Avoiding Technology Surprise for Tomorrows Warfighter: A Symposium Report

Committee for the Symposium on Avoiding Technology Surprise for Tomorrows Warfighter; National Research Council

ISBN: 0-309-14229-6, 70 pages, 6 x 9, (2009)

avoiding technology surprise for tomorrow's warfighter
a symposium report

Committee for the Symposium on
Avoiding Technology Surprise for Tomorrow's Warfighter

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, N.W. 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 is a report of work supported by contract HHM40205D0011 between the Defense Intelligence Agency and the National Academy of Sciences. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the view of the organizations or agencies that provided support for the project.

Cover: Front cover design by Shannon Thomas. Top image courtesy of the United States Department of Defense; bottom image courtesy of Digital Vision/Flying Colours Ltd.

International Standard Book Number-13: 978-0-309-14228-1
International Standard Book Number-10: 0-309-14228-8

Limited copies are available from:

Division on Engineering and Physical Sciences
National Research Council
500 Fifth Street, N.W.
Washington, DC 20001
(202) 334-3118

Additional copies are available from:

The National Academies Press
500 Fifth Street, N.W.
Lockbox 285
Washington, DC 20001
(800) 624-6242 or (202) 334-3313
(in the Washington metropolitan area)
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 FOR THE SYMPOSIUM ON AVOIDING TECHNOLOGY SURPRISE FOR TOMORROW'S WARFIGHTER

RUTH A. DAVID, *Chair*, ANSER, Arlington, Virginia
STEVEN R.J. BRUECK, University of New Mexico
ANN N. CAMPBELL, Sandia National Laboratories
STEPHEN W. DREW, Drew Solutions, Inc., Summitt, New Jersey
JOHN GANNON, BAE Systems
SHARON C. GLOTZER, University of Michigan
CHRISTOPHER C. GREEN, Wayne State University
LESLIE GREENGARD, Courant Institute, New York University
DIANE E. GRIFFIN, Johns Hopkins University
J.C. HERZ, Batchtags, Inc.
J. JEROME HOLTON, Tauri Group
FREDERICK R. LOPEZ, Raytheon Company
GILMAN G. LOUIE, Alsop Louie Partners, San Francisco
JULIE J.C.H. RYAN, George Washington University
JAMES B. SMITH, Raytheon Company
DIANNE S. WILEY, The Boeing Company

Staff

MICHAEL A. CLARKE, Lead DEPS Board Director
DANIEL E.J. TALMAGE, JR., Study Director
CARTER W. FORD, Program Officer
LISA COCKRELL, Associate Program Officer
ERIN C. FITZGERALD, Associate Program Officer
SARAH CAPOTE, Research Associate
SHANNON THOMAS, Program Associate

Preface

The symposium described in this report represents a new venue for the ongoing engagement between the National Research Council's (NRC's) TIGER (Technology Insight—Gauge, Evaluate, and Review) Standing Committee, the scientific and technical intelligence (S&TI) community, and the consumers of S&TI products. TIGER's sponsor—the Defense Intelligence Agency's (DIA) Defense Warning Office (DWO)—described this symposium as the first annual gathering of this type, intending that both the personal interactions that occurred throughout the symposium, as well as this report and similar products from future sessions, would help drive systemic strengthening of U.S. S&TI capabilities.

We wish to express our appreciation to the members of the Committee for the Symposium on Avoiding Technology Surprise for Tomorrow's Warfighter for their thoughtful contributions to the symposium discussions as well as to the generation of this report. We also are grateful for the active participation of many members of the defense community in this symposium, especially those contributing to the discussion as panelists and invited speakers, as well as to the members of the S&TI community for their support. The committee would also like to express sincere appreciation for the support and assistance of the NRC staff, including Michael Clarke, Daniel Talmage, Carter Ford, Lisa Cockrell, Erin Fitzgerald, Sarah Capote, and Shannon Thomas.

Ruth A. David, *Chair*
Committee for the Symposium on Avoiding
Technology Surprise for Tomorrow's Warfighter

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 (NRC'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:

Jim Carafano, The Heritage Foundation,
Natalie W. Crawford (NAE), RAND Corporation,
Lawrence A. Delaney, Titan Corporation (retired),
Alan H. Epstein (NAE), Pratt & Whitney,
Robert J. Hermann (NAE), Global Technology Partners, LLC,
Alton D. Romig, Jr. (NAE), Sandia National Laboratories, and
Robert M. Shea, Smartronix, Inc.

Although the reviewers listed above have 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 Chris G. Whipple (NAE), ENVIRON. Appointed by the NRC, 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

Acronyms and Abbreviations

AT&L	Acquisition, Technology, and Logistics
COCOM	combatant command
DARPA	Defense Advanced Research Projects Agency
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DTWS	Defense Technology Warning System
DWO	Defense Warning Office
IC	intelligence community
IED	improvised explosive device
ISR	intelligence, surveillance, and reconnaissance
ITAR	International Traffic in Arms Regulations
(US)JFCOM	United States Joint Forces Command
JWICS	Joint Worldwide Intelligence Communication System
NASA	National Aeronautics and Space Administration
NRC	National Research Council
NSF	National Science Foundation
ODUSD	Office of the Deputy Under Secretary of Defense
ONR	Office of Naval Research

OUSDI	Office of the Under Secretary of Defense, Intelligence
Q&A	question and answer
R&D	research and development
S&T	science and technology
S&TI	scientific and technical intelligence
SIPRNet	Secret Internet Protocol Router Network
USSOCOM	United States Special Operations Command
TIGER	Technology Insight—Gauge, Evaluate, and Review

1

Motivation for the Symposium

This symposium report[1] summarizes the themes that were identified and discussions that occurred over the course of a 1-day symposium, "Avoiding Technology Surprise for Tomorrow's Warfighter," held at the National Academy of Sciences on April 29, 2009. The report and the symposium itself were produced under the auspices of the National Research Council's (NRC's) Committee for the Symposium on Avoiding Technology Surprise for Tomorrow's Warfighter, sponsored by the Defense Intelligence Agency's (DIA's) Defense Warning Office (DWO). This ad hoc symposium committee was composed of members of the Standing Committee for Technology Insight—Gauge, Evaluate, and Review (TIGER).

An earlier NRC report, *Avoiding Surprise in an Era of Global Technology Advances*, provided the intelligence community (IC) with a methodology that the IC had not previously possessed to gauge potential implications of emerging technologies for U.S. warfighting capabilities (NRC, 2005). This methodology is now used by parts of the IC as a tool for assessing potential future national security threats stemming from emerging technologies. As part of a continuing relationship with the TIGER Standing Committee, the DIA/DWO identified the need to gather insights and perspectives from warfighters that consume scientific and technical intelligence (S&TI), and asked the NRC to host this symposium for that purpose.

