Capability Surprise for U.S. Naval Forces: Initial Observations and Insights: Interim Report

ISBN
978-0-309-26910-0

43 pages
8 1/2 x 11
2013

Committee on Capability Surprise for U.S. Naval Forces; Naval Studies Board; Division on Engineering and Physical Sciences; National Research Council

Capability Surprise for U.S. Naval Forces: Initial Observations and Insights

Interim Report

Committee on Capability Surprise for U.S. Naval Forces
Naval Studies Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract No. N00014-10-G-0589, DO #5 between the National Academy of Sciences and the Department of the Navy. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number-13: 978-0-309-26910-0
International Standard Book Number-10: 0-309-26910-5

Copies of this report are available free of charge from:

Naval Studies Board
National Research Council
The Keck Center of the National Academies
500 Fifth Street, NW
Washington, DC 20001

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; http://www.nap.edu.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON CAPABILITY SURPRISE FOR U.S. NAVAL FORCES

JERRY A. KRILL, Johns Hopkins University, Applied Physics Laboratory, *Co-Chair*
J. PAUL REASON, ADM, USN (retired), Washington, D.C., *Co-Chair*
ANN N. CAMPBELL, Sandia National Laboratories
TIMOTHY P. COFFEY, McLean, Virginia
STIRLING A. COLGATE, Los Alamos National Laboratory
CHARLES R. CUSHING, C.R. Cushing & Co., Inc.
SUSAN HACKWOOD, California Council on Science and Technology
LEE M. HAMMARSTROM, Pennsylvania State University, Applied Research Laboratory
NATHANIEL S. HEINER, Northrop Grumman Corporation
LEON A. JOHNSON, Brig Gen, USAFR (retired), Irving, Texas
CATHERINE M. KELLEHER, University of Maryland, Brown University
JEFFREY E. KLINE, Naval Postgraduate School
ANNETTE J. KRYGIEL, Great Falls, Virginia
THOMAS V. McNAMARA, Raytheon Integrated Defense Systems
RICHARD W. MIES, ADM, USN (retired), Fairfax Station, Virginia
C. KUMAR N. PATEL, Pranalytica, Inc.
HEIDI C. PERRY, Charles Stark Draper Laboratory, Inc.
GENE H. PORTER, Institute for Defense Analyses
DANA R. POTTS, Lockheed Martin Aeronautics Company
JOHN E. RHODES, LtGen, USMC (retired), Balboa, California
ROBERT M. STEIN, Brookline, Massachusetts
VINCENT VITTO, Lexington, Massachusetts
DAVID A. WHELAN, The Boeing Company
PETER G. WILHELM, Naval Research Laboratory
JOHN D. WILKINSON, MIT Lincoln Laboratory

NRC Staff
CHARLES F. DRAPER, *Director and Study Director* (as of June 21, 2012)
BILLY M. WILLIAMS, *Study Director* (through June 20, 2012)
RAYMOND S. WIDMAYER, Senior Program Office
MARTA V. HERNANDEZ, Associate Program Officer
SUSAN G. CAMPBELL, Administrative Coordinator
MARY G. GORDON, Information Officer

NAVAL STUDIES BOARD

MIRIAM E. JOHN, Livermore, California, *Chair*
DAVID A. WHELAN, The Boeing Company, *Vice Chair*
TIMOTHY P. COFFEY, McLean, Virginia
CHARLES R. CUSHING, C.R. Cushing & Co., Inc.
JAMES N. EAGLE, Naval Postgraduate School
ANUP GHOSH, George Mason University
JAMES R. GOSLER, Sandia National Laboratories
SUSAN HACKWOOD, California Council on Science and Technology
JAMES L. HERDT, Chelsea, Alabama
BARRY M. HOROWITZ, University of Virginia
JAMES D. HULL, Annapolis, Maryland
TAMARA E. JERNIGAN, Lawrence Livermore National Laboratory
BERNADETTE JOHNSON, Massachusetts Institute of Technology, Lincoln Laboratory
LEON A. JOHNSON, Irving, Texas
CATHERINE M. KELLEHER, University of Maryland, Brown University
JERRY A. KRILL, Johns Hopkins University, Applied Physics Laboratory
TERRY P. LEWIS, Raytheon Company
RICHARD S. MULLER, University of California at Berkeley
JOSEPH PEDLOSKY, Woods Hole, Massachusetts
HEIDI C. PERRY, Charles Stark Draper Laboratory, Inc.
J. PAUL REASON, Washington, D.C.
JOHN E. RHODES, Balboa, California
ALLAN STEINHARDT, Booz Allen Hamilton, Inc.
TIMOTHY M. SWAGER, Massachusetts Institute of Technology

Navy Liaison Representatives
RADM JAMES G. FOGGO III, USN, Director, Assessment Division, Office of the Chief of Naval Operations, N81
RADM MATTHEW L. KLUNDER, Chief of Naval Research/Director, Innovation, Technology Requirements, and Test & Evaluation, N84

Marine Corps Liaison Representative
LTGEN RICHARD P. MILLS, USMC, Commanding General, Marine Corps Combat Development Command

Staff
CHARLES F. DRAPER, Director
BILLY M. WILLIAMS, Senior Program Officer (through June 20, 2012)
RAYMOND S. WIDMAYER, Senior Program Officer
MARTA V. HERNANDEZ, Associate Program Officer
SUSAN G. CAMPBELL, Administrative Coordinator
MARY G. GORDON, Information Officer

ACKNOWLEDGMENT OF REVIEWERS

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Ruth A. David, Analytic Services, Inc. (ANSER),
David J. Dorset, VADM, USN (retired), Northrop Grumman Corporation,
Leslie Greengard, Courant Institute of Mathematical Sciences, New York University,
Harry W. Jenkins, Jr., MajGen, USMC (retired), Independent Consultant,
Kathryn B. Laskey, George Mason University,
Alton D. Romig, Jr., Lockheed Martin Corporation,
Neil G. Siegel, Northrop Grumman Information Systems, and
James Ward, Massachusetts Institute of Technology, Lincoln Laboratory.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Stephen M. Robinson, University of Wisconsin, Madison. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

CONTENTS

INTRODUCTION

A letter dated December 21, 2011, to National Academy of Sciences President Dr. Ralph Cicerone from the Chief of Naval Operations, ADM Jonathan W. Greenert, U.S. Navy, requested that the National Research Council's (NRC's) Naval Studies Board (NSB) conduct a study to examine the issues surrounding capability surprise—both operationally and technically related—facing the U.S. naval services. Accordingly, in February 2012, the NRC, under the auspices of its NSB, established the Committee on Capability Surprise for U.S. Naval Forces.

The study's terms of reference, provided in Enclosure A of this interim report, were formulated by the Office of the Chief of Naval Operations (CNO) in consultation with the NSB chair and director. The terms of reference charge the committee to produce two reports over a 15-month period. The present report is the first of these, an interim report issued, as requested, following the third full committee meeting. The terms of reference direct that the committee in its two reports do the following:[1]

(1) Select a few potential capability surprises across the continuum from disruptive technologies, to intelligence inferred capability developments, through operational deployments and assess what U.S. Naval Forces are doing (and could do) about these surprises while mindful of future budgetary declines;

(2) Review and assess the adequacy of current U.S. Naval Forces' policies, strategies, and operational and technical approaches for addressing these and other surprises; and

(3) Recommend any changes, including budgetary and organizational changes, as well as identify any barriers and/or leadership issues that must be addressed for responding to or anticipating such surprises including developing some of our own surprises to mitigate against unanticipated surprises.

This first report highlights issues brought to the committee's attention during its first three meetings and provides initial observations and insights in response to each of the three tasks above. It is very much an interim report that neither addresses in its entirety any one element of the terms of reference nor reaches final conclusions on any aspect of capability surprise for naval forces. The committee will continue its study during the coming months and expects to complete by early summer 2013 its final report, which will address all of the elements in the study's terms of reference and explore many potential issues of capability surprise for U.S. naval forces not covered in this interim report.

In its initial three meetings, the committee received a number of helpful briefings from commands across the U.S. Navy, the U.S. Marine Corps, and the U.S. Coast Guard, as well as expert briefings from individuals working at a number of other government agencies, including the following: the Office of Naval Intelligence, Office of Naval Research; Deputy Assistant Secretary of Defense for Rapid Fielding; the Defense Advanced Research Projects Agency (DARPA); the U.S. Navy SSBN Security Program;

[1]The full terms of reference for this study are provided in Enclosure A of this report.

the Missile Defense Agency; MIT Lincoln Laboratory's Air Vehicle Survivability Evaluation Program (Air Force Red Team); the Naval War College; Deputy Assistant Secretary of the Navy, Research Development & Acquisition for Science and Technology; OPNAV N81; OPNAV N4; OPNAV N3/N5; OPNAV N2/N6; U.S. Fleet Cyber Command/U.S. Tenth Fleet; Combat Development Command/Combat Development and Integration, U.S. Marine Corps; the Assistant Commandant for Capability, U. S. Coast Guard; and the National Maritime Intelligence-Integration Office. In addition, the committee conducted preliminary data-gathering sessions on capability surprise-related issues with the U.S. Naval Research Laboratory, the U.S. Navy Warfare Development Command, and U.S. Pacific Fleet. When combined with the collective knowledge of the committee, these briefings are considered to constitute a sufficient basis for development of the initial observations and insights offered by the committee in this report.

FRAMING THE PROBLEM—BACKGROUND ON CAPABILITY SURPRISE AND U.S. NAVAL FORCES

Recent reports have addressed the issue of surprise, although not surprise specific to U.S. naval forces (i.e., the U.S. Navy, U.S. Marine Corps, and U.S. Coast Guard). A 2009 Defense Science Board (DSB) report on capability surprise noted that: "[s]urprise can spring from many sources. It can arise in the laboratory—

> a result of scientific breakthrough. It can arise during the transition from concept to fielded product: rapid fielding of the same technology can create tremendous advantage to whoever fields the system first. It can also arise when an existing capability is employed in an unconventional way or when low-end technology is adapted in unforeseen ways that create an effective capability against high-end U.S. systems.[2]

The DSB report reviewed many historical surprises experienced by the United States and categorized them as either known surprises (i.e., surprises that should have been anticipated and acted on because it was clear that they were in the offing) or surprising surprises (i.e., those that may have been anticipated by some but were not addressed—swamped by the thousands of other surprises possible—or were true surprises).[3]

In addition, a 2008 Naval Research Advisory Committee (NRAC) report titled *Disruptive Commercial Technologies* noted, among other things, that "the internet

---

[2]Defense Science Board. 2009. *Report of the Defense Science Board 2008 Summer Study on Capability Surprise*, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., September, pp. vii-viii.

[3]The temporal and impact aspects of capability surprises vary widely and call for different approaches to prepare for and respond to such surprises. As additional background for this study, the committee examined several historical examples of 'surprises" that have had significant impact on naval and military operations, including short lived surprises (such as the suicide bomb attacks on the USS *Cole*, and the 911 World Trade Towers); and longer term surprises, resulting in major changes in U.S. naval and military forces (such as the *Monitor* and *Merrimac* introduction of ironclad warships; as well as Russia's launch of Sputnik (surprising use of space—leading to the creation of DARPA) and Germany's Blitzkrieg (uniquely combining and exploiting the capabilities of known entities.))

functions effectively as both a research and development (R&D) resource and supply chain for irregular forces throughout the world. Commercial technologies pose a real and enduring threat to Marine forces."[4] In summary, the NRAC report concluded that globally available commercial technologies exist that might be used in adverse ways against Marine forces. Although it did not focus on "technology surprise" per se, the NRAC report did examine, in part, the power of unconventional and unconstrained imagination that can be brought to bear against Marine forces operating around the world.

