "Correspondence: Costs and Difficulties of Blocking the Strait of Hormuz." *International Security* 33, no. 3 (2008/2009).

Organization for Economic Cooperation and Development. "Chairman's Summary Note of the 14–15 June 2005 Meeting of the Round Table on Sustainable Development." Paris, September 6, 2006. http://www.oecd.org/dataoecd/48/50/39386783.pdf.

Peck, Allen G. "Airpower's Crucial Role in Irregular Warfare." *Air & Space Journal* XXI, no. 2 (Summer 2007). http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/sum07/peck.html.

Petersen, John L. *Out of the Blue: Wild Cards and Other Big Future Surprises, How to Anticipate and Respond to Profound Change*. Arlington, Va.: Arlington Institute, 1997.

Pew Forum on Religion and Public Life. "Little Support for Terrorism Among American Muslims." *Pew Research Center*, December 17, 2009. http://pewforum.org/Politics-and-Elections/Little-Support-for-Terrorism-Among-Muslim-Americans.aspx.

Pew Global Attitudes Project. *Most Muslim Publics Not So Easily Moved: Confidence in Obama Lifts U.S. Image Around the World*. Washington, D.C.: Pew Research Center, 2009. http://pew-global.org/reports/pdf/264.pdf.

———. *World Publics Welcome Global Trade—But Not Immigration*. Washington, D.C.: Pew Research Center, 2007. http://pewglobal.org/reports/pdf/258.pdf.

Pincus, Walter. "Pentagon reviewing strategic information operations." *Washington Post*, December 27, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/12/26/AR2009122601462.html.

Pomfret, John. "China's Wen Jiabao rebuffs U.S. on letting yuan appreciate against dollar." *Washington Post*, March 15, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/03/14/AR2010031402304.html.

Posen, Barry R. "Command of the Commons: The Military Foundation of U.S. Hegemony." *International Security* 28, no. 1 (2003).

Pudas, Terry. "Commentary: A new strategic construct for defense planning." *Federal Times*, May 14, 2007. Quoted in: http://enterpriseresilienceblog.typepad.com/enterprise_resilience_man/2007/05/trends_and_shoc.html.

Ramo, Joshua Cooper. *The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It*. New York: Little, Brown, 2009.

Ricks, Thomas E. "Calculating the Risks in Pakistan: U.S. War Games Weigh Options for Securing Nuclear Stockpile." *Washington Post*, December 2, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/12/01/AR2007120101618.html.

Riedel, Bruce, Rolf Mowatt-Larssen, Karin von Hippel, Daniella Pletka, Michael E. O'Hanlon, Ellen Laipson, and Parag Khanna. "Pakistan's Nuclear Scenarios, U.S. Solutions." Room for Debate: A Running Commentary on the News. *New York Times*, May 5, 2009. http://roomfordebate.blogs.nytimes.com/2009/05/05/pakistan-scenarios-us-solutions/.

Robock, Alan, and Owen Brian Toon. "Local Nuclear War, Global Suffering." *Scientific American* 302, no. 1 (2010).

Rodgers, Walter. "War over the Arctic? Global warming skeptics distract us from security risks." *Christian Science Monitor*, March 2, 2010. http://www.csmonitor.com/Commentary/Walter-Rodgers/2010/0302/War-over-the-Arctic-Global-warming-skeptics-distract-us-from-security-risks.

Scales, Major General Robert H. (Ret). *Future Warfare Anthology, Revised Edition*. Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, 2001.

Schwartz, Peter. *Inevitable Surprises: Thinking Ahead in a Time of Turbulence*. New York: Gotham Books, 2003.

Shlapak, David A. *Shaping the Future Air Force*. Santa Monica, Calif.: RAND Corporation, 2006.

Smol, Robert. "When will we get serious about Arctic defence?" CBC News, May 11, 2009. http://www.cbc.ca/canada/story/2009/05/11/f-vp-smol.html.

Soucy, Jon. "DoD relooks at plans for Guard response capabilities." WWW.ARMY.MIL, March 24, 2010. http://www.army.mil/-news/2010/03/24/36269-dod-relooks-at-plans-for-guard-response-capabilities/.

Stevens, Paul J. "Oil and the Gulf: Alternative Futures." In *The Persian Gulf at the Millennium: Essays in Politics, Economy, Security, and Religion*. Edited by Gary G. Sick and Lawrence G. Potter. New York: St. Martin's Press, 1997.