[1]In accordance with NRC guidelines for workshop reports, this document does not include consensus findings and recommendations and instead presents the views expressed by individual participants in the symposium.

SYMPOSIUM OBJECTIVE

The purpose of the symposium and of this report is to highlight key challenges confronting the S&TI community and to explore potential solutions that might enable the S&TI community to overcome those challenges. The symposium objective, as described in the symposium brochure, is shown in Figure 1-1.

The goal of the symposium was to capture comments and observations from individual members of the symposium panels, composed of representatives from combatant commands (COCOMs) and supporting governmental organizations, together with those of symposium participants, in order to elucidate concepts and trends, knowledge of which could be used to improve the Department of Defense's (DOD's) technology warning capability. The panels were moderated by members of the ad hoc symposium committee. Topics addressed included issues stemming from globalization of science and technology (S&T), challenges to U.S. warfighters that could result from technology surprise, examples of past technological surprise, and the strengths and weaknesses of current S&TI analysis.

This symposium featured invited presentations and included discussions on topics of interest to the DIA/DWO. (The full symposium agenda can be found in Appendix A.) Kiosks were also set up to showcase the Defense Technology Warning System prototype, recent NRC reports issued under the auspices of the TIGER Standing Committee, experimental verification efforts sponsored by DIA, relevant data-mining and visualization techniques developed at the Naval Surface Warfare Center, and technology forecasting by the Institute for the Future. Topics addressed at the symposium included:

- Discussion of pre-workshop questionnaire data collected by the DIA/DWO;
- General discussion of trends in S&T issues of interest to the sponsor, with particular emphasis on challenges to U.S. warfighters stemming from technology surprise;
- Examples of technological surprise experienced by a cross section of intelligence and military communities; and
- Identification of strengths and observation of shortfalls in S&T intelligence analysis from the perspective of participating consumers of that intelligence.

This report summarizes the key themes from and views expressed by symposium participants. Although the NRC symposium committee (see Appendix B) is responsible for the overall quality and accuracy of the report as a record of what transpired at the symposium, the views described in the workshop report are not necessarily those of the committee. Box 1-1 provides the statement of task for the symposium activity.

Avoiding Technology Surprise for Tomorrow's Warfighter Symposium

Symposium Objective:

The goal of the Avoiding Technology Surprise for Tomorrow's Warfighter Symposium is to capture comments and observations from warfighter panels and participants, in order to elucidate trends that can be used to improve the Department of Defense's technology warning capability. The panels will be moderated by members of the National Academies' Standing Committee for Technology Insight-Gauge, Evaluate, and Review (TIGER). Topics addressed will include science and technology (S&T) issues, challenges to U.S. warfighters that could result from technology surprise, examples of past technological surprise, and the strengths and shortfalls of current S&T intelligence analysis.

The key themes of the symposium will be summarized in an unclassified report by The National Academies.

FIGURE 1-1 Objective of the symposium as stated in the symposium brochure.

BOX 1-1
Committee for the Symposium on
Avoiding Technology Surprise for Tomorrow's Warfighter

Statement of Task

An ad hoc committee, composed of members of the Standing Committee on Technology Insight—Gauge, Evaluate, and Review (TIGER), will convene a 1-day symposium with the theme "Avoiding Technology Surprise for Tomorrow's Warfighter." This event will feature invited presentations and include discussions on science and technology topics of interest to the sponsor. The committee will:

- Attend and participate in all symposium sessions;
- Capture comments and observations from the panel discussions, and elucidate any trends presented in the discussions; and
- Produce a report that summarizes the themes of the symposium, with specific emphasis on challenges to U.S. warfighters involving technology surprise covered in the presentations and discussions.

SYMPOSIUM PARTICIPANTS

There were approximately 140 symposium participants in attendance, including both producers and users of S&TI as well as symposium committee members and representatives from other governmental and nongovernmental organizations with an interest in the topic of emerging technologies and technology surprise. Participant demographics are shown in Figure 1-2. A complete list of the organizations represented by symposium attendees is included in Appendix C.

All participants heard from the featured speakers and broke into two groups for the panel discussions. The break-out sessions included invited panelists, committee members (some of whom served as moderators), and attendees.

SETTING THE SCENE

A major challenge inherent in technology forecasting was illustrated through reference to an experiment conducted by the *Wall Street Journal* (Anders, 2008). In 1998 a group of executives, academics, and entrepreneurs was asked to predict what the world would look like 10 years later, with an emphasis on technological advances. While their forecasts were relatively accurate in terms of technical

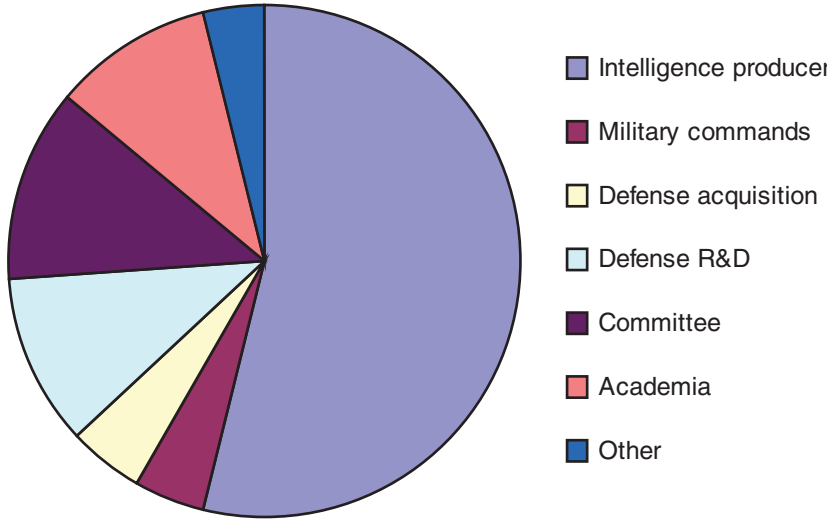

FIGURE 1-2 Distribution of symposium attendees according to S&TI role.

specifications, they were unable to anticipate how that technology would be put to use. This theme recurred throughout the NRC's 1-day symposium as many participants emphasized the need to anticipate how adversaries might use specific technologies rather than simply the availability of raw technical capabilities.