This committee has found that addressing surprise as it might impact U.S. naval forces is a complex subject with multiple dimensions, including time, mission and cross-mission domains, anticipation of enabling technologies, physical phenomena, and new tactics that may enable surprise. In terms of time, surprises may come over scales ranging from seconds up to minutes in a complex engagement, to the evolving, break-through surprise that might have been secretly developed over decades. The mission domains such as air defense and undersea warfare, which require that U.S. naval forces operate across the open ocean and littoral (land, air, space, and cyberspace), all have myriad entry points from which capability surprises can originate. There are also accelerating new technological advancements globally, which again, alone or in combination, can constitute the basis of a capability surprise.

Given its complexity, there is no simple answer regarding how to guard against surprise. A number of explicit actions are needed. First and foremost, leaders must help others recognize the importance of understanding capability surprise and what it means to U.S. naval forces, such as ensuring that organizations include preparation for and mitigation of surprise as part of their functions, including scanning and related activities in order to advise naval forces of potential emerging surprises. It is important that organizations are timely and diligent in examining the scope and seriousness of potential emerging surprises, and that they are capable of identifying other organizations that might be able to help anticipate, mitigate, or respond to potential emerging surprises.

Defining "Surprise"

From a military operational point of view, surprise can be an event or capability that could affect the outcome of a naval mission or campaign for which preparations are not in place. The committee believes that there are two classes of surprise that fall within this military operational context and can be described using the terminology provided in the study's terms of reference: (1) intelligence-inferred surprise and (2) disruptive technology and tactical surprise.

Intelligence-inferred surprise is an event or capability developed on a relatively long timeline—years—whose looming operational introduction naval forces were aware of in advance, but might not adequately have prepared for. Disruptive technology (including disruptive application of existing technology) and tactical surprise are types of short-timeline—hours to months—events or capabilities for which naval forces will likely not have had sufficient time to prepare contingency counters in advance unless the

---

[4]Naval Research Advisory Committee. 2008. *Disruptive Commercial Technologies*, Assistant Secretary to the Navy for Research, Development and Acquisition, Department of Defense, Washington, D.C., June 26, p. 15.

surprises have been at least somewhat anticipated. In some cases both types of surprise can occur, for example, a much anticipated surprise capability found on the battlefield to have tactical war reserve modes.

The committee recognizes that a preponderance of intelligence-inferred surprise is being addressed (on a continuous basis) within naval program areas such as air and missile defense, antisubmarine warfare, and strike warfare. In such instances, the future threat is projected and upgrades to naval systems are developed and fielded to meet the threat. This report does not address this class of already-addressed intelligence-inferred surprises. It does, however, address intelligence-inferred surprises for which "cradle-to-grave" upgrades do not exist or for which the capability represented by the projected threat requires coordination among a number of program areas. An example of such a scenario surprise—denial of access to space—is discussed in the next section of this report.

The committee also recognizes two variants of disruptive technology and tactical surprise. One variant is the "pop up" emergence of a new capability enabled by a new technology or an unexpected application of a pre-existing well known technology, e.g., improvised explosive device triggers, as well as an unexpected tactic such as an adversary's use of previously unknown war-reserve modes. The other variant—"black swan" events—may be self-inflicted surprises, e.g., an anticipatory "blind spot" that no amount of surveillance would have overcome.[5] These may be the result of a sudden U.S. policy change or directed action, such as Operation Burnt Frost,[6] or natural disasters that may have been anticipated, but not at the extreme scale of the event as it actually occurred, e.g., the March 2011 Fukushima Disaster.[7]

In the broadest sense, surprise grants the adversary the ability to take unexpected action and/or to produce consequences for which U.S. forces did not prepare in advance. In summary, surprises may result from new technologies or from the application of existing technologies in new ways, or may evolve from operational, social, natural, or political factors for which technology or lack of mitigating technology may not be the primary determinant of outcome.

---

[5]Nassim Taleb defines a black swan as "a highly improbable event with three principal characteristics: It is unpredictable; it carries a massive impact; and, after the fact, we concoct an explanation that makes it appear less random, and more predictable, than it was." For additional reading on black swan events see Nassim Nicholas Taleb, 2007, *The Black Swan: The Impact of the Highly Improbable,* Random House Press, New York.

[6]A nonfunctioning U.S. National Reconnaissance Office satellite was successfully shot down by a Standard Missile (SM)-3 on February 20, 2008. The code name for this mission was Operation Burnt Frost. See RADM Brad Hicks, USN, Program Director, Aegis Ballistic Missile Defense, "Aegis Ballistic Missile Defense: Press Briefing, March 19, 2008," presented to the committee by RADM Joseph A. Horn, Jr., USN, Program Executive, Aegis Ballistic Missile Defense, and Conrad J. Grant, Johns Hopkins University Applied Physics Laboratory, May 16, 2012, Washington, D.C.; and press release by the U.S. Air Force, lst Lt. Angela Webb, USAF, 30th Space Wing Public Affairs, 2008, "Joint Effort Made Satellite Success Possible," February 26; found at http:www.af.mil/news/story.asp?id=123087750. Accessed January 15, 2013.

[7]A partial profile of U.S. naval response to the Fukushima disaster—a combined earthquake, tsunami, and nuclear reactor catastrophe—in a coordinated effort known as "Operation Tomodachi" is found at http://www.nbr.org/research/activity.aspx?id=121. Accessed June 13, 2012.

Examples of Surprise

The committee discussed a number of different examples of surprise, ranging from an adversary's potential deployment of disruptive technologies against naval operations (such as specific "Day 0" cyber offense payloads), to the potential interruption of critical supply chains (such as for rare-earth elements), to the potential unfolding of national security-related geopolitical events (such as regional economic instability). The committee also reviewed case studies of previous surprises and the circumstances leading up to the surprises and will discuss several of these in its final report for illustrative purposes. Examples of some intelligence-inferred surprises and disruptive technology and tactical surprises are provided in Box 1; however, these examples should not be viewed as a definitive list of all the types of surprises naval forces might face.

BOX 1
Some Examples of Surprises

Examples of Intelligence-Inferred Surprises

- **Cyber intrusions (e.g., programmable logic computer worms).**
- **Ballistic missile attacks (e.g., medium-range ballistic missiles).**
- **Use of uninhabited vehicles (e.g., semisubmersibles for attacks).**
- **International security and cooperation (e.g., nuclear weapon proliferation, economic instability, cultural/tribal/religious conflicts).**
- **Denial of access to space (e.g., jamming, use of antisatellite weapons).**

Examples of Disruptive Technology and Tactical Surprises

- **Use of synthetic biological weapons.**
- **Use of small nuclear weapons.**
- **Use of highly energetic sources.**
- **Use of improvised explosive device triggers.**
- **Social media utilizations.**

In addition to reviewing previous case studies of surprises, the committee has, so far, selected the following three surprise scenarios, which it believes are important to U.S. naval forces, as starting points from which it can examine, illustrate by example, and, ultimately, recommend potential changes as requested in the study's terms of reference:[8]

- Scenario 1: Denial of access to space;
- Scenario 2: An asymmetric engagement with complex use of cyber attacks in a naval context; and

[8]In addition to the surprise scenarios listed in this interim report, the committee anticipates further illustration of surprise in the final report by examining additional scenarios, such as potential nonkinetic effects to counter missile magazine limits, and the potential impact of unmanned underwater vehicles (UUVs) to represent both a surprise threat and opportunity.

- Scenario 3: A "black swan" event for which the front-end scanning and prioritization framework for mitigating surprise (to be described) is not applicable.

Surprise Scenario 1 (intelligence-inferred surprise): *Potential loss of access to space due to antisatellite capabilities and electronic or optical countermeasures, including loss of intelligence, surveillance, and reconnaissance (ISR) feeds, communications, navigation (GPS), and timing (also GPS).* The loss of access to space scenario has been broadly discussed in the open media.[9] In particular, U.S. naval warfighting systems depend heavily on positioning, navigation, and timing. In essence an adversary, in denying U.S. forces' access to space, could employ the following measures against U.S. space assets, either simultaneously or with unpredictable frequency to render those assets unreliable:

- Jamming U.S. combatant or weapons GPS receivers within the line-of-sight of adversary surface and airborne platforms,
- Cyber attack on command and control centers and combatants,
- Jamming or dazzling surveillance sensors to obscure U.S. orbital ISR observations,
- Jamming of communications reception by satellite receivers within the receive antenna's main beams or side lobes,
- Jamming of satellite downlink receivers within the line-of-sight of adversary surface or airborne combatants or weapons, or
- Kinetic engagement of orbital systems.

The committee also recognizes that cyber attacks or other interference in this scenario could originate from imbedded threats in commercial off-the-shelf hardware and software that are widely deployed in present naval systems and could render naval systems and networks inoperable at a critical moment of need. The heavy dependence on certain widely used satellite communications operating in frequency bands that can be more readily jammed is a particular concern. Jamming of communications and denial-of-service attacks are clearly an intelligence-inferred surprise that can be mitigated with alternatives.[10]

For the final report, the committee intends to explore the broader issue of an anti-access/area denial environment, one element of which is the loss of access to space. Such an enquiry will allow for further examination of the following issues:

---

[9]For example, see *Background Briefing on Air-Sea Battle by Defense Officials from the Pentagon*, News Transcript, U.S. Department of Defense, Office of the Assistant Secretary of Defense, November 9, 2011; available at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4923, accessed May 9, 2012. See also Toshi Yoshihara and James R. Holmes, 2012, "Asymetric Warfare, American Style," *Proceedings of the Naval Institute,* April, pp. 24-29; Andrew Erickson and Amy Chang, 2012, "China's Navigation in Space," *Proceedings of the Naval Institute,* April, pp. 42-47; and David Fulghum, 2012, "Under Siege: Foreign Countermeasures Proliferate as U.S. Electronic Warfare Programs Falter," *Aviation Week & Space Technology,* April 9, pp. 22-23.

[10]The issue of cyber defense for U.S. naval forces will be covered more extensively in an upcoming NSB study, commissioned by the CNO, and anticipated to be ready in the first quarter of 2013.

- Potential gaps between missions that could provide openings for surprise, e.g., between strike, antisubmarine warfare defense, antisurface warfare defense, and air defense capabilities, as well as the complexities of multiplicative use of every asset from every mission area to "take out" a Navy aircraft carrier;
- New concepts of operations for emerging advanced new capabilities such as low-observable, unmanned aerial vehicles; precision strike; 5th generation air; Mach 3+ air, high-speed, and surface threats;
- Potential novel uses of nonkinetic, rapidly reconfigured assets such as electronic warfare, especially in the context of "red versus blue and blue versus red";
- Implications for logistics chain protection;
- Potential cultural expectations and blind spots;
- Use of social media in a propaganda strike in an attempt to influence attitudes at home and even debilitate a nation's will to fight; and
- The role of surprise tactics.