Sui, Cindy. "Taiwan polls hint at China unease." BBC News, December 7, 2009. http://news.bbc.co.uk/nolpda/ukfs_news/hi/newsid_8398000/8398607.stm.

Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2007.

Talmadge, Caitlin. "Closing Time: Assessing the Iranian Threat to the Strait of Hormuz." *International Security* 33, no. 1 (2008).

Tangredi, Sam J. *All Possible Wars? Toward a Consensus View of the Future Security Environment, 2001–2025*. McNair Paper 63. Washington, D.C.: Institute for National Strategic Studies, National Defense University, 2000. http://www.ciaonet.org/wps/tas04/tas04.pdf.

———. *Futures of War: A Consensus View of the Future Security Environment, 2010–2035*. Newport, R.I.: Alidade Press, 2008.

Thompson, Mark. "China's Missile Test: A Symbolic Warning to U.S." *Time*, January 13, 2010. http://www.time.com/time/world/article/0,8599,1953233,00.html.

Townsend, Fran. "Defending the Homeland" panel discussion, Military Strategy Forum, CSIS, Washington, D.C., June 16, 2009, http://csis.org/event/defending-homeland.

UK Ministry of Defence. *The DCDC Global Strategic Trends Programme: 2007-2036, Third Edition*. Swindon: Development, Concepts and Doctrine Centre, 2007.

———. *Strategic Trends: Methodology, Key Findings and Shocks*. Shrivenham: Joint Doctrine and Concepts Centre, 2003.

U.S. Air Force. *Foreign Internal Defense: Air Force Doctrine Document 2-3.1*. Washington, D.C. U.S.

Department of Defense, September 15, 2007. http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_3_1.pdf.

U.S. Army. "Security Force Assistance." *Field Manual No. 3-07.1.* Washington, D.C.: Department of the Army, 2009. http://usacac.army.mil/cac2/Repository/FM3071.pdf.

U.S. Bureau of the Census, Population Division. *International Data Base*. Washington, D.C., 2009. http://www.census.gov/ipc/www/idb/worldpopgraph.php.

U.S. Central Intelligence Agency. "Country Comparison: Oil—Proved Reserves." *The World Factbook*. https://www.cia.gov/library/publications/the-world-factbook/rankorder/2178rank.html.

———. "Israel." *The World Factbook*. https://www.cia.gov/library/publications/the-world-factbook/geos/is.html.

U.S. Commission on National Security/21st Century. *New World Coming: American Security in the 21st Century*. Washington, D.C.: U.S. Commission on National Security/21st Century, 1997.

U.S. Congress. House Armed Services Committee. Statement of General Kevin P. Chilton, commander, U.S. Strategic Command, 111th Cong., 2nd sess., March 16, 2010. http://armedservices.house.gov/pdfs/StratForces031610/Chilton_Testimony.pdf.

———. House Armed Services Committee, Subcommittee on Terrorism and Unconventional Threats and Capabilities. Testimony of Victor E. Renuart, Jr., commander, U.S. Northern Command, 111th Cong., 1st sess., July 28, 2009. http://armedservices.house.gov/pdfs/TUTC072809/Renuart_Testimony072809.pdf.

———. House Committee on Science and Technology. "Witnesses, Members Discuss How to Secure Cyberspace." Press Release, June 16, 2009. http://science.house.gov/press/PRArticle.aspx?NewsID=2517.

———. Senate Committee on Homeland Security and Government Affairs. "The US Pakistan Strategic Relationship and Nuclear Safety/Security." Testimony of Stephen P. Cohen, 110th Cong., 2nd sess., June 12, 2008. http://www.brookings.edu/testimony/2008/0612_pakistan_cohen.aspx.

U.S. Congressional Budget Office. *The Long-Term Budget Outlook.* Washington, D.C.: U.S. Congressional Budget Office, December 2007. http://www.cbo.gov/ftpdocs/88xx/doc8877/12-13-LTBO.pdf.

U.S. Department of Defense. "2010 QDR Terms of Reference Fact Sheet." Washington, D.C.: U.S. Department of Defense, April 26, 2009. http://www.defense.gov/news/d20090429qdr.pdf.

———. *Mobility Capabilities and Requirements Study 2016—Executive Summary*. Washington, D.C.: U.S. Department of Defense, 2010. http://www.afa.org/EdOp/PDFs/MCRS-2016_execsummary.pdf.