Prior to the symposium, the DIA/DWO distributed questionnaires to selected governmental participants to elicit their perspectives regarding key topics to be discussed during the symposium. Responses were received from the major stakeholder communities—including COCOMs, defense acquisition, defense research and development (R&D), and S&TI producers. The results were tabulated and shown graphically during the opening session to help set the scene for the subsequent panel discussions. While the sample was small and the results not statistically significant, the distribution of responses served to focus and stimulate panel discussions. The charts shown here as Figures 1-3 through 1-6 were shared with symposium participants and are summarized below. Additional charts shown during this opening session are provided in Appendix D.

As is evident from the charts and the discussion they stimulated, symposium participants were increasingly concerned about the potential for technology surprise, and nearly half of the respondents indicated that surprise had been experienced in the past. Furthermore, participants regarded S&TI as very important today and saw the need for increasing support from this intelligence mission area in the future. The responses summarized in these charts were corroborated by symposium attendees throughout the day.

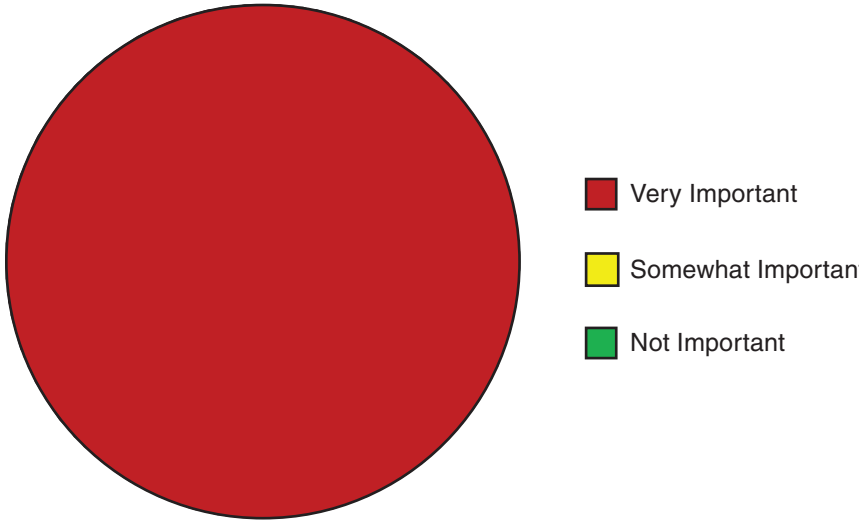

FIGURE 1-3 Results in response to the question, How important is scientific and technical intelligence (S&TI) analysis to you in your position? SOURCE: Survey by DIA/DWO.

Participants spanning mission areas from current warfighting to research in support of future military capabilities agreed that S&TI—understanding the technology-based capabilities of others—is "very important" as indicated in Figure 1-3.

Globalization, commercialization, and commoditization were identified as contributors to the concerns regarding the potential for technology surprise indicated by the responses summarized in Figure 1-4.

A number of symposium participants identified specific instances of technology surprise experienced in the past, as suggested by the responses graphed in Figure 1-5.

More than three-quarters of the respondents to the DIA/DWO's pre-symposium questionnaire indicated that their need for S&TI would grow in the future, as indicated in Figure 1-6. This belief was reinforced during panel discussions throughout the day.

Other pre-symposium questions were designed to elicit perspectives on S&TI time horizons of interest, the basic level of satisfaction with current S&TI support, and a sense of what S&TI delivery mechanisms might be of value to S&TI consumers. The summarized responses in Appendix D were used to stimulate the panel discussions.

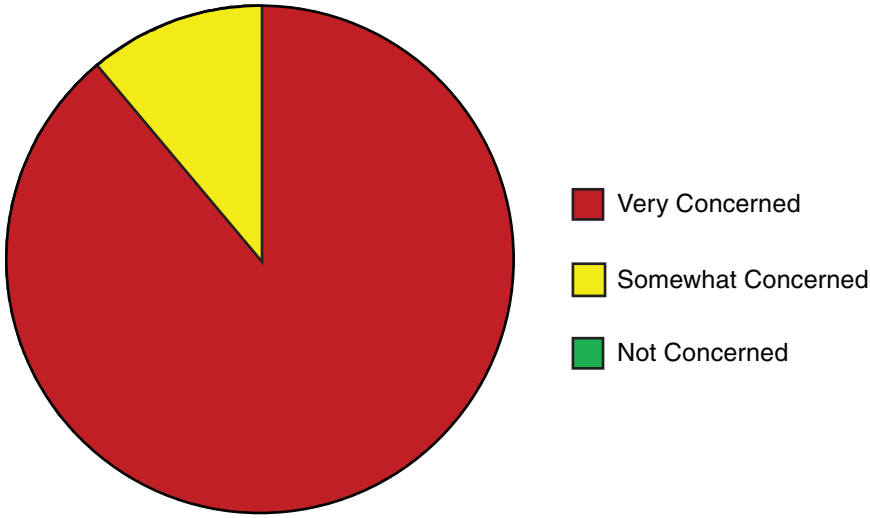

FIGURE 1-4 Results in response to the question, How concerned are you about the potential for technology surprise? SOURCE: Survey by DIA/DWO.

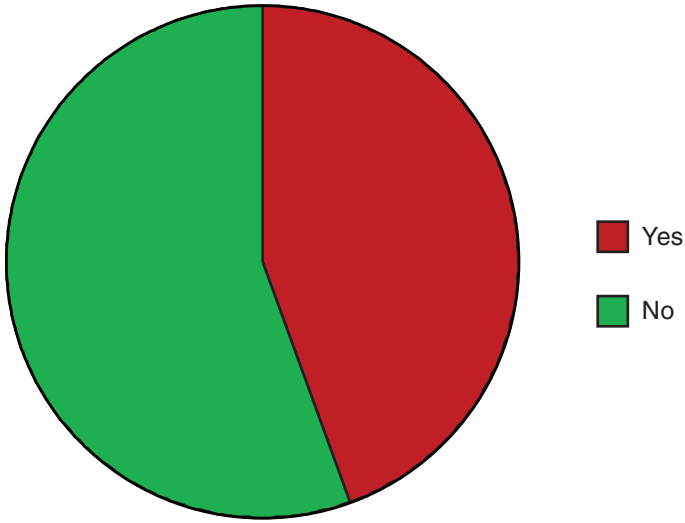

FIGURE 1-5 Results in response to the question, Have you ever experienced surprise? SOURCE: Survey by DIA/DWO.