Surprise Scenario 2 (disruptive technology and tactical surprise): *Potential consequences of social media crowd emergence that could place U.S. personnel and property at risk in foreign areas or threaten U.S. domestic infrastructure.* The committee has begun to explore the potential implications of population unrest, whether spontaneous or induced, in which social media is used to turn a local population against the United States and to facilitate coordinated search and engagement of U.S. citizens and U.S. assets on the ground in a manner not unlike some of the uses of social media during the Arab Spring.[11] This is an area that may require a combination of tactics, techniques, and procedures (TTPs) and perhaps creation of a new situation awareness capability, especially as it might apply to naval ships or other U.S. naval personnel operating in foreign ports. This scenario is also a mechanism for examining the complexities of attempted cyber manipulation of a crowd's mood and actions, and it provides a context for considering potential effects of surprise in on-the-ground and coastal operation of naval forces.

Surprise Scenario 3 ("black swan" surprise): *Black swan* **(***self-inflicted and/or natural disaster) surprises include a full range of potential actions that might have a significant impact on the capability of U.S. naval forces.* These include events such as acts of nature (e.g., tsunamis, earthquakes, or disease outbreaks), as well as surprises that might evolve from actions such as national strategic decisions and/or national budget priority changes. Examples of national strategic decisions include the recent decision to deploy the U.S. Coast Guard to remote areas of global conflict and the earlier U.S. naval forces humanitarian assistance/disaster relief response to the 2010 catastrophic earthquake in Haiti.

---

[11]See Lisa Anderson, 2011, "Demystifying the Arab Spring," *Foreign Affairs*, May/June. Available at http://www.foreignaffairs.com/articles/67693/lisa-anderson/demystifying-the-arab-spring. Accessed May 12, 2012.

In addition to data gathering and discussions that helped the committee formulate the three surprise scenarios described above, the committee also received briefings from exemplar programs that appear quite capable of timely anticipation of and response to surprise. In this interim report, the committee applies the above three surprise scenarios and three exemplars—the Navy SSBN Security Program, the Air Vehicle Survivability Evaluation Program (Air Force Red Team), and the Aegis Ballistic Missile Defense Program—as example cases to help illuminate the following:

- Impediments that currently exist for certain areas of potential surprise outside of mainstream acquisition programs that may be hampering anticipation and response;
- Successful principles and infrastructures that might be integrated into already existing naval organizational structures and processes to address the broader realm of potential surprises;
- Structures and processes that could accommodate the above three examples of unaddressed/under-addressed surprises (denial of access to space, flash mob activity via social media, disaster response);
- Key capabilities, policies, and metrics that support successful structures and processes for dealing with surprise; and
- Potential changes to better prepare for, and be more resilient in the face of capability surprise for naval forces.

These concepts, and opportunities for improvements, are explored and integrated below.

A POTENTIAL NAVAL FRAMEWORK FOR DEALING WITH SURPRISE

Complexities in Dealing with Surprise

The committee has observed and acknowledges the challenges and complexities for naval forces in dealing with potential capability surprise as exemplified in the above three surprise scenarios. In each of the three scenarios, various stakeholders (e.g., operational, intelligence, technical, and acquisition related) should be involved in raising awareness of potential vulnerabilities that capability surprise could expose. Likewise, different entities should be responsible for prioritizing, resourcing, exercising, and developing TTPs against such scenarios. For example, entities ranging from Atlantic and Pacific Fleets, to the Office of Naval Intelligence, to the Office of Naval Research may be involved in scanning for potential surprise. Entities ranging from laboratories to naval operating forces, U.S. Marine Corps Combat Development Command (MCDDC), Navy's OPNAV N2/N6 and N9 organizations, and the Program Executive Offices have key roles to play in prioritizing and developing responses and assuring readiness. Although many stakeholders are involved, there is currently no designated lead working across the Navy to ensure not only recognition of potential capability surprises, but also the required integration and prioritization of efforts to help mitigate their negative impact. A supporting infrastructure or lead integrating authority that can rapidly work through the complexities and that cuts across various naval authorities does not, in most cases, appear to exist.[12] It is crucial to understand that to be effective, counter-surprise efforts not only must scan for and address new or emerging technologies but also must anticipate and search for the use in unforeseen ways of technologies and capabilities that already exist. The Navy must scan for other countries' military exercises, doctrine, and publications as well as technologies.

A Model for Dealing with Potential Surprise

Despite the above complexities, a positive factor is that the committee has been briefed on example programs that have demonstrated the ability to anticipate and respond to surprises with material solutions that are timely, even within the currently acknowledged process-laden, acquisition system. These "exemplar programs" are (1) the Navy SSBN Security Program,[13] (2) the Air Vehicle Survivability Evaluation Program (Air Force Red Team),[14] and (3) the Aegis Ballistic Missile Defense (BMD) Program (whose responsiveness was exemplified by the shoot-down in Operation Burnt Frost of a wayward National Reconnaissance Office satellite.[15] The principles and key "ingredients" for dealing with potential capability surprise in each exemplar program are similar: a stable program and infrastructure; a capability thread that includes research and technology development, modeling and simulation, expert staff, acquisition and industrial capability, and testing infrastructure; and very visible senior leadership support and top cover. Furthermore, several organizations, including the U.S. Marine Corps expeditionary forces, the U.S. Coast Guard operations for responding to natural disasters, OSD Rapid Prototyping, and the Joint Interagency Task Force-South (JIATF-S) organizations, have each developed remarkable resilience for anticipating and responding to rapidly developing, on-the-ground needs.[16] Key common attributes of these successful programs will be discussed and developed more fully as the committee continues its data-gathering work toward producing a final report.

---

[12]The potential impact of a recently announced OPNAV structural reorganization, creating the N9 as a single baron to oversee warfighting programs is a step towards providing structure that may help mitigate capability surprise. The impact of this new structure will be explored further as this study progresses. For additional information on this realignment see "CNO Realigns OPNAV Staff," Navy Office of Information, March 3, 2012; available at http://www.navy.mil/search/display.asp?story_id=65845. Accessed May 24, 2012.

[13]Stephen C. Schreppler, Andrew F. Slaterbeck, and CAPT Christopher J. Kaiser, USN, Office of the Chief of Naval Operations, N97, "SSBN Security Technology Program," presentation to the committee, April 12, 2012, Washington, D.C.

[14]Christopher Roeser, MIT Lincoln Laboratory, "Air Force Red Team Overview," presentation to the committee, May 16, 2012, Washington, D.C.

[15]RADM Brad Hicks, USN, Program Director, Aegis Ballistic Missile Defense, "Aegis Ballistic Missile Defense: Press Briefing, March 19, 2008," presented to the committee by RADM Joseph A. Horn, Jr., USN, Program Executive, Aegis Ballistic Missile Defense, and Conrad J. Grant, Johns Hopkins University Applied Physics Laboratory, May 16, 2012, Washington, D.C.

[16]Benjamin Riley, Director, Rapid Prototyping Technology Office, and Principal Deputy, Deputy Assistant Secretary of Defense for Rapid Fielding, "Rapid Prototyping Perspectives," presentation to the committee, February 29, 2012, Washington, D.C, For additional information on the OSD Rapid Prototyping Office, see National Research Council, 2009, *Experimentation and Rapid Prototyping in Support of Counterterrorism*, National Academies Press, Washington, D.C.

To help guide the approach and understanding needed to address potential capability surprise for U.S. naval forces, the committee has developed a functional framework, shown in Figure 1, consisting of five phases that can be aligned with the development functions, accountabilities, and principles observed in the exemplar programs noted above.

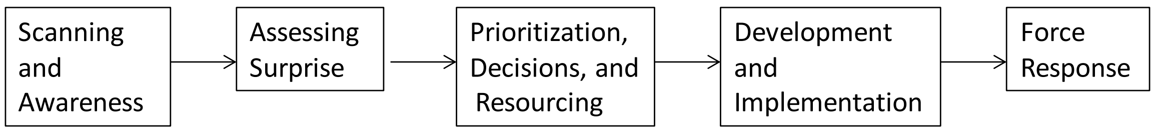

FIGURE 1 Five phases required for mitigating capability surprise. This is a continuous process in which each element informs the other. For example, Force Response adjustments may generate a loop-back in the process. Further reaction to a tactical or Black Swan surprise may enter one of the three right-most phases depending on the nature and timing of the required response.

The five phases—(1) scanning and awareness; (2) assessing the potential for surprise; (3) setting priorities, decision making, and resourcing; (4) development and implementation of tactics and capabilities; and (5) force response—are discussed below. All are necessary to successfully anticipate or react to potential or real surprises. Specifically, the first three phases allow for the impact of a surprise to be assessed, with either a high or low priority as the outcome. In phase 4, several outcomes are possible, including the development of new tactics. At the same time, there is a natural tendency to implement a “quick and dirty” partial solution between phases 4 and 5, and to ignore the limitations that the solution may leave as residual risks to operations. Accordingly, the adequacy of proposed responses should be assessed before any outcome emerges from phase 5.

In the context of the two classes of surprise previously noted, the first three phases would help naval forces better anticipate intelligence-inferred surprises. On the other hand, natural disasters whose occurrence may have been anticipated, but not at the scale of a black swan event (e.g., the March 2011 Fukushima disaster), would enter the framework at phase 4. Moreover, events in-theater may require tactical or strategic operational adjustments in phase 5 as a result of assessing the adequacy of proposed responses.

Scanning and Awareness

Phase 1—Scanning and Awareness—involves scanning the horizon for potential technologies, technical applications, and operational behaviors that could cause surprise, which is defined here as “an adverse event whose outcome is worsened by lack of preparedness or awareness to counter unexpected developments.” The committee’s initial data gathering confirms that certain capabilities are already available to anticipate surprise, including the Office of Naval Research-Global (ONR-G) global science and technology network and the technical intelligence provided by the Office of Naval

Intelligence (ONI).[17] Integration of these and other broader capabilities can inform a potential risk spectrum relating each potential surprise to the standard measures of "likelihood of occurrence" and "operational impact if such an event transpired." More specifically, the committee believes that collaboration among operational, intelligence, and technical experts to fully vet which capability could become surprises, and in what timeframe, in the context of standard risk framework would significantly increase awareness.

Assessing Surprise

Phase 2—Assessing Surprise—includes such key items as effective modeling, simulations analysis, and "red teaming." The somewhat over-used term "red teaming" is applied here to emphasize the dynamic tension required of the operational, technical, and intelligence communities to flesh out potential negative impacts of surprise and prioritize which should be addressed in each timeframe, from short term through long term. Key to the success of this process is application not only of operational experience and campaign-level modeling as it is used currently, but also of the more detailed system- and physics-level modeling, coupled with experiments, as necessary, to determine feasibilities and maturity levels of the potential surprise events as well as their potential operational impacts. Further, the cultural thinking of potential adversaries must be part of the red team formulation. This assessment process must inform decisions about use of resources in subsequent phases.

Prioritization, Decisions, and Resourcing

Phase 3—Prioritization, Decisions, and Resourcing—includes strategic naval planning, budgeting, and evaluation of policy implications for executing a response to the prioritized risks identified in phase 2, and budgeting and allocating resourcing for the response. Here, naval commands with resources must possess the span of control in rapid prototyping, development of tactics, acquisition program adjustments, and force introduction to ensure that the vetted, validated risk response priorities are implemented in a timely manner. A key element that this authority should expect of the assessment process is that first priority will be given to making use of existing systems and capabilities, perhaps with modifications. Such an approach would minimize the expectation of new-start programs that consume much more time and funds.