———. *The National Defense Strategy of the United States of America*. Washington, D.C.: U.S. Department of Defense, 2005.

———. *National Defense Strategy*. Washington, D.C.: U.S. Department of Defense, 2008.

———. Office of the Assistant Secretary of Defense/Homeland Defense and America's Security Affairs. "Department of Defense Support to Domestic Incidents." Washington, D.C.: U.S.

Department of Defense, 2008. http://www.fema.gov/pdf/emergency/nrf/DOD_SupportToDomesticIncidents.pdf.

———. Office of the Under Secretary of Defense for Acquisition, Technology & Logistics. Counterproliferation Program Review Committee. *Report on Activities and Programs for Countering Proliferation and NBC Terrorism, Volume I, Executive Summary*. Washington, D.C.: USD (AT&L), 2009. http://fas.org/irp/threat/nbcterror2009.pdf.

———. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Defense Science Board 2006 Summer Study on 21st Century Strategic Technology Vectors, Volume 1: Main Report.* Washington, D.C.: Defense Science Board, 2007. http://www.acq.osd.mil/dsb/reports/ADA463361.pdf.

———. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Report of the Defense Science Board 2008 Summer Study on Capability Surprise, Volume 1: Main Report.* Washington, D.C.: Defense Science Board, 2009. http://www.acq.osd.mil/dsb/reports/ADA506396.pdf.

———. *Trends and Shocks: A Conceptual Basis for Strategic Planning*. Washington, D.C.: U.S. Department of Defense, 2009.

———. *Quadrennial Defense Review Report, 2001*. Washington, D.C.: U.S. Department of Defense, 2001.

———. *Quadrennial Defense Review Report, 2006*. Washington, D.C.: U.S. Department of Defense, 2006.

———. *Quadrennial Defense Review Report, 2010*. Washington, D.C.: U.S. Department of Defense, 2010.

U.S. Department of Defense Strategy Office. *Trends Analysis Construct: Trends and Discontinuities Overview*. Washington, D.C.: U.S. Department of Defense, 2009.

U.S. Department of Homeland Security. *National Response Framework*. Washington, D.C.: U.S. Department of Homeland Security, 2008. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

U.S. Geological Survey. "Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle." USGS Fact Sheet 2008-3049 (2008). http://pubs.usgs.gov/fs/2008/3049/fs2008-3049.pdf.

U.S. Government Accountability Office. *Defense Logistics: Lack of Key Information May Impede DOD's Ability to Improve Supply Chain Management*. Washington, D.C.: GAO, 2009. http://www.gao.gov/new.items/d09150.pdf.

———. *Defense Space Activities: DOD Needs to Further Clarify the Operationally Responsive Space Concept and Plan to Integrate and Support Future Satellites*. Washington, D.C.: GAO, 2008. http://www.gao.gov/new.items/d08831.pdf.

———. *Emergency Communications: Establishment of the Emergency Communications Preparedness Center and Related Interagency Coordination Challenges*. Briefing prepared for the Subcommittees on Homeland Security, Committees on Appropriations, U.S. Senate and House of Representatives, 111th Cong., 2nd Sess. Washington, D.C.: GAO, 2010. http://www.gao.gov/new.items/d10463r.pdf.

———. *Forces that Will Shape America's Future: Themes from GAO's Strategic Plan 2007–2012*. Washington, D.C.: GAO, 2007. http://www.gao.gov/new.items/d07467sp.pdf.

———. *Homeland Defense: Planning, Resourcing, and Training Issues Challenge DOD's Response to Domestic Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Incidents*. Report to Congressional Requestors. Washington, D.C.: GAO, October 2009. http://www.gao.gov/new.items/d10123.pdf.

———. *National Response Framework: FEMA Needs Policies and Procedures to Better Integrate Non-Federal Stakeholders in the Revision Process*. Washington, D.C.: GAO, 2008. http://www.gao.gov/new.items/d08768.pdf.

U.S. Joint Forces Command. *Capstone Concept for Joint Operations: Version 3.0*. Washington, D.C.: Department of Defense, 2009.

———. *The Joint Operating Environment 2008: Challenges and Implications for the Future Joint Force*. Suffolk: USJFCOM, 2008.