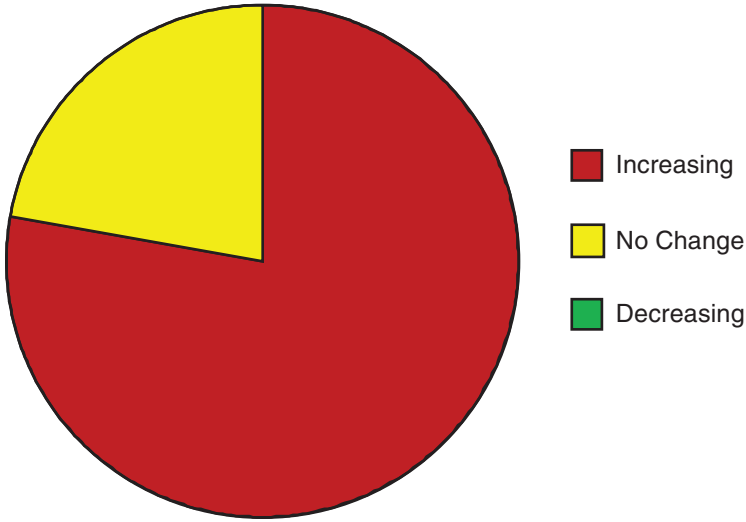

FIGURE 1-6 Results in response to the question, Do you see your need for S&TI support increasing or decreasing in the future? SOURCE: Survey by DIA/DWO.

THIS REPORT

Chapter 1—this chapter—describes the motivation for the symposium, sponsor expectations for the report, and information presented to stimulate a dialogue. Current challenges for technology warning, as identified by symposium participants, are described in Chapter 2, and discussion regarding potential S&TI solutions is summarized in Chapter 3.

The symposium featured three distinguished guests with unique perspectives on the S&TI community: Director of National Intelligence Dennis Blair; former Under Secretary of Defense (Acquisition, Technology, and Logistics (AT&L)) Jacques Gansler; and the Director of the Battlespace Awareness Portfolio in the Office of the Under Secretary of Defense, Intelligence (OUSDI), Robert Hegstrom. Summaries of discussions that took place with each of these three speakers are provided in Chapter 4. Chapter 5 contains a distilled list of key themes derived from discussions throughout the day.

REFERENCES

Anders, George. 2008. Predictions of the past. *Wall Street Journal*. January 28.

NRC (National Research Council). 2005. Avoiding Surprise in an Era of Global Technology Advances. Washington, D.C.: The National Academies Press. Available from http://www.nap.edu/catalog.php?record_id=11286. Last accessed May 6, 2009.

2

Current Technology Surprise Problems

The symposium attendees were divided into two parallel panel discussion groups, each of which was presented with the same list of starter questions to motivate discussion. (For a list of these questions, see Appendix E.) An effort was made to balance the distribution of organizational perspectives across the two groups such that a single viewpoint was less likely to dominate the discussion. Both the panelists and the audience were active participants in the discussions. While discussions were not restricted to the questions provided, the moderators used those questions to focus the two independent discussions around common issues and to address the symposium goal of elucidating trends that could be used to improve the DOD's technology warning capability.

This chapter summarizes discussion topics from the first panel session that emphasized understanding current issues related to technology surprise from the perspective of COCOMs and other key S&TI consumer communities as well as S&TI producers.

DEFINING TECHNOLOGY SURPRISE

From the discussion, it quickly became apparent that there is no standard definition of "technology surprise." The following four-fold definition was provided by the DIA/DWO sponsor.

- **Type 1: A major technological breakthrough in science or engineering.** These are generally rare events, enabled by experts within the field.
- **Type 2: A revelation of secret progress** by a second party which may have an unanticipated impact. For example, at the end of the Cold War,

the United States was surprised to learn that the Soviet Union had not stopped its production of biological agents as Moscow had pledged more than 21 years earlier during the Nixon Administration.

- **Type 3: Temporal surprise,** when a party makes more rapid development or advancement in a particular technology than anticipated, such as recent progress in North Korea's nuclear program. This type of surprise is often facilitated by technology transfer that accelerates progress beyond a traditional linear development cycle.
- **Type 4: Innovative technology applications,** such as using an airplane as a weapon on September 11, 2001, or increasing the lethality of improvised explosive devices (IEDs) in Iraq. Such innovations do not necessarily require technical expertise, but rather the creativity to use available resources in a new way.

AREAS OF CONCERN

Participants acknowledged that technology R&D is a global enterprise. The United States is no longer assured dominance in that enterprise, but still appears to cling to an S&T foreign policy that is U.S.-centric. Panel participants expressed that this policy has been more effective at keeping technology out (i.e., limiting U.S. ability to exploit advances made elsewhere in the world) than at keeping technology in (i.e., limiting the access of others to U.S. advanced technologies).

Much of the discussion emphasized the point that the U.S. government is not adequately staffed, networked, or integrated to avert technology surprise. Within the IC specifically, there is a need to integrate S&T and regional analysis, along with socio-cultural input, to better assess potential threats stemming from the widespread availability of technology. In the IC, there is a need for more scientists and technologists who understand the intelligence community culture and can help to both craft focused collection requirements and provide scientific data and insight on a continuing basis. It was acknowledged that even individuals with deep technical expertise may be poorly equipped to translate that knowledge into discrete indicators that would focus intelligence collection assets. Furthermore, the need to understand not only the raw technical capability but also how that capability might be used against the United States on the battlefield was highlighted as an issue of particular importance.

Participants felt that the current paucity of scientists and engineers in the S&TI community is sometimes reflected in the quality and content of S&TI currently produced and distributed to consumers. It was specifically mentioned that, in recent decades, the number of S&TI analysts with postgraduate degrees in S&T fields has decreased by a factor of five. The magnitude of this decrease, together with the decline in the number of American students being trained as scientists and engineers, was a common concern.

Beyond related topics of general concern regarding U.S. technical dominance,

other discussion topics emphasized the S&TI creation and dissemination process, a new paradigm for the use of information, and additional specialized technical areas of concern.

Process-Specific Concerns About Technology Surprise

Many participants' concerns focused on the end-to-end S&TI process, from data collection to analysis to dissemination to the end user. Below are some key observations of panel participants.