[17] Walter Jones, Executive Director, Office Naval Research, discussion with the committee on the operations of ONR-Global, February 29, 2012, Washington, D.C. Also, Wayne Mason, Chief Scientist, Office of Naval Intelligence (ONI), "Capabilities Surprise: S&TI Perspective," presentation to the committee, February 28, 2012, Washington, D.C.

Development and Implementation

Phase 4—Development and Implementation—can take several forms, as options, including:

1. Development of new tactics, perhaps using existing assets or technologies in unexpected ways;
2. Development of new variant capabilities within existing programs, e.g., converting the software of a surface-to-air missile to make it a surface-strike missile as was done with the Standard Missile 1 (SM-1) in the 1970s;
3. Rapid prototyping to field a few critical units as either sufficient to meet the need or as a "stop-gap" prior to acquisition program production unit introduction;
4. Use of naval support centers to make changes to systems that are in service but out of production; and
5. More aggressive use of quick reaction capability (QRC) or other authorities.[18]

The options for development and implementation should be considered based on the expected time frame of the emergence of the surprise, the technology readiness level of the requisite counter-capability, and the community resources and schedule capacity to develop the capability. Note that these options may be exercised not only to accommodate anticipated surprises, but also to develop U.S. counter-surprises that could be used to disrupt an adversary in the midst of its unleashing a surprise on U.S. forces to, for example, buy time for a U.S. response.

Force Response

In Phase 5—Force Response—U.S. naval forces test the capability, leveraging the U.S. naval test infrastructure, ensure training and proficiency, and determine the impact of the new capability on a readiness level against surprise. This additional attribute, fleet/forces readiness level against surprise, is the basis from which the preparedness is characterized. As each new urgent need arises, it should be determined whether the surprise element is a driver and, if so, characterized in terms of this attribute.

INITIAL OBSERVATIONS AND INSIGHTS

The five functional elements outlined above, provide the framework as illustrated in Figure 1, which the committee chose to organize its interim report and ultimately address the study's terms of reference. Within this framework, the committee has begun to examine what works well, along with what does not work well (i.e., the obstacles, barriers, and bottlenecks preventing progress) in the three example surprise scenarios

[18]"QRC programs leverage DODI [Department of Defense Instruction] 5000.02 procedures and authorities to speed up the fielding of systems and capabilities to satisfy near-term urgent warfighting needs." See Air Force Instruction 63-114, January 4, 2011, *Quick Reaction Capability Process*, p. 5, para. 1.1.

examined thus far. Accordingly, the committee offers the following initial observations and insights, which will be expanded and built upon in its final report, to help mitigate the impact of potential surprise and to address capability surprise as integral to the naval enterprise.

Observation 1: Scanning and Awareness (Surprise is Unavoidable, Prepare for It!)

The recommendations for surveillance in a 2009 Defense Science Board (DSB) study[19]) differ slightly from those in a 2008 Naval Research Advisory Committee (NRAC) study,[20] and a 2011 report of the Center for a New American Security report (CNAS)[21] has prescriptions to better account for predictive failure. Taken together, these documents form a reasonable starting point for the strategy this committee seeks to develop. The committee categorizes the recommendations of these three reports as either "preparation" or "avoidance" strategies. It specifically notes that DSB 2009 argues that surprise is unavoidable and thus places less emphasis on avoidance strategies and greater emphasis on preparation, flexibility, and speed of response, whereas the NRAC 2008 emphasizes the surveillance aspect; i.e., both of these previous reports deal almost exclusively with the front end of the framework suggested in this report.

It is worthy of note that the DSB 2009 study on capability surprise does not recommend any specific efforts to avoid the effects of surprise. The study concludes by presenting options for decision makers, including the integration and management of surprise at a high enough level to affect senior decision making; among other things, it recommends a pair of definite "surveillance" tasks (scanning and sifting and capability projection). In the present report, scanning and sifting is included in "scanning" and capability projection is part of "awareness."

Scanning and sifting may not appear as a priority in the National Intelligence Priorities Framework (NIPF), but the NIPF nevertheless requires mindfully gathered inputs.[22] There may not be sufficiently high NIPF categories to allow careful collection of surprise-based intelligence. Science and technology information will have to be collected even if there is no "smoking gun" that points to specific subject matter as a concern. Scanning and sifting will be useful only if enough data are used to make good guesses.

---

[19]Defense Science Board. *2009. Report of the Defense Science Board 2008 Summer Study on Capability Surprise*, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., September.

[20]Naval Research Advisory Committee. 2008. *Disruptive Commercial Technologies,* Assistant Secretary to the Navy for Research, Development and Acquisition, Department of Defense, Washington, D.C., June 26.

[21]Richard Danzig. 2011. *Driving in the Dark: Ten Propositions About Predictions and National Security,* Center for a New American Security, Washington, D.C., October.

[22]The National Intelligence Priorities Framework (NIPF) is "a means to capture issues of critical interest to senior intelligence community customers and communicating those issues to the IC for action. The NIPF consists of a dialogue with the senior policy community, a matrix of intelligence priorities, and written guidance to the community explaining critical information needs associated with the priorities in the matrix." See http://www.dni.gov/content/AT/NIPF.pdf. Accessed May 12, 2012.

Capability projection requires the support of technically and operationally qualified experts and an adversarial mindset. Scanning and sifting requires operations in multiple intelligence modes: financial, open-source, human, and other clandestine means. Surveillance may require an organization within the Navy to "own" this responsibility lest it be neglected, and it should be a standing organizational element because surveillance activities need to be ongoing throughout the lifetime of any product enabling a surprise. Awareness is a further extension identified by this committee in which a risk assessment is performed on the capability projections to surmise which are more likely and in what timeframe. The primary product of phase 1 in the committee's proposed framework is a standard risk assessment to gauge which potential surprises represent the greatest risk to naval forces in the expected time frame. The expected timeframe would be based partly on trends in technology readiness level (TRL) of technologies enabling surprises, which can be different for different potential adversaries.

Observation 2: Assessing Surprise (Adopt Nonconventional Thinking!)

In discussions with leaders from the three example programs named above, the committee has observed the following characteristics of a strong anticipatory modeling and analysis capability:[23]

- Team independence;
- Access to a strong base of cross-disciplining technical, and operational expertise;
- An ability to identify threats through campaign-level modeling, system-of-systems simulation, and high-fidelity physics-based models;
- Precise vulnerability modeling, and analysis capability;
- Mechanisms for recommending and/or deploying solutions as necessary;
- Significant steady funding; and
- Focus on a particular mission.

Delving into each of these areas in greater detail, the committee has observed that successful red teams have been granted independence in their assessment of vulnerabilities and evaluation of threat responses.

The committee has also observed that in order to identify threats and anticipate surprise, successful red teams perform modeling and analysis at three levels of fidelity: (1) campaign-level modeling validated through (2) system-of-systems simulation made realistic by (3) high-fidelity, physics-based models. Successful implementation of this multitiered modeling involves an ability to leverage simulations that exist today and are being developed in government laboratories and industry, often by individuals in the small and medium enterprises networks. Running exercises and threat scenarios through

---

[23]As discussed earlier in this report, these example programs are (1) the Navy SSBN Security Program, (2) the Air Vehicle Survivability Evaluation Program (Air Force Red Team), and (3) the Aegis Ballistic Missile Defense Program (whose responsiveness was exemplified by the shoot down of the wayward National Reconnaissance Office satellite, code name Operation Burnt Frost).

this 3-tiered modeling and analysis capability will identify potential threats, allow for response evaluation, and identify potential vulnerabilities. Subsequent, in-depth vulnerability assessment (including precise evaluation of algorithm, software, hardware, or system performance issues) has proven essential to determining the impact of a threat and an effective response.

Following on the theme, as understanding of the implementation of and capabilities for potential surprises mature it is important that independent red teams are engaged with the appropriate balance of skills to ensure as complete an understanding as possible, particularly from military and/or cultural perspectives that may not exist within core organizations. Their own cultural ethos makes U.S. forces vulnerable to unanticipated surprise by determined foes that do not play by U.S. rules or values, as is all too visible in hostage taking and exploitation of civilians. For example, misrepresentation coupled with media exploitation to influence world opinion and rally discontent could provide a fatal punch to a military operation. Social media could be exploited to interfere with the executions of naval missions as in the Surprise Scenario 3 example, flash mob-like surprises.

In this committee's opinion, radical departures from conventional thinking are essential to preparing forces for combat and the development of new tactics. Indeed, various organizations have looked at methods to expand the composition of red teams to achieve diversity in thinking to better represent the adversary. Desired attributes of red teams include cultural, ethnic, and international diversity; are multiservice, multigenerational, multidiscipline makeup; independence, and inclusion of nonmilitary, business, commercial, and academic-sector members. The NRAC 2008 "Commercial Technology Red Cell Experiment" that allowed a group of nonspecialists to brainstorm possible responses to U.S. power projection was an example of a good experiment to predict capabilities.[24] This experiment demonstrated that "credible threats to [naval] forces could be developed from imaginative combinations of commercial products and that the internet functions as an R&D resource and global supply chain for irregular forces." An expected outcome of this activity is the continually updated prioritization of projected surprises based on the risk and expected timeframe from the scanning and awareness function and the projected impact of the most likely surprise capabilities from the red-teaming assessment.

Observation 3: Prioritization, Decisions, and Resourcing
(Evaluate and Prepare to Make Tough Choice Trade Offs!)

With inputs on both (1) risk assessment of emerging technologies and behaviors and (2) technology readiness level (TRL) of those technologies with greater risk of surprise, including projected timeline, from the Scanning and Awareness phase, and with vetted impact prioritization by an authoritative red teaming community from the Assessing Surprise phase, the Prioritization, Decisions, and Resourcing process can focus on the tradeoff options for the most cost-effective, lowest risk to deliver, and timeliest

[24] Naval Research Advisory Committee. 2008. *Disruptive Commercial Technologies*, Assistant Secretary to the Navy for Research, Development and Acquisition, Department of Defense, Washington, D.C., June 26, pp. 5-11.

introduction of surprise mitigation or contingency capabilities. This tradeoff is not trivial, since the relative value of effective, "time-to-market" cost and risk may not be easy to establish and, in fact, may lead to a series of capability releases—one that can be fielded quickly by that is only partially effective and a follow-on release that provides more needed capability at a later time.

In this context, a new program start is a last resort as it is the most expensive and has the longest time to deliver. As this is typically not a new program start, the full assessment of alternatives methodology may not be warranted due to cost and time constraints. A model-based, and perhaps experiment-verified, approach to mitigate or provide contingency against surprise in a straightforward and timely manner is envisioned. If an operational TTP is deemed most appropriate, the Navy's Fleet Forces Command (FFC) or its U.S. Marine Corps or U.S. Coast Guard counterpart would be resourced to develop, train, and field the capability. The operation of the SSBN Security Program provides a very useful and model and example for prioritization, decision making, and resourcing in adopting mitigating actions against an array of potential surprises.[25]

Given the prioritization of needs against surprises presenting high risk to U.S. forces, and based on the potential impacts that have been identified and red teamed, what is needed next is to determine how to best programmatically integrate each surprise-mitigating capability into the force. This determination requires anticipatory analysis and the associated modeling. It is important that each of these mitigation determination efforts be done at the appropriate modeling resolution and scale; i.e, model fidelity, so that the potential program impact is properly understood for operational system and resource requirements development.