U.S. Navy, Task Force Climate Change/Oceanographer of the Navy. *U.S. Navy Arctic Roadmap.* October 2009. http://www.wired.com/images_blogs/dangerroom/2009/11/us-navy-arctic-roadmap-nov-2009.pdf.

U.S. Office of Management and Budget. *Historical Tables: Budget of the United States Government, Fiscal Year 2009*. Washington, D.C.: Government Printing Office, 2010. http://www.whitehouse.gov/omb/budget/fy2011/assets/hist.pdf.

van der Veer, Jeroen. *Shell Global Scenarios to 2025*. Royal Dutch/Shell Group, 2005.

Westing, Arthur H. "Overpopulation and Climate Change." *New York Times*, February 17, 2010.

White House. *2002 National Strategy to Combat Weapons of Mass Destruction*. Washington, D.C.: White House, 2002.

———. *Cyberspace Policy Review*. Washington, D.C.: White House, 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

———. *Drug Control Strategy: FY 2010 Budget Summary*. Washington, D.C.: White House, 2009. http://www.whitehousedrugpolicy.gov/publications/policy/10budget/fy10budget.pdf.

———. National Security Council. *National Strategy for Countering Biological Threats*. Washington, D.C.: White House, 2009. http://www.whitehouse.gov/sites/default/files/National_Strategy_for_Countering_BioThreats.pdf

———. Office of Science and Technology Policy. *U.S. National Space Policy*. Washington, D.C.: White House, 2006. http://www.whitehouse.gov/sites/default/files/microsites/ostp/national-space-policy-2006.pdf.

———. *The National Security Strategy of the United States of America, 2002.* Washington, D.C.: White House, 2002.

———. *The National Security Strategy of the United States of America, 2006.* Washington, D.C.: White House, 2006.

———. "Remarks by the President on Securing our Nation's Cyber Infrastructure," May 29, 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

Wolpin, Stewart. "The Decade's Top 10 Trends." *Invention & Technology* 24, no. 4 (2010)

World Health Organization. *The World Health Report 2007—A Safer Future: Global Public Health Security in the 21st Century.* Geneva: World Health Organization, 2007. http://www.who.int/whr/2007/whr07_en.pdf.

World Health Organization. *The World Health Report 2008—Primary Health Care: Now More Than Ever.* Geneva: World Health Organization, 2008. http://www.who.int/whr/2008/en/index.html.

Wright, Austin. "Coast Guard Examines Future of Patrolling the Arctic." *National Defense*, January 2010. http://www.nationaldefensemagazine.org/archive/2010/January/Pages/CoastGuardExaminesFutureofPatrollingTheArctic.aspx.

Yudkowsky, Eliezer. "Why Is the Future So Absurd?" In *lesswrong blog*, administered by University of Oxford, September 7, 2007. http://lesswrong.com/lw/j6/why_is_the_future_so_absurd/.

Zysk, Katarzyna. "Russia's Arctic Strategy: Ambitions and Constraints." *Joint Force Quarterly* 57 (Second quarter 2010). http://www.ndu.edu/press/jfq_pages/editions/i57/zysk.pdf.

APPENDIX B
ROUNDTABLE PARTICIPANTS

Trends and Shocks: Hedging and Shaping Strategies Workshop Attendees

CSIS, Washington, D.C., January 26, 2010

Mr. Joseph Angello Jr.
Office of the Under Secretary of Defense, Personnel & Readiness

Mr. David Berteau
CSIS

Dr. Daniel Chiu
Office of the Under Secretary of Defense, Policy

CDR Doug Fears
CSIS

Mr. Nathan Freier
CSIS

Ms. Meg Giles
CSIS

COL Simon Goerger
Office of the Under Secretary of Defense, Personnel & Readiness

CDR Gregory Gombert
Office of the Under Secretary of Defense, Policy

CAPT John Griffin
CSIS

LtCol Glenn Guenther
CSIS

Dr. Robert Haffa
Northrop Grumman Corporation

Mr. Mike Hix
RAND Corporation

Mr. Bill Huggins
Toffler Associates

Mr. William Inglee
Lockheed Martin Corporation

Mr. Kenneth Knight
National Intelligence Council

Dr. Maren Leed
CSIS

Mr. Raphael Marcus
CSIS

Dr. Steven Metz
U.S. Army War College

Ms. Tara Murphy
CSIS

Mr. Rick "Ozzie" Nelson
CSIS

Ms. Rachel Posner
CSIS

Ms. Hilary Price
CSIS

Mr. Ben Riley
Office of the Under Secretary of Defense, Acquisition, Technology & Logistics