- A disconnect exists between the requirements, collection, and analysis communities. Participants articulated sometimes divergent understandings of the responsibilities and missions of the component communities. Specifically, participants observed a "lack of shared meaning" across the community, and some expressed frustration with what was seen as excessive bureaucratic finger pointing in place of a discussion of how to fix problems.
- Participants' views regarding the relevance and potential impact of emerging social networking technologies revealed significant disagreement. In discussion of specific tools (such as FaceBook, Twitter, and other social networking platforms), disparate views surfaced about both the importance and the relevant time frame of emerging social networking technologies in the context of potential security threats.
- Participants expressed concerns about "mirror imaging" U.S. assumptions, meaning that the intentions of an adversary are too often evaluated using U.S. cultural biases rather than the opponents' culture, beliefs, and value systems. Western bias also tends toward the formal (and somewhat rigid) development of technology-based solutions versus organic or improvised solutions that allow for agility. To prevent surprise, symposium participants emphasized that assumptions must be examined through the lens of the appropriate operational context and culture, with a particular focus on innovative and ad hoc applications of technology. This point is further addressed in the section "Making S&TI Actionable for COCOMs" in Chapter 3.
- There was a general view that S&TI producers need to focus products and more directly target the needs of specific consumer communities. For example, products should be tailored to address issues specific to operational communities, whose needs differ from those of the community working long-term acquisition programs. As an example, a description of raw technical capabilities is not particularly useful to consumers outside the defense R&D community. S&TI information must be provided together with sufficient operational context to help consumers understand the potential impact if the capability is used against the United States on the battlefield.

- Several panel participants complained that it is difficult to direct questions to the right place within the S&TI community; similarly, when consumers of S&TI possess information that might be of value to producers of S&TI, they do not have clear mechanisms to get that information into the community.
- Information about potentially threatening technological developments is not, in general, shared with the S&TI community by corporate, academic, and U.S. government agencies outside the IC. Participants again identified the need for the S&TI community to develop a stronger understanding of S&T advances in the United States, as well as worldwide, and to build networks with these communities.

Use of Information in New Ways

In a world of collaborative systems, what is the proper balance between information sharing and information protection? How might adversaries use information to their advantage? Panel participants emphasized that it is imperative to consider these questions in the context of an open and global information world. Several points of discussion are listed below.

- Given new means of communication and information dissemination, individuals and groups are able to influence masses of people nearly instantaneously.
- The projection of power has become possible with the use of information as opposed to only the movement of troops. This change has obvious implications for governments as well as businesses. Previously, information campaigns always accompanied the "war plan"; now, the information campaign sometimes *is* the war plan. For example, during the incursion of Russia into Georgia in 2008, national security decisions were affected by implied threats even without a large-scale movement of troops.
- Systems integration has devolved to the level of an individual in some important areas. The major barrier to technology combination and utilization is no longer technical competence. Even without specific systems engineering experience, it is now possible to innovate and create novel capabilities via plug-and-play of available technologies as dictated by the situation at hand (leading to Type 4 surprises as characterized in the "Defining Technology Surprise" section above).
- Many participants identified concerns stemming from vulnerability in cyberspace—broadly defined. Information is increasingly available via open sources, as is demonstrated, for example, by the proliferation of biometric information. Similarly, software is increasingly obtained from open sources or developed commercially by teams distributed globally. At the same time, vulnerabilities are pervasive in battlefield infrastructures as well as in civil systems infrastructures. Participants noted that many

university researchers are not adequately protecting data beyond backups, leaving their research findings potentially accessible to adversaries. In addition, the anonymity of the cyber actor remains a significant issue.

- International Traffic in Arms Regulations (ITAR) was originally developed to keep technology within U.S. borders. ITAR-imposed constraints restrict the ability of some U.S. companies to export their technology overseas. As a result, companies have relocated both manufacturing and research facilities to overseas locations to avoid these restrictions, defeating the purpose of ITAR. The U.S. export control regime was viewed by symposium participants as symptomatic of U.S.-centric policy that is not aligned with today's world.[1]

Specific Areas of Concern for Technology Surprise

The immediate concerns of COCOMs center on the threat from weapons of mass destruction. Additional concerns stem from a lack of understanding of how adversaries might employ rapidly evolving and often commercially available technologies. When considering potential threats in the longer term, panel participants specifically mentioned the following areas:

- Information technology;
- Biotechnology, nanotechnology, and neuroscience;
- Cyber security;
- Material sciences;
- Directed energy; and
- Preserving current U.S. technology advantages, such as those in space, aviation, and maritime domains.

An imperative for the S&TI community is not only to share information and collaborate on technological advances but also to help protect U.S. dominance in critical areas. These goals must be reconciled within the reality of an increasingly global R&D enterprise.

SOURCES OF FUTURE TECHNOLOGY SURPRISE

Threats span a spectrum from individuals to small groups to nation-states. Rapid advancement of technologies and increasingly easy access to these technologies provides sophisticated capabilities to nation-states, non-state actors, and

[1]For additional information on ITAR and how it affects the exchange of unclassified, scientific information, please see the NRC report *Beyond Fortress America: National Security Controls on Science and Technology in a Globalized World*. Available from http://www.nap.edu/catalog.php?record_id=12567.

combinations thereof. Some symposium participants felt that a growing source of technology surprise, especially in the realm of cyber security, may stem from young, smart, and motivated but disenfranchised youth. Given the information revolution, this group could pose a significant threat, using peer-to-peer information sharing and social networking in ways not currently addressed or even fully understood by the S&TI community.

Parts of the private sector are now eclipsing nation-states in the accumulation of information about individuals, their actions, and their transactions. For example, the data accumulated by companies purposefully collecting large quantities of information might represent a significant threat if used maliciously or acquired by an adversary with intent to harm U.S. interests. There is a growing challenge relating to exploitation of personal information and identity theft. Exploitation of this type of data represents an opportunity for surprise not yet fully appreciated.

The challenge of technology warning is further complicated by differing approaches stemming from strategic versus tactical actors. While nation-states generally implement longer-term strategies that leverage technological advances, individual adversaries (and insurgents) tend to emphasize short-term tactical actions, often exploiting existing technologies in novel ways. The blurring of the boundary between technological advancement and innovative application of existing technologies further complicates this challenge. These points came out in the symposium during discussion of specific state actors of concern, including China (described in further detail in Box 2-1).

BOX 2-1
China

The symposium participants discussed China as an example of a potential source of technology surprise. It was agreed that the relationship between China and the United States is multifaceted and shaped by the U.S. view of China as a competitor and pursuer of U.S. technology, a collaborative partner, an economic rival, and a potential adversary. The relationship is further complicated by the fact that China is a major investor in the U.S. economy.

Participants expressed the view that asymmetry in the transparency between U.S. and other S&T enterprises is sometimes quite stark, depending on the domain (e.g., academic versus official), and cited past interactions with China in both academic and military-to-military settings to illustrate this point.

TIMING

Panel participants discussed the role of timing in anticipating surprise. The priorities for S&TI producers are impacted by COCOM timing requirements, the length of the acquisition cycle, and government research agendas.

Many participants agreed that surprise will increasingly occur sooner rather than later. Nevertheless, there was significant disagreement as to the time horizon to which most S&TI resources should be committed. The symposium discussions reflected disagreements between the commands and the S&TI community on this question. While the COCOMS are necessarily concerned with the near term, S&TI producers tend to be more focused on the long term (i.e., 10-15 years) due to the pull of the defense acquisition community.

Several topics of discussion related to the issue of timing are included below.

- Military commands tend to see S&TI within the narrow context of their explicit mission directives. They want to improve capabilities to do what they currently do, but better. However, they do not actively look over the horizon at potential technological developments that might defeat current capabilities. The focus of commands is on training to use currently available technologies, not on planning for future capabilities.
- S&TI producers present at the symposium felt that most S&TI resources are currently applied to relatively near term issues (the next 5 years). Because the procurement cycle for major new systems tends to be on the order of 20 years, the gap between these two time frames, and therefore the current value of S&TI to the acquisition community, is considerable.
  - — Demand for S&TI focused on the 0- to 5-year period is high because the acquisition community needs it to provide countermeasures that protect currently fielded capabilities. This demand, however, takes resources away from longer-term research. There was a general view that the 5- to 10-year time frame is very important, and that ignoring it leaves the United States very vulnerable to technology surprise.
  - — Longer-term forecasts are also important when considering initiation of major procurement efforts. There is a counterproductive lack of alignment between the rapidly changing environment and the lengthy and rigid military acquisition cycle. Technology is moving much faster than the acquisition cycle.
- COCOMs claimed that assessments far into the future (e.g., 20 years) seem to be of little value because of the uncertainty associated with the forecast, particularly in terms of the ability to anticipate operational impact. The counterpoint was voiced that while the technology procurement cycle may not lend itself to quick responses to changes in technology assessments, forecasts do inform the evolution of tactics and strategies

for using inventory when available and for innovating to develop novel solutions when not.

Technology Commoditization

How will adversaries make use of what is increasingly available to create new ways to surprise the United States? Wide availability of increasing computational capabilities will continue and will enable more surprises. Participants described this phenomenon in terms of "lego blocks": today the United States invests great resources in creating technology that very soon will be packaged into plug-and-play components for use by the general public, including future adversaries.

The Stages of Surprise

Panel participants questioned what the trigger is for the recognition of a surprise. For example, a bomb explosion immediately indicates that a surprise has occurred, while the realization that identity theft has occurred may come days, months, or years after the event itself. Panel participants identified four stages at which the potential for surprise might be recognized:

1. Technology is developed;
2. An adversary decides to commit a hostile act;
3. Technology is used by an adversary; and
4. Technology use is discovered by the target.

The time lag between the third and fourth events is what determines a viable response; participants observed an increase in this interval—particularly in the cyber domain. In addition, the stages suggest that both technology and policy evaluations are necessary components of an effective technology warning system.

CONCLUDING THOUGHTS

The first panel session of the symposium centered on defining and identifying areas of concern for technology surprise. Secondary discussions emphasized time lines for prioritization by COCOMs of information needs and the impact of development and acquisition cycles on adequately preparing to react to unexpected adversarial challenges.

3

Solutions Offered by Scientific and Technical Intelligence

This chapter summarizes discussion from the second panel session, which emphasized the composition and dissemination of S&TI products from the perspective of COCOMs and other consumers as well as S&TI producers. Additionally, potential solutions to better prevent technology surprise were discussed. Both panelists and the panel audience were active participants in the discussion, which was guided by a set of questions posed by the DIA/DWO. A list of these discussion prompts can be found in Appendix E.

TOPICS DISCUSSED

S&TI Resources

When asked whom S&TI consumers go to for information on technology developments that may lead to surprise, panel participants listed several of the "usual suspects" as their primary resources for S&TI information, including:

- The Defense Advanced Research Projects Agency (DARPA);
- The Defense Science Board;
- Think-tanks (e.g., RAND Corporation and the Brookings Institution);
- Department of Energy laboratories such as Lawrence Livermore, Los Alamos, and Sandia National Laboratories;
- DOD laboratories such as the Office of Naval Research;
- Federally funded research and development centers; and
- Private sector institutions via cooperative research and development agreements.

It was noted, however, that younger generations often seek information less from specific institutions than from knowledgeable individuals within those institutions, and that their searches are often buttressed by peer-to-peer cultural practices.

Making S&TI Actionable for COCOMs

When evaluating the relevance of S&TI, COCOM panel participants expressed the need for a clear assessment of time (when the threat might be realized), impact (an assessment of the consequences), mitigation actions (ways that the impact might be reduced), and a concept of operations describing how the technology might be used against the United States. Related discussion themes are described below.

- Sharing of information between S&TI and the warfighter community is important, but it must be in context to be of value. The commands expressed a preference for information sharing through some type of interactive dialogue rather than formal documents that may not sufficiently address the potential operational impact.
- Limited access to classified networks such as the JWICS (Joint Worldwide Intelligence Communication System) and the SIPRNet (Secret Internet Protocol Router Network) was discussed as a bottleneck restricting the distribution of S&TI products. Additional limiting factors for information sharing include over-classification within the government as well as the lock-down of intellectual property in private and academic entities. While these issues are challenges, they were highlighted in the discussion of S&TI solutions needed—ways to overcome these impediments in order to make S&TI more readily available to COCOMs.
- Participants acknowledged that sometimes the information needed to answer a query is not available, or is incomplete, when the question is asked. They suggested that information systems be expanded to retain the questions asked together with all subsequent S&TI exchanges to improve the continuity and consistency of S&TI products. Similarly, participants felt that adoption of the research community's trend toward publishing negative results as well as positive results might also be of value to consumers—as well as to other S&TI producers.
- The U.S. cultural inclination—particularly in the defense establishment—is to solve problems with technology-based systems. But, as mentioned in the section "Process-Specific Concerns About Technology Surprise" in Chapter 2, too often the U.S. assumption is that others behave similarly. Instead, the S&TI community must consider social systems and decision processes to account for varying adversary thought processes. This issue can be addressed by including cultural and social science factors as part of

the formal requirements generation process and by ensuring that technology assessments include the cultural and social science context.
- Some panelists expressed concern that open announcement of acquisition requirements in effect telegraphs strategic capabilities and potentially allows adversaries to develop countermeasures in concert with a U.S. research, development, testing, and evaluation cycle, with the result that advanced procurement offers a U.S. strategic advantage only for a limited time.

When prompted to characterize useful S&TI based on the categories of long-term forecasts, technology transfer risk assessments, or current military system capabilities, panel participants from COCOMs generally prioritized S&TI from warning of the most immediate threats (i.e., threats to current capabilities) to longer-term forecasts (e.g., forecasts of the potential for electronic warfare). Some past failures were discussed in reaction to this prioritization. Participants cited instances in which S&TI information was available, but appropriate action was not taken—either because the impact was not fully appreciated or because mitigation options were not apparent (or not feasible).

S&TI Production and Delivery

It was widely agreed that data and products should be available in a variety of forms. Capturing both the questions and the answers, and then revisiting those to generate updates, are critical to the evolution of S&TI capability. Tools for populating and maintaining information relationships in A-space (an analytical tool on JWICS) are of value, but access to A-space is currently too limited to address the needs of S&TI consumers.

Panel participants discussed the potential utility of the ability to infer correlations from R&D activities as well as benefits associated with the mapping and mining of both openly available and protected data (assuming that access can be obtained). Commercial examples of such inferences include companies' suggested spelling alternatives during Internet searches and automatic recommendations based on previous customer purchases.

Panel participants from COCOMs expressed a desire for on-demand, persistent, and real-time S&TI, and in fact some wanted to receive only information with those characteristics. This preference is inconsistent with the general consensus that S&TI should also monitor and warn of technology-based threats that may emerge over the longer term. This stimulated additional discussion regarding the need to tailor S&TI products for diverse consumer communities that have divergent needs, particularly in terms of the time frame of greatest importance.

Another point that surfaced during the discussion was that it is important to understand not only what a product does but also the methodology by which it is made. What was the development process? What size group with what composition was required? These and other related attributes suggest indicators that could

be tracked through collection to monitor emerging threats. Thus, these attributes are relevant to the requirements process.

Finally, there was significant discussion regarding how best to assess over time the quality and value of S&TI products from the perspective of the consumers of those products. Participants pointed out that feedback on S&TI quality could be gathered not only through face-to-face interaction between S&TI analysts and end users, but also through indirect means such as automatic tracking and analytics to quantify who is accessing specific information and how often. In general, participants felt that indirect means would be more productive because consumers are too busy to provide feedback on individual products.

STEPS TO PREVENT TECHNOLOGY SURPRISE

Many participants believed that adversaries evolve both capabilities and tactics inside the U.S. decision loop—that, particularly in current conflicts, they are more agile. Concerns were expressed that adversaries are making use of technology that is increasingly available to create new ways to surprise us.

"Red teaming," or considering an adversarial perspective in a simulated military conflict, is a useful way for operators to anticipate both current and future threats. The need to improve U.S. red teaming capability, particularly to improve the integration of adversarial culture and values, was discussed by several participants. S&TI has a role to play in this regard, but it also was acknowledged that there is a potential advantage in having S&TI analysts without access to classified information since they may be more collaborative and imaginative in their exploration of how technology might be used by adversaries to pose a threat to U.S. warfighters.

Box 3-1 describes an ONR-funded project discussed briefly in one of the panel sessions. With a small investment and using only publicly available databases, undergraduate researchers acting as a red cell were able to exploit vulnerabilities in current systems.

Other important solutions suggested by participants over the course of the panel discussions include the following.

- The IC should work with other U.S. government agencies to improve information flow, specifically regarding S&T advances.
- Information sharing within the IC should be better organized. There was an expressed belief that intelligence functions would benefit from integration. For example, regional and biographical analysts, working together, better understand each other's priorities and deliver more meaningful products; similarly, integration of regional and S&TI analysts could improve the value of S&TI products by providing greater operational context. Any technological capability described only as an abstraction will not appear relevant or urgent to consumers of S&TI.

BOX 3-1
Case Study: Unmanned Underwater Vehicle Exercise

Groups of college students were tasked to act as red cells. The sponsor prompted the groups with the hypothetical situation of a maritime threat. Teams created threat devices, identified targets, and deduced vulnerabilities to naval assets. Using open-source data (including Twitter and FaceBook), they were able to identify vessel schedules, locations of high-value targets, and sources of maritime components. Through this exercise, the teams identified holes in capabilities and previously unidentified vulnerabilities.

This project demonstrated a potential for surprise stemming from a small group with limited resources and only open-source information. It was pointed out that this exercise did not and would not trigger existing warning mechanisms.

Similar red team exercises have been proposed for the future, including ones targeted to cyber technology.

In general, participants felt that there is a need to better recognize where and how priorities are set for S&TI, particularly with regard to resource allocation. Relevant metrics discussed included available budget, number of assigned analysts, and the scientific reputation of the assigned leadership. A number of participants expressed the view that S&TI needs both more resources and stronger leadership and advocacy across the IC, particularly given the growing potential for technology surprise.

4

Discussions with Invited Speakers

The symposium featured three distinguished speakers with unique perspectives on the S&TI community:

- Dennis Blair, Director of National Intelligence;
- Jacques Gansler, Director of the Center for Public Policy and Private Enterprise at the University of Maryland and former Under Secretary of Defense (Acquisition, Technology, and Logistics (AT&L)); and
- Robert Hegstrom, Director of the Battlespace Awareness Portfolio, Office of the Under Secretary of Defense, Intelligence (OUSDI).

A summary of each speaker's remarks and the resultant discussions is provided below. Biographies for all three speakers can be found in Appendix F.

THE HONORABLE DENNIS BLAIR

During his address to the symposium audience on the importance of anticipating technological surprise, Director of National Intelligence (DNI) Dennis Blair emphasized that the responsibility of his office is not just to send out warnings of technology surprise, but also to employ technology in prosecution of the IC mission.

The United States does a reasonably good job of identifying both offensive and defensive ramifications of high-end technology threats, especially at the nation-state level. However, Admiral Blair stressed that surprise seems to come when benign, well-understood technologies are used in novel ways. An example of this is the use of commercial aircraft as weapons to take down buildings in

the attacks on September 11, 2001. It was referred to as a failure of imagination to not have anticipated this act. IEDs used in Iraq and Afghanistan are another example of a game-changing surprise despite the U.S. military having previously encountered booby traps during the Vietnam War. IEDs are not new technologies, but instead use existing technologies in a way that was not anticipated and is difficult to counter. Predicting this type of surprise requires more than technological expertise; it necessitates an understanding of how technology may be used in different contexts.

The proliferation of technology around the world presents new challenges for the IC in anticipating technology surprise. Potential adversaries have sophisticated tools available to them—capabilities that were once accessible only to well-resourced nation-states.

Particular Areas of Technology to Watch

The DNI discussed with the symposium participants three key areas to watch in anticipating surprise: cyber technology, biology, and the evolution of existing technologies.

Cyber technology was emphasized as an area of great focus at present. While the subject is well-warned about in that much has been published about cyber threats, the area retains high potential for surprise. Current governmental strategies may not fully consider the combination of technological expertise and imagination that exists elsewhere.

While the 19th century was transformed by chemistry and the 20th century by physics, the 21st century may be defined by advances in *biology*. This progress may bring both benefits and potential threats. Just as advances in precision in time and space (e.g., GPS technology) revolutionized warfare, so establishing identity through biometrics could similarly influence warfare and national security.

Finally, *evolving technologies* may change the operational assumptions upon which systems are built. For example, joint munitions effectiveness manuals' models for explosive devices had been based on old values for the strength of concrete. As concrete formulations have improved, attacks on hard targets have required specialized technologies to deliver the same effect. This change, caught by the DIA/DWO, demonstrates the importance of reexamining assumptions as seemingly mature technologies evolve over time.

Additional Discussion

During a question-and-answer (Q&A) session, several additional points were discussed, as described below.

A major point brought up for discussion was the observation that it cannot be assumed that adversaries will make decisions based on their own self-preservation.

Examples of this phenomenon include Kamikaze pilots of World War II and suicide bombers today. Accordingly, the value of integrating the social sciences into threat warning has become increasingly important. A recent case concerns the involvement of the social sciences to understand the psychology of radicalism.

To tap technical knowledge from academic institutions, there is no substitute for face-to-face visits. Directly connecting scientists and engineers with warfighters was suggested as a way to identify new solutions for on-the-ground problems.

The FY10 and FY11 budgets reduce funding for S&T, specifically within the IC. Although R&D budgets may grow in some areas, there is a shortfall in program budgets to continue development if a technology is successful. As Admiral Blair told the symposium audience, "The only substitute for having enough money for everything is agility." In keeping with this philosophy, it was expressed that there should be an effort to reduce single-purpose information/intelligence collection systems, which are less agile, and instead focus on multipurpose collection systems built to accommodate a changing array of intelligence requirements.

THE HONORABLE JACQUES GANSLER

The second address to the symposium was presented by Dr. Jacques Gansler, Director of the Center for Public Policy and Private Enterprise, University of Maryland, and former Under Secretary of Defense (AT&L). In his address to the symposium participants, Dr. Gansler emphasized that facing significant national security challenges—both in scope and in uncertainty—requires a holistic view of security, a broad spectrum of security missions, an ability to take advantage of globalization, and recognition of the long-term national security implications of non-military events (e.g., the global financial crisis, a worldwide pandemic, the aging U.S. population). Addressing these challenges requires addressing four highly interrelated acquisition issues:

- What goods and services to buy (the requirements process),
- How to buy them (acquisition reform),
- Who does the acquiring (the acquisition workforce), and
- From whom it is acquired (the industrial base).

The following list is a summary of what Dr. Gansler identified as the top five priorities in overcoming the challenges he discussed.

1. **Acquisition workforce.** The service chiefs and various national security secretaries and directors must recognize and promote senior acquisition personnel (military and civilian) in order to demonstrate their personal recognition of how critical smart acquisition personnel and practices are to U.S. military posture in the 21st century.

2. **Weapons costs as a military requirement.** This will require early and enhanced systems engineering (throughout both government and industry) and incentives to industry for achieving lower-cost systems.
3. **The value of "rapid acquisition"** for both military and economic benefits. This will require the full use of what was referred to as *spiral development*. Each development block is based on proven technology; continuous user and logistician feedback yields subsequent "block" improvements.
4. **Balancing of resources.** There is currently a strategy/resource mismatch that requires realignment.
5. **Taking full advantage of the potential benefits of globalization,** while not ignoring the potential vulnerabilities and risks.

Key take-aways and points from the symposium discussion of these core issues are summarized in Table 4-1.

Additional Discussion

During a Q&A session, the following points were among those discussed. First, in a discussion on Title 10 regarding who is responsible for the equipping and maintaining of armed forces, it was agreed that both service chiefs and COCOMs must work better together.

Another point concerned the need for better systems engineering and engineers able to address the underlying science that may impact complex systems integration. In particular, the independence of systems engineering, integration issues, and independent cost estimation should be high-priority considerations for decision makers.

As is addressed in the panel discussions summarized in Chapters 2 and 3, acquisition reform alone is not enough. Human dimensions such as social and cultural aspects must also be integrated into how technologies are used. Another suggestion brought up during the panel discussions, red teaming, was recommended by participants to be part of the acquisition process.

MR. ROBERT HEGSTROM

Mr. Robert Hegstrom, Director of the Battlespace Awareness Portfolio in the OUSDI, began his talk by describing current efforts in the Battlespace Awareness Portfolio. Preventing technology surprise was described as a core priority of his office, in addition to work with the Military Intelligence Program and the National Intelligence Program.

Threat concerns highlighted over the course of the discussion included longer-range ballistic missiles, the recent Chinese anti-satellite test, and IEDs. Currently, there is also a need to focus on new-technology-based threats, especially those disruptive in nature.

TABLE 4-1 Key Considerations for Core Acquisition Issues

What goods and services to buy? (requirements process)	In a resource-constrained environment, the priorities must be addressed: • Lower-cost systems and services; • Optimized, network-centric systems-of-systems (vs. individual "platforms"); • A "reserve" of resources to rapidly respond to urgent COCOM needs (vs. the current 15- to 20-year acquisition cycle); • A balanced allocation of resources to address irregular operations; • Interoperability of "Joint" and coalition systems; and • Planning and exercising "as we will fight" with allies, multiple agencies, and contractors on the battlefield.
How to buy them? (acquisition reform)	To achieve higher performance faster and at lower costs: • Require cost as a design/military requirement. • Provide viable, continuous competition options (e.g., competitive prototypes) to incentivize higher performance at lower costs. • Maximize use of commercial products and services at all levels. • Implement modern, enterprise-wide IT systems (logistics, business, personnel, etc.). • Institutionalize a rapid-acquisition parallel process to respond to COCOM urgent needs. • Create incentives for contractors to achieve desired results (in cost, schedule, and performance). • Minimize conflict of interest concerns. • Fully utilize *spiral development*: get basic capabilities out and improve them incrementally.
Who does the acquiring? (acquisition workforce)	The acquisition workforce lacks expertise in key areas. A large workforce turnover in