The newer models at all levels of detail that have been developed and are being used in various programs are of much higher fidelity as compared to older models, based on evolving computing capabilities and increasingly instrumented test data for validation. These should be used as appropriate to gain sufficiently accurate predictive data and metrics on a potential capability surprise. Further, some of the potential surprises may be of such a nature that new models must be developed to make adequate evaluations.

In performing the model-based analysis, it is also important to define metrics that can put surprises in an operational context that will permit reasonable program tradeoff

[25]In the prioritization of efforts against the access denial scenario, the committee believes the best near-term mitigation to an unfavorable offensive/defensive missile exchange in an anti-access/area denial (A2AD) environment may be to advance the capabilities of networked electronic warfare and creation of cyber attack contingencies for which missile engagements become a last resort. It envisions a program to resource development of nonkinetic system modifications and solutions (electronic countermeasures and deception, cyber intrusion, and directed energy) as a viable prioritization option. A key focus area would be to develop approaches for which the nonkinetic means would be attempted first with sufficient kill assessment indication to provide a reliable input to the decision to engage with kinetic means. Alternatively, if such kill assessment is not readily identified in the near term, the contingency conditions for which nonkinetic measures are most appropriately used separate from kinetic measures should be investigated. For this example, investigations of nonkinetic approaches be considered along the entire threat kill chains.

evaluations to be conducted.[26] For example, the operational concept for unmanned undersea vehicles (UUVs) both as a surprise threat and as a potential U.S. surprise enabler, would likely require new system level and, at least upgraded campaign level models to allow capability impact assessments and development of operational and resourcing requirements.

The committee recognizes that hedging against surprise is not free, and that in a period of declining national security budget "top lines," protecting the flexibility to deal with surprise will perforce come at the direct expense of reductions in traditional naval capabilities.

Observation 4: Development and Implementation (Use New Acquisition Starts Only as a Last Resort!)

In the early stages of this study, the committee was exposed to several critical cases where acquisition of new capability was identified as a process that is inordinately slow, and has the risk of impeding naval forces ability to respond to potential surprises—even for those surprises that fall into the category of intelligence-inferred surprise. For example, in the committee's exploration of potential capability surprises associated with denial-of-space (Scenario #1) discussions with NRL's Tactical Electronic Warfare Division provided examples wherein multiyear acquisition strategies do not appear to be pacing the evolving threat.[27]

A natural and easy response to why it takes so long to field new potential capabilities (in address to potential surprises by adversaries) would be to point to the DOD acquisition system and address changes through an update to the DOD 5000 procedures.[28] Traditionally this has focused on the Federal Acquisition Regulations System (FARS)/Defense Federal Acquisition Regulations Systems (DFARS) procedures with a particular emphasis on the requirements oversight (e.g., the Joint Requirements Oversight Council (JROC), the Joint Capabilities Integration and Development System (JCIDS), etc.) processes.

Unfortunately, while the problem is widely recognized and while numerous studies over the past few years have recommended changes or adjuncts to the DOD 5000 process, little meaningful progress has been made in speeding up the acquisition process. Therefore, as this study moves forward, it is the intent of this committee to take a different approach to the acquisition challenge and focus less on the procurement process and more on the way that we ask industry to develop and provide capability. As with any solution, the answers must not only be capable but also affordable to both the military

---

[26]To date, the committee has received input from several organizations that have modeling and analysis capabilities for use by naval forces, including OPNAV N81, the Naval Research Laboratory, the Office of Naval Research, the Naval War College, the Naval Post Graduate School, the Navy Warfare Development Command, MIT's Lincoln Laboratory, and the Johns Hopkins University Applied Physics Laboratory. One output of this committee's final report is anticipated to be a brief profile of the various type modeling capabilities in organizations at the disposal of U.S. naval leadership.

[27]Naval Research Laboratory, Tactical Electronic Warfare Division, discussion with the committee on naval tactical electronic warfare capabilities and research, May 2, 2012, Washington, D.C.

[28]The Department of Defense acquisition policy is contained in DOD Directive 5000.1.

and industry alike. As suggested earlier, because of the burdens associated with DFARS, a new program start is a last resort, as the most expensive and longest time to deliver.[29]

Several organizations interviewed by the committee indicated that a regulation-burdened acquisition program as an almost insurmountable barrier to preparation and rapid technology response to any capability surprise.[30] The committee recognized an even more foundational issue: that naval surprise normally occurs at the operational and mission level, while naval acquisition organizations and processes are centered on platform delivery. Several promising suggestions were raised during our investigations. Consciously building in capacity and capability reserve (software, hardware, and weapons) in platform payloads, including mission modules for the littoral combat ships, has potential for a cost-effective way to establish agility to respond to surprise. This method minimizes the changes to the capital intensive investments to platforms, while focusing on the packages that actually deliver mission capabilities and offers the emphasis on incremental improvements that may be rapidly implemented. Another suggestion explored formalizing and resourcing mission syndicates composed of the platform, sensor, and weapon research, requirements, resource, and acquisition organizations that provide contributions in delivery of a particular mission's capability. This is an enhancement to OPNAV N95 coordination of a mine warfare enterprise and the naval laboratory warfare center concepts, where the syndicate lead is the holder of resources and "buys" mission platforms, sensors, and weapons from the providers. A mission focus approach to acquisition may inspire a more "systems of systems" engineering approach, and could reach across a board category of mission resources to anticipate and respond to surprise.

Observation 5: Force Response (Exercise, Exercise, Exercise!)

In its current preparation for addressing known gaps that might arise from a new surprise, naval forces typically identify shortfalls in capabilities and flow these into the Department of the Navy and Department of Homeland Security requirements process—including use of urgent operational needs. The process by which gaps are identified, articulated, and prioritized is essential to maximizing naval capabilities and aligning appropriate countermeasures. Current success utilizing the requirements process in

[29]The committee notes with interest the computer-model-based approach that the U.S. Army, in partnership with DARPA is taking to develop the next generation ground combat vehicle, a new start program. The premise is that validated model-based calculation and simulations can expedite passage through the complex acquisition milestones by providing a more quantitative basis for decisions without requiring the building and testing of critical components. This development bears monitoring. LTC Nathan Wiedenman, USA, and Paul Eremenko, Program Managers, DARPA's Tactical Technology Office, discussion with the committee on DARPA's perspectives on capability surprise, February 29, 2012, Washington, D.C.

[30]The committee was briefed by several experts who pointed out acquisition challenges associated with capability and readiness, including discussions with the Deputy Assistant Secretary of the Navy for Research, Development, Test and Evaluation on April 12. For detailed discussion of a concrete example of concern, see U.S. Government Accountability Office, Report to the Committee on Armed Services, House of Representatives, 2012, *Airborne Electronic Attack: Achieving Mission Objectives Depends on Overcoming Acquisition Challenges,* GAO-12-15, Washington, D.C., March.

establishing capabilities for surprise will be reviewed in detail in the final report. Any deficiencies noted by the committee addressed through recommendations.

The committee's initial observations are that naval forces may not be preparing realistically for surprise, such as through reliance on games, modeling and simulation, exercises, and challenging red-teaming that creates and exploits simulated failures in networks and in space capabilities like GPS. Moreover, naval forces must adopt unconventional thinking and a common weakness is letting the designers of systems and concepts do their own red teaming. Experience teaches time and time again that people do not find a lot of flaws with their own work and, as such, independent red teaming is vital. At the same time, it is reasonable to state that red teams are subject to the same cultural influences discussed earlier and, as such, the committee plans to address these and other areas related to red teaming in greater depth in its final report.[31]

Rather, this committee's impressions are that it is more typical for naval forces to exercise assuming chat rooms are operating and networks are functioning, because the denial of these would be "too hard" and/or require substantially more resources than available for the exercises. Yet it is well known that this potential surprise exists. The presence of cyber attacks, for instance, would be so disruptive that it is imperative that top cover be provided to execute any game or exercise with it. The Navy has not trained to operate in a denied environment for many years, though that condition was typical in past practice events some 20 years ago. There is a need to move out aggressively with realistic red-teaming, exercises, and training to establish procedures—such as for voice recognition—that must function in less-optimum environments.

To date, the committee has conducted only preliminary discussion on preparation and readiness with naval fleet. This area will be explored more completely in the final report and will utilize the surprise examples of this study (mitigation of space access, missile magazine depletion and social media surprise), plus potentially other scenarios as 'pathfinders' to develop and exercise the new organizational processes.

Observation 6: Factoring Surprise into Naval Preparedness (Drive a Cultural Shift!)

As discussed earlier in this report, capability surprise is an inherently complex and multifaceted issue. As such, a sustainable and effective approach will likely require a shift in organizational thinking. An organization's ability to react to any type of surprise depends on all levels of leadership to properly assess the situation, understand the overall mission objectives, create a mental decision model on which to act, and have the authority to call on as many diverse naval capabilities as required to respond.

For example, while some surprises arise slowly with ample indicators of a potential capability, the future types of very short-term capability surprises such as suicide bomb attacks on the USS *Cole*, and the 911 World Trade Towers require having

[31] Similar remarks pertain to the statements about the need to shift to a more "surprise ready" organizational culture, and the concomitant need for metrics for surprise readiness. Strong evidential support for the lack of surprise readiness and clear justification of the benefits of moving toward a culture of surprise readiness is important will be important for the committee to consider in its final report.

"meta-organizations"[32] approaches understood and ready to be executed in minutes to hours across the appropriate skill and authority areas. This is important not only to support the immediate responses, but to rapidly examine other areas where an adversary might use these capabilities and very rapidly prepare responses to mitigate those potential capability surprise extensions across the entire regime that might be at risk.

While the committee has not yet explored the potential for generating meaningful metrics that might be used in addressing naval preparedness for dealing with potential capability surprise, we believe a cultural shift is needed towards increased flexibility and agility to react when such surprise or "black swan" events occur. This committee believes that integral to the organizations' effectiveness in dealing with surprise is the issue of metrics, and the potential incorporation of surprise readiness into these metrics. Concepts to develop and integrate the culture of surprise readiness across the naval enterprise will be presented in the final report.

THE WAY AHEAD

All naval forces of the world have been nurtured in an environment that breeds on honing one's ability to deal with surprise. Professionalism as a mariner was often judged by an ability to "read" the winds and seas or to "weather" a storm without lost of limb or ships capability. This single-handed ability to deal with the surprises faced by the captain of a vessel is a classic template that has colored naval operations since 1776.

Thankfully, tremendous advances in technology and information sharing have given captains enhanced tools and data with which to face today's surprises—as long as the event has been previously experienced and a reliable solution known.

However, when a totally new surprise emerges, it takes strong leadership to steer away from "let the captain handle it" or "let the commander and his staff figure this one out." An ad hoc approach to facing a new problem is not likely to result in a high-quality solution, even less likely to be worthy of attribution to the mature and capable naval forces of the United States.

Historically, the Navy, Marines, and Coast Guard have registered some "eye-watering" successes based upon timely and thoughtful ad hoc reaction to surprise. Similarly, some solutions have been less than stellar.

The goal of naval forces must be to always find the best reaction to a surprise, using the fullest measure of knowledge, intelligence, experience, and talent that can be brought to bear.

In the coming months, the committee plans to continue its work to provide an expanded and more comprehensive examination of the topics covered in this interim report and to complete its final report expeditiously. Furthermore, in the preparation of its final report, the committee will explore additional capability-surprise-related topics,

---

[32]Meta-organizations or meta-leadership are used when there are unexpected or fast changing situations such as in public health or homeland security to coordinate/lead across different organizations. An example was the response led by ADM Thad Allan, former Commandant of the Coast Guard, in response to Hurricane Katrina. Additional discussion on meta-organizations is found in the *Scandinavian Management Journal*, 2005, Vol. 21, Issue 4, 2005, pp. 429-449; available at http://www.sciencedirect.com/science/article/pii/S0956522105000813. Accessed June 8, 2012.

such as the interaction of intelligence and operations, and the potential use of offensive means to create surprises of U.S. origin to help mitigate or deter unanticipated surprise. It will also pursue additional interaction with the fleet to explore additional operational concepts for dealing with potential surprise based on hypothesized scenarios. Finally, the committee will explore the potential refinement of organizational concepts and suggested authorities against the committee's postulated framework for addressing surprise.

Enclosure A
Terms of Reference

At the request of the Chief of Naval Operations, the Naval Studies Board of the National Research Council will conduct a study to examine capability surprise—operationally and technically related—facing U.S. Naval Forces, i.e., the U.S. Navy, Marine Corps, and Coast Guard. Specifically, the study will:

(1) Select a few potential capability surprises across the continuum from disruptive technologies, to intelligence inferred capability developments, through operational deployments and assess what U.S. Naval Forces are doing (and could do) about these surprises while mindful of future budgetary declines;

(2) Review and assess the adequacy of current U.S. Naval Forces' policies, strategies, and operational and technical approaches for addressing these and other surprises; and

(3) Recommend any changes, including budgetary and organizational changes, as well as identify any barriers and/or leadership issues that must be addressed for responding to or anticipating such surprises including developing some of our own surprises to mitigate against unanticipated surprises.

This 15-month study will produce two reports: (1) a letter report following the third full committee meeting that provides initial observations and insights to each of the three tasks above; and (2) a comprehensive (final) report that addresses the tasks in greater depth.

Enclosure B
Summary of Committee Meetings and Site Visit

The committee on Capability Surprise for U.S. Naval Forces was first convened in February 2012. Over a period of 4 months, the committee has held three data-gathering meetings which included presentations from outside experts and discussion and debate among the committee. A summary of the committee's meetings, thus far, is provided below:

February 28-March 1, 2012, in Washington, D.C.: First full committee meeting. Briefings on information and intelligence perspectives from the Office of Naval Intelligence Scientific and Technical Center and the National Maritime Intelligence-Integration Office; operational perspectives from the Assistant Deputy Chief of Naval Operations for Operations, Plans, and Strategy (N3/N5B); Marine Corps perspectives from the Commanding General, Marine Corps Combat Development Command/Deputy Commandant for Combat Development and Integration; Office of Naval Research perspectives from the Executive Director, Office of Naval Research; fleet readiness and logistics perspectives from the Deputy Chief of Naval Operations for Fleet Readiness and Logistics (N4); cyber perspectives from the Deputy Commander, U.S. Fleet Cyber Command/Deputy Commander, U.S. TENTH Fleet; rapid prototyping perspectives from the Director, Rapid Prototyping Technology Office, Principal Deputy, Deputy Assistant Secretary of Defense for Rapid Fielding; U.S. Coast Guard perspectives from the Assistant Commandant for Capability; and the Defense Advanced Research Projects Agency (DARPA) perspectives from the program managers, Tactical Technology Office, DARPA.

April 11-12, 2012, in Washington, D.C.: Second full committee meeting. Briefings on capability surprise with perspectives from the Office of the Chief of Naval Operations, Assessment Division (N81); the Assistant Secretary of the Navy for Research, Development, Test and Evaluation; the former Commandant of the U.S. Coast Guard (ADM Thad W. Allen, USCG, retired); the Program Executive Officer, Littoral Combat Ships; the Naval War College and its Modeling and Analysis Department; SSBN (nuclear powered, ballistic-missile-carrying submarine) Security Program; Chief of Naval Operations Strategic Studies Group; and the NRC Committee on Avoiding Technology Surprise for Tomorrow's Warfighter.

May 2, 2012, in Washington, D.C. at the Naval Research Laboratory: Site visit and small group data-gathering session. Briefings from the Tactical Electronic Warfare Division, Naval Research Laboratory on electronic warfare support measures, electronic countermeasures and supporting counter-countermeasures, and studies on modeling and simulation for improving the performance of electronic warfare systems.

May 16-17, 2012, Washington, D.C.: Third full committee meeting. Briefings on capability surprise with perspectives from the NeXTech, Emerging Capabilities Division Rapid Reaction Technology Office, Deputy Assistant Secretary of Defense for Rapid Fielding; Air Force Red Team, Lincoln Laboratory Air Vehicle Survivability Evaluation Program; Space Systems, Strategic and Space Systems, Office of the Assistant Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, and the Office of the Deputy Chief of Naval Operations for Information Dominance (N2/N6), “Operation Burnt Frost,” Program Executive, Aegis Ballistic Missile Defense, and the Air and Missile Defense Department, Johns Hopkins University, Applied Physics Laboratory; the Assistant Chief of Staff for Concepts, Navy Warfare Development Command; and the Pacific Fleet Command, Warfighting Assessment and Readiness.

Enclosure C
Biographies of Committee Members

Jerry A. Krill (Co-Chair) is assistant director for science and technology and chief technology officer at the Johns Hopkins University Applied Physics Laboratory, leading APL's innovation initiative and establishing a new Research and Exploratory Development Department. Previously he served as the JHU/APL assistant director for programs and chief quality officer. In that position Dr. Krill was responsible for all of APL's over 700 programs, implemented an ISO-based quality management system, and co-chaired milestone and program management reviews for APL's NASA science missions and instruments. Previous positions at JHU/APL include executive for air defense programs and head of the Power Projection Systems Department with its precision engagement and "info-centric" operations program portfolios. Dr. Krill's expertise includes combat systems, systems engineering, sensor and weapons networks, and microwave technology. He was a principal in developing the U.S. Navy's Cooperative Engagement Capability that networks air defense systems and, in 2000, led a joint Navy/BMDO working group to develop technical concepts for the Navy's role in national and regional missile defense. He holds 18 patents, and his awards include Innovator of the Year by the *Baltimore Daily Record* and the American Society of Naval Engineers "Jimmie" Hamilton Award. A member of the Naval Studies Board, he has served on NRC and Defense Science Board studies. Other memberships include the Institute of Electrical and Electronics Engineers, American Institute of Aeronautics and Astronautics, National Defense Industrial Association, National Space Society, and the International Council of Systems Engineering. He received his Ph.D. in electrical engineering from the University of Maryland.

J. Paul Reason, ADM, USN (Ret.). (Co-Chair) is an independent consultant having retired from the U.S. Navy with the rank of Admiral after 35 years of service. His background includes naval and joint operations, as well as Department of Defense planning, programming, and budgeting. In his last position, he served as Commander-in-Chief, U.S. Atlantic Fleet, where his responsibilities included the training, maintenance, and readiness of naval forces deployed to the Mediterranean and Caribbean seas, South America, and the Persian Gulf. He was also responsible for the operations of most U.S. Navy bases and facilities along the East and Gulf coasts of the United States, in Puerto Rico, Cuba, and Iceland. He has served on numerous scientific boards and advisory committees, including as a member of the NRC Committee on The "1,000-ship Navy"—A Distributed and Global Maritime Network and the Committee on U.S. Forces' Capabilities for Responding to Small Vessel Threats; he is a member of the Naval Studies Board. He received his M.S. in computer systems management from the Naval Postgraduate School.

Ann N. Campbell is director, Information Solutions and Services, at Sandia National Laboratories. She previously served as senior manager and deputy to the chief technology officer for Cyber Security Science and Technology. In this role she is responsible for developing and implementing an institutional strategy for cyber S&T. She was recently acting director for Sandia's Cyber Security Strategic Thrust, leading the laboratory's activities to expand its cyber workforce and infrastructure, and strategies to provide increased support for Sandia's national security sponsors' cyber missions. Dr. Campbell has also served as deputy for technical programs for the Defense Systems and Assessments Strategic Management Unit (DSA SMU). In that role she advised the DSA SMU vice president regarding the national security programs, was responsible for strategic planning and the investment strategy for the DSA SMU, and assisted with implementation of the laboratory's cyber strategy. From 2003 to 2007, Dr. Campbell led the Assessment Technologies Group in Sandia's Information Systems Analysis Center. She was responsible for development, coordination and oversight of programs focusing on vulnerability assessments and development of national security solutions in information technologies for multiple government sponsors. From 1999 to 2003 she was manager of the Microsystems Partnerships Department which assessed and addressed microelectronics vulnerabilities for a variety of government sponsors. Dr. Campbell led Sandia's program to support the DOD Anti-Tamper Initiative. Dr. Campbell joined the Technical Staff at Sandia in 1985 and had assignments in the Materials and Process Center and Microsystems Science, Technology, and Components Center where she conducted research on the microstructure and physical properties of advanced materials, the physics of microelectronics failures, and the development of advanced microelectronics failure analysis techniques. Dr. Campbell serves on the NRC's Standing Committee on Technology Insight—Gauge, Evaluate, and Review (TIGER). She is a Senior Member of IEEE and served as Vice President Membership for the IEEE Reliability Society and on the Management Committee and Board of Directors for the IEEE International Reliability Physics Symposium. She has over 20 publications and several patents. She holds M.S. and Ph.D degrees in applied physics (materials science concentration) from Harvard University and a B.S. degree in materials engineering from Rensselaer Polytechnic Institute.

Timothy P. Coffey is an independent consultant having recently retired as the Edison Chair at the Center for Technology and National Security Policy at the National Defense University. He graduated from the Massachusetts Institute of Technology in 1962 with a B.S. degree in electrical engineering, and obtained his M.S. (1963) and Ph.D. (1967), both in physics, from the University of Michigan. Dr. Coffey joined the Naval Research Laboratory (NRL) in 1971 as head of the Plasma Dynamics Branch, Plasma Physics Division. In this position, he directed research in the simulation of plasma instabilities, the development of multidimensional fluid and magnetohydrodynamic codes, and the development of computer codes for treating chemically reactive flows. In 1975, Dr. Coffey was named superintendent, Plasma Physics Division; he was appointed associate director of research for general science and technology in 1980. Two years later, Dr. Coffey was named director of research at NRL. Today, he serves on numerous scientific boards and advisory committees such as the recently completed NRC Committee on Operational Science and Technology Options for Defeating Improvised Explosive Devices; he is a member of the Naval Studies Board.

Stirling A. Colgate is a physicist at the Los Alamos National Laboratory and a professor emeritus of physics at the New Mexico Institute of Mining and Technology (New Mexico Tech) where he still continues an experiment on the origin of the magnetic fields of the universe. During World War II he served in various positions in the U.S. Merchant

Marine. After World War II, Dr. Colgate returned to Cornell University completing his B.S. and Ph.D. in nuclear physics, taking up a position as a postdoctoral fellow at Berkeley. In 1952, he moved to Livermore National Laboratory where he performed the diagnostic measurements for the nuclear tests of the hydrogen bomb, just developed at Los Alamos National Laboratory. He was responsible for the design and execution of the "fast nuclear diagnostics, (gamma rays, neutrons, and x-rays)" of the "Bravo" test, 15 Mega Ton equivalent yield, including a dozen vacuum pipe lines 2 miles long. Later, he served as the scientific advisor to the State Department during the test ban negotiations in Geneva where he proposed the mutual need for the detection of nuclear testing in space by use of spy satellites. The surprising Soviet acceptance of this concept pre-dated "peristrika." Dr. Colgate went on to serve as president of New Mexico Tech from 1965 to 1974 where he also conducted research in astrophysics and atmospheric physics. He became an adjunct professor at New Mexico Tech, moving to Los Alamos National Laboratory where he currently continues work in astrophysics and inertial confinement fusion. Dr. Colgate is a fellow of the American Physical Society and the American Association for the Advancement of Science; he is a member of the American Astronomical Society and the American Meteorological Society among others; and he was a founding board member of the Santa Fe Institute. He is a member of the National Academy of Sciences.

Charles R. Cushing is president of C.R. Cushing & Co., Inc., a firm of naval architects, marine engineers, and transportation consultants with offices in New York and Europe. He has been responsible for the design and/or construction of over 250 ocean-going vessels in the United States, Europe, and the Far East. Specifically, he has directed the concept, preliminary, and contract design; strategic planning; plan approval; and supervision of construction of vessels from tankers and container ships to bulk carriers and passenger ships. His work has included new construction, conversion, repair, and refurbishment of vessels. Dr. Cushing has been directly responsible for risk analyses, safety audits, energy audits, and the preparation of the U.S. Coast Guard's *Tankerman's Manual*. He has designed intermodal shipping containers and a myriad of container handling equipment, and he holds a number of patents in maritime and intermodal technology. For 26 years he has taught a course "Ship Acquisition" and for 7 years "Maritime Casualty Investigation" at the United Nation's World Maritime University. For 12 years he has served on the final selection committee of the National Shipbuilding Research Program which sponsors and funds naval and commercial shipbuilding research in the United States. Dr. Cushing has served on scientific boards and advisory committees, and he is a former member of the NRC's Marine Board as well as a current member of the Naval Studies Board. He is a member of the National Academy of Engineering. He received his Ph.D. in maritime studies from the University of Wales Aberystwyth.

Susan Hackwood is executive director of the California Council on Science and Technology (CCST) and professor of electrical engineering at the University of California, Riverside, where her research interests include electrical engineering, signal processing, cellular robotic systems to name just a few. CCST is a not-for-profit corporation comprised of 150 top science and technology leaders sponsored by the key academic and federal research institutions in California, and it advises the state on all aspects of science and technology including nanotechnology, stem cell research, intellectual property, climate change, energy, information technology, biotechnology, and technical workforce development and education. Dr. Hackwood has worked extensively with industry, academic, and government partnerships to identify policy issues of importance and is active in regional and state economic development. Dr. Hackwood is a fellow of the Institute of Electrical and Electronics Engineers and the American Association for the Advancement of Science. Dr. Hackwood received a Ph.D. in solid-state ionics from DeMontfort University. She has served on other scientific boards and advisory committees including a member of the NRC Committee on Improving the Decision Making Abilities of Small Unit Leaders; she is a member of the Naval Studies Board.

Lee M. Hammarstrom is special assistant to the director at the Applied Research Laboratory/Pennsylvania State University. Previously, he was division head at the Naval Research Laboratory, head of the National Reconnaissance Office (NRO) Technology Office, the first chief scientist at NRO, and chief scientist at the Office of the Secretary of Defense for Command, Control, Communications, and Intelligence. Mr. Hammarstrom has broad expertise in areas ranging from technology development to the testing and deploying of military and intelligence systems. He has served on numerous scientific and advisory committees including the Naval Studies Board and a number of other communities. He is an NRO Pioneer. He received his B.S. in electrical engineering from Pennsylvania State University.

Nathaniel S. Heiner is a Northrop Grumman technical fellow as well as director and principal architect, C4I Integration, for Northrop Grumman Corporation's Technology and Engineering Group. He previously worked as the U.S. Coast Guard's senior civilian officer for technology, often acting as the Coast Guard chief information officer. In his prior tour with Northrop Grumman and Federal Data Corporation in the 1990s, he was director of Web/Internet Security Services, focusing on emerging threats to Internet-based systems. He spent his early career as a Unix networking expert, writing networked database applications and peripheral drivers, and securing communications systems law firms, Congress, AT&T, and MCI.uard systems. Specializing in mathematical logic and linguistics, Dr. Heiner earned Ph.D., M.Phil., M.A., and B.A. degrees at Columbia University, where he also taught.

Leon A. Johnson, Brig Gen, USAFR (Ret.) is an independent consultant having recently retired from the United Parcel Service (UPS) after nearly 20 years of service where he served as the Flight Operations Employment Manager and concluded his career working on a special project as the manager of airline manuals. He retired earlier from the U.S. Air Force with the rank of brigadier general after 33 years of service. During his career, General Johnson commanded a fighter squadron, fighter group, was the vice commander of 10th Air Force at the Joint Reserve Base in Ft. Worth, Texas, and served as mobilization assistant to the Assistant Secretary of the Air Force and director operations at Air Education and Training Command. Following the events of 9/11, he served as a director of the Air Force Crisis Action Team in the Pentagon. General Johnson is a member of several organizations including the Air Force Association, Military Officers Association of America, Military Order of World Wars, Veterans of

Foreign Wars, Reserve Officers Association, League of United Latin American Citizens, Women in Aviation, the International Black Aerospace Council, Inc., and Tuskegee Airmen, Inc. General Johnson was elected to a two-year term as the Tuskegee Airmen, Inc. national president in July of 2010. In 2011, General Johnson was awarded a Doctorate in Humane Letters by Tuskegee University. In November 2011, he received an appointment by the Secretary of the Air Force to the Civil Air Patrol Board of Governors, the senior policy making body for that body as established by Public Law. He is a Trustee of the U.S. Air Force Falcon Foundation and is a member of the Naval Studies Board. He received his B.S. in political science from Oregon State University.

Catherine M. Kelleher is professor for public policy at the University of Maryland and senior faculty associate at Brown University's Watson Institute where her research interests include cooperative European defense and security policies, North Atlantic Treaty Organization relations, and international security and arms control. Dr. Kelleher served in the Clinton Administration as personal representative of the Secretary of Defense in Europe and as Deputy Assistant Secretary of Defense for Russia, Ukraine, and Eurasia. She has served on numerous scientific boards and advisory committees, including as a member of the NRC Committee on National Security Implications of Climate Change for U.S. Naval Forces and the NRC Committee on the "1,000-ship Navy—A Distributed and Global Maritime Network. She is a member of the Naval Studies Board. She received her Ph.D. in international relations from the Massachusetts Institute of Technology.

Jeffrey E. Kline is a senior lecturer in the Operations Research Department, and program director, Consortium for Robotics and Unmanned Systems Education and Research (CRUSER), at the Naval Postgraduate School (NPGS). He oversees over 25 interagency and interschool research and educational initiatives related to maritime security, maritime domain awareness, port security, counter-piracy operations, and maritime critical infrastructure with sponsors ranging from the Secretary of the Navy, Office of the Secretary of Defense, Department of Energy, Secretary of the Navy, and the U.S. Coast Guard. He retired as a captain from the U.S. Navy and has over 26 years of extensive naval operational experience including commanding two U.S. Navy ships and serving as deputy operations for Commander, Sixth Fleet, where he participated in theater-wide operational planning. In addition to his sea service, Mr. Kline spent three years as a naval analyst in the Office of the Secretary of Defense. He is a 1992 graduate of the NPGS's Operations Research Program where he earned the Chief of Naval Operations Award for Excellence in Operations Research, and is a 1997 distinguished graduate of the National War College where he earned the Chairman of the Joint Chief's Strategic Writing Award. Mr. Kline's NPGS faculty awards include the 2011 Institute for Operations Research and Management Science Award for Teaching of Practice, the 2007 Hamming Award for interdisciplinary research, 2007 Wayne E. Meyers Award for Excellence in Systems Engineering Research, and the 2005 Northrop Grumman Award for Excellence in Systems Engineering.

Annette J. Krygiel is an independent consultant with expertise in the management of large-scale systems, particularly in regard to software development and systems integration. She served as a distinguished visiting fellow at the Institute for National

Strategic Studies at the National Defense University, where she wrote a book on large-scale system integration. Prior to that, she was director of the Central Imagery Office (CIO), a Department of Defense combat support agency, until CIO joined the National Imagery and Mapping Agency in October 1996. Dr. Krygiel began her career at the Defense Mapping Agency, where she held various positions including chief scientist. Dr. Krygiel previously served as chair of the NRC Committee on the Role of Experimentation in Building Future Naval Forces and recently served as a member of the NRC Committee on U.S. Naval Forces' Capabilities for Responding to Small Vessel Threats. She received her D.Sc. in computer science from Washington University St. Louis.

Thomas V. McNamara is currently director, Strategy and Business Creation, Raytheon Integrated Defense Systems. He served previously as senior vice president and chief technology officer for Textron Systems where he focused on long-term strategic technical investments and program execution to support Textron Systems' businesses. He was responsible for the development of technology and systems to address the emerging challenges in the areas of precision engagement, maritime and land platforms, advanced controls, and aircraft engines. His areas of expertise include guidance, navigation and control; intelligent autonomy; precision weapons delivery; micro-electromechanical sensors; dismounted soldier systems; mission planning; and systems integration for naval submersible and aircraft platforms. He recently served as a member of the NRC Committee on The "1,000-ship Navy"—A Distributed and Global Maritime Network, the Committee on Distribute Remote Sensing for Naval Undersea Warfare, and as co-chair of the Committee on U.S. Naval Forces' Capabilities for Responding to Small Vessel Threats. He received his MBA from Boston College.

Richard W. Mies, ADM, USN (Ret.) is the chief executive officer (CEO) and president of The Mies Group, Ltd. and provides strategic planning and risk assessment advice and assistance to clients on international security, energy, defense, and maritime issues. A distinguished graduate of the U.S. Naval Academy, he completed a 35-year career as a nuclear submariner in the U.S. Navy and commanded U.S. Strategic Command for four years prior to retirement in 2002. Admiral Mies served as a senior vice president and deputy group president of Science Applications International Corporation (SAIC) and as the president and CEO of Hicks and Associates, Inc., a wholly owned subsidiary of SAIC from 2002 to 2007. He also served as the chairman of the Department of Defense Threat Reduction Advisory Committee from 2004 to 2010 and as the chairman of the board of the Navy Mutual Aid Association from 2003 to 2011. He presently serves as the chairman of the Strategic Advisory Group of U.S. Strategic Command, chairman of the Board of the Naval Submarine League, and more recently became a trustee of the U.S. Naval Academy Foundation. He is a member of the Committee on International Security and Arms Control of the National Academy of Sciences, a member of the Boards of Governors of Los Alamos National Laboratory and Lawrence Livermore National Laboratory, and a member of the Board of Directors of Mutual of Omaha Company, Babcock and Wilcox Company, and Exelon Corporation. He also serves on numerous advisory boards. Admiral Mies completed post-graduate education at Oxford University, England, the Fletcher School of Law and Diplomacy, and Harvard University. He holds a Masters degree in government administration and international relations.

C. Kumar N. Patel is the founder, president, and chief executive officer of Pranalytica, Inc., a Santa Monica based company that is the leader in quantum cascade laser technology for defense and homeland security applications. He is also professor of physics and astronomy, electrical engineering, and chemistry at the University of California, Los Angeles (UCLA). He served as vice chancellor for research at UCLA from 1993-1999. Prior to joining UCLA, he was the executive director of the Research, Materials Science, Engineering and Academic Affairs Division at AT&T Bell Laboratories, where he began his career by carrying out research in the field of gas lasers. He is the inventor of the carbon dioxide and many other molecular gas lasers that ushered in the era of high-power sources of coherent optical radiation. Dr. Patel was awarded the National Medal of Science for his invention of the carbon dioxide laser. His other awards include the Ballantine Medal of the Franklin Institute, the Zworykin Award of the National Academy of Engineering, the Lamme Medal of the Institute of Electronic and Electrical Engineers, the Texas Instruments Foundation Founders Prize, and many more. Dr. Patel holds a B.E. in telecommunications from the College of Engineering in Poona, India, and received his M.S. and Ph.D. in electrical engineering from Stanford University. He is a member of the National Academy of Sciences and the National Academy of Engineering. He received his Ph.D. in electrical engineering from Stanford.

Heidi C. Perry is director, Algorithms and Software, at the Charles S. Draper Laboratory, Inc. Previously she was director, Internal Research and Development, at the Draper Laboratory. Her expertise includes guidance, navigation and control; global position system antijam and ground control; precisions weapons delivery command and control, autonomous systems, mission critical software, and C4ISR systems. She served as a member of the NRC Committee on National Security Implications of Climate Change for U.S. Naval Forces and on the NRC Committee on the “1,000-ship Navy—A Distributed and Global Maritime Network. She is a member of the Naval Studies Board. She received her M.S. in computer engineering from the National Technical University.

Gene H. Porter is an adjunct staff member at the Institute for Defense Analyses. His areas of expertise include national security planning and weapons systems development and in defining the defense planning scenarios that are intended to guide the development of the U.S. military force structure. Mr. Porter formerly served as the Director of Acquisition Policy and Program Integration at the Office of the Under Secretary of Defense for Acquisition. He has served on numerous scientific boards and advisory committees, including as chair of NRC Committee for Mine Warfare Assessment and more recently as a member of the NRC Committee on U.S. Naval Forces’ Capabilities for Responding to Small Vessel Threats. He received an M.S. in physical oceanography from the University of Washington.

Dana R. Potts is the senior Navy experienced systems engineer principal for the Horizontal Integration Operational Concepts Team at Lockheed Martin Aeronautics Advanced Development Programs (Skunk Works) having retired from the U.S. Navy with the rank of captain. He is responsible for projects that include any maritime component. He was scenario lead for two corporate-level Marine Air Ground Task Force Experiments, creating the scenarios and coordinating the efforts involving aeronautics, electronic systems, enterprise operations, information systems and global solutions, mission systems, and space systems. He also led the man-in-the-loop experiment studying the attributes of the Skunk Works concept for the Unmanned Carrier Launched Airborne Surveillance and Strike system. He has received two Lockheed Martin Nova awards for projects involving teamwork with these scenarios. Prior to joining Lockheed, Mr. Potts completed over 28-years with the U.S. Navy with leadership positions both ashore and at sea, primarily in tactical aviation flying the F4 Phantom and the F14 Tomcat. Significant operational experience included command of Fighter Squadron ONE FIVE FOUR and command of Carrier Air Wing SEVENTEEN in combat operations. He was also a fellow with the CNO Strategic Studies Group XXIII that conducted research, developed innovative concepts, and made recommendations to the Chief of Naval Operations concerning the "Navy After Next." He earned a B.S. in computer science from Texas A&M and an M.S. in national security strategy from the National Defense University, National War College.

John E. Rhodes, LtGen, USMC (Ret.) is an independent consultant having retired from the U.S. Marine Corps with the rank of Lieutenant General after 36 years of service. His background is in development of warfighting concepts and in the integration of all aspects of doctrine, organization, training and education, equipment, and support and facilities to enable the Marine Corps to field combat-ready forces. In his last position, he served as commanding general of the U.S. Marine Corps Combat Development Command, where his responsibilities included assessments of current and future operating environments and adaptation of the Corps' training infrastructure and resources in order to ensure that integrated capabilities were delivered to the combatant commanders. General Rhodes has served on numerous scientific boards and advisory committees, including as a member of the NRC Committee on Manpower and Personnel Needs for a Transformed Naval Force and the Committee on U.S. Forces' Capabilities for Responding to Small Vessel Threats; he is a member of the Naval Studies Board. He received an M.S. in systems management from the University of Southern California.

Robert M. Stein is an independent consultant, having served previously as vice president of the Raytheon Company until he retired in 2000. He managed Raytheon's Advanced Systems Office. He was responsible for the formulation and implementation of advanced systems and concepts for current and future Raytheon product lines. Mr. Stein led concept formulation and advanced development studies for the company and the U.S. Government addressing the advanced strategic and tactical defense needs for the United States and many of our allies. These have spanned the spectrum from early concept studies on the protection of the continental United States (CONUS) and the defense of retaliatory forces against nuclear attack in the 1960s, to tactical defense of land and sea forces in the 1970s, to defense of CONUS, theater, and allied military and civilian assets against air, cruise, or ballistic missile attack in the 1980s and 1990s. He has participated in a number of Army Science Board, Air Force Scientific Advisory Board, and Navy Research Advisory Committee task forces. He has served on and/or co-chaired many Defense Science Board Task Forces and Summer Studies and is currently a senior fellow on the Board. He also currently serves as a member of the Missile Defense Agency Advisory Committee. Mr. Stein performed undergraduate work in electrical engineering at Massachusetts Institute of Technology (MIT) and has performed extensive graduate studies at MIT and Boston University in mathematical physics. He holds a patent in multibeam radar antenna techniques, has published numerous articles on defense technology and related policy issues, and has taught a variety of courses on radar and information theory. In 1992, Raytheon awarded Mr. Stein the Thomas L. Phillips Award of Excellence in Technology—the company's highest recognition for technical achievement. He earned his BSEE from the Massachusetts Institute of Technology.

Vincent Vitto is the retired president and chief executive officer of Charles Stark Draper Laboratory, Inc., where he served for 9 years until 2006. Since 2006, he has been working as an independent consultant. Before joining Draper in 1997, he spent 32 years at Massachusetts Institute of Technology's Lincoln Laboratory, rising to Assistant Director of Surface Surveillance and Communications. He holds an M.S. in physics from Northeastern University and a B.S. in physics from the Polytechnic Institute of Brooklyn. Currently, Mr. Vitto is Chairman of the Board of Directors of Mercury Computer Systems, a member of the QinetiQ North America Proxy Board of Directors, and a member of the Board of Trustees for the Aerospace Corporation. He is also a member of the National Associates of the National Academies and a fellow of the American Institute of Aeronautics and Astronautics. He serves on the Board of Trustees at the Massachusetts Eye and Ear Infirmary. Mr. Vitto has received numerous public service awards in his career including the Meritorious Public Service Award and Superior Public Service Award from the Department of the Navy, the Decoration for Exceptional Civilian Services from the Department of the Air Force, and in 2009 the Department of Defense Medal for Distinguished Public Service Award. He has served on numerous scientific boards and advisory committees, including the Intelligence Science Board, the Defense Science Board, National Reconnaissance Office Technical Advisory Group, and the National Geospatial Intelligence Agency Advisory Group. He also chaired the Naval Studies Board from 1999 to 2004.

David A. Whelan is chief scientist, Boeing Defense, Space, and Security, and Vice President, Strategic Innovation, Phantom Works, at the Boeing Company. His areas of expertise include defense research, development, and enabling technologies, such as autonomous vehicles and space-based moving target indicator radar systems. Prior to joining Boeing, he served as Director of the Tactical Technology Office at the Defense Advanced Research Projects Agency. His high-technology development experience includes roles as a research physicist for Lawrence Livermore National Laboratory, and as a lead engineer at Northrop Grumman. Dr. Whelan has served on numerous scientific boards and advisory committees, including the Defense Science Board, the Air Force Scientific Advisory Board, and the NRC Committee on Research, Development and Acquisition Options for U.S. Special Operations Command, and the NRC's Committee on National Security Implications of Climate Change for U.S. Naval Forces and the NRC's Americas Climate Choices: Panel on Advancing the Science of Climate Change; he is Vice Chair of the Naval Studies Board. He is a member of the National Academy of Engineering. He earned his Ph.D. in physics from the University of California, Los Angeles.

Peter G. Wilhelm is director of the Naval Center for Space Technology (NCST) at the Naval Research Laboratory (NRL). He is responsible for the technical and managerial leadership of the NCST's mission, which is to preserve and enhance a strong space technology base and provide expert assistance in the development and acquisition of space systems which support naval missions. During Mr. Wilhelm's tenure, the space program at NRL has grown from a branch to a division to a Center. Under his direction, NCST and the Navy have achieved numerous successes and "firsts" in space including the Global Positioning System satellite and the highly successful Clementine Deep Space Mission, which demonstrated the capability of, and has become the model for low-cost, high-value space exploration. Mr. Wilhelm's achievements include contributions to the design, development and operation of 100 scientific and fleet-support satellites. Mr. Wilhelm is a Fellow for the American Institute of Aeronautics and Astronautics (AIAA) and the Washington Academy of Science. He is a member of the National Academy of Engineering. He received his B.S. in electrical engineering from Purdue University.

John D. Wilkinson is an assistant group leader at MIT Lincoln Laboratory, in the Air Defense Techniques Group of the Air and Missile Defense Technology Division. He has worked at Lincoln Laboratory since 1998, beginning in the Intelligence, Test, and Evaluation Group. After a decade of radar data analysis, radar system engineering, and radar testing experience, Mr. Wilkinson now serves as the Lincoln Laboratory program manager for several science and technology programs related to air defense. In this role he proposed and led the development of a ultra high frequency radar installed on Lincoln Laboratory's Boeing 707, and helped design, build, and deploy two other radar systems as well. He was awarded a B.S. in physics from the University of Massachusetts at Amherst and an M.S. in electrical engineering from Tufts University.

Enclosure D
Acronyms and Abbreviations

BMD	ballistic missile defense
CNAS	Center for a New American Security
CNO	Chief of Naval Operations
DARPA	Defense Advanced Research Projects Agency
DFARS	Defense Federal Acquisition Regulations System
DSB	Defense Science Board
FARS	Federal Acquisition Regulations System
FFC	Fleet Forces Command
GPS	Global Positioning System
ISR	intelligence, surveillance, and reconnaissance
JCIDS	Joint Capabilities Integration and Development System
JIATF-S	Joint Interagency Task Force-South
JROC	Joint Requirements Oversight Council
MCCDC	Marine Corps Combat Development Command
MIT	Massachusetts Institute of Technology
NIPF	National Intelligence Priorities Framework
NRAC	Naval Research Advisory Committee
NRC	National Research Council
NRL	Naval Research Laboratory
NSB	Naval Studies Board
ONI	Office of Naval Intelligence
ONR	Office of Naval Research
ONR-G	Office of Naval Research-Global
OPNAV	Office of the Chief of Naval Operations
OSD	Office of the Secretary of Defense
QRC	quick reaction capability
R&D	research and development
SM	Standard Missile
SSBN	ballistic missile submarine
SSN	nuclear-powered submarine

TRL	technology readiness level
TTPs	tactics, techniques, and procedures
UUV	unmanned undersea vehicle