Col. Rickey Rupp
CSIS

Dr. Wayne Schroeder
Lockheed Martin Corporation

Mr. Robert Simpson
U.S. Army Training and Doctrine Command

Mr. David Sokolow
CSIS

ABOUT THE AUTHORS

Maren Leed is a senior fellow and director of the CSIS New Defense Approaches Project, where she works on a variety of defense issues. She previously served as an analyst at the RAND Corporation, where she led projects concerning intelligence, surveillance, and reconnaissance (ISR) and countering improvised explosive devices (IEDs). From 2005 to 2008, she was assigned as a special assistant to the vice chairman of the Joint Chiefs of Staff and was responsible for a range of issues including IEDs, ISR, cyber operations, biometrics, rapid acquisition, and Iraq policy. From 2001 to 2005, she was a professional staff member on the Senate Armed Services Committee, where she handled the operation and maintenance accounts and conducted oversight of military readiness, training, and logistics and maintenance for committee members. She was an analyst in the Economic and Manpower Analysis Division of the Office of Program Analysis and Evaluation in the Office of the Secretary of Defense from 2000 to 2001, where she conducted macroeconomic analyses relating to military manpower and coordinated Department of Defense performance contracts with its defense agencies. She was a doctoral fellow at RAND from 1995 to 1999, analyzing military manpower issues, training for operations other than war, and leader development, and providing strategic planning support for the military and private-sector organizations. She received her A.B. in political science from Occidental College, and her Ph.D. in quantitative policy analysis from the RAND Graduate School.

Hilary Price is a fellow with the CSIS New Defense Approaches Project. She recently defended her doctorate in international relations at St. Antony's College, University of Oxford. She wrote her dissertation on the NATO-Russia relationship in the 1990s, focusing on military cooperation between Russia and NATO during the Bosnian conflict. From 2004 through 2006, she was executive director of public programs at the Chicago Council on Foreign Relations, where she was responsible for conceptualizing, organizing, and implementing the council's public lecture program. From 2001 to 2003, she was a research fellow in Foreign Policy Studies at the Brookings Institution in Washington, D.C. Prior to graduate school, Ms. Price was coordinator of the Preventive Defense Project, a joint research venture between Harvard University and Stanford University focusing on U.S. defense policy. From 1995 to 1997, she worked for the National Democratic Institute, where she spent 1996 in Armenia and Azerbaijan working with political parties, parliamentarians, and civic organizations in an effort to strengthen democratic institutions. Ms. Price holds a B.A. in political science and Russian studies from Williams College and is a member of both the International Institute for Strategic Studies and Women in International Security.

Tara Murphy is a fellow with the CSIS Defense and National Security Group, where she works on a wide range of international security and U.S. defense issues. While at CSIS, she developed a conceptual framework of the broad range of issues related to U.S. nuclear weapons policy and nonproliferation, with particular emphasis on the implications of the convergence of such policy issues for the Toward a Comprehensive Framework for Integrating Nuclear Issues project. She is a contributing author to *Transforming NATO (…again): A Primer for the NATO Summit in Riga 2006* (CSIS, 2006). Previously, she was project coordinator for the Project on Nuclear Issues at CSIS. From 2003 to 2004, she was a presidential fellow at the Center for the Study of the Presidency (CSP), where she wrote "Widening the Divide: The Role of Leadership in the Transatlantic Rift" (CSP, 2004). Ms. Murphy holds an M.A. in security studies from Georgetown University and a B.S. magna cum laude in international affairs with a minor in French from the Georgia Institute of Technology.

Becca Smith is a research associate in the CSIS International Security Program. Before joining CSIS, she analyzed National Security Council processes from Harry S. Truman to George W. Bush for the Project on National Security Reform in Washington, D.C. Prior to that, she witnessed foreign policy in operation as a public affairs intern at the U.S. embassy in Paris. Ms. Smith holds a M.A. in international affairs from the George Washington University, a French studies diploma from the Université de Tours, France, and a B.A. in English and French from Bryn Athyn College.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1800 K Street, NW | Washington, DC 20006
Tel: (202) 887-0200 | Fax: (202) 775-3199
E-mail: books@csis.org | Web: www.csis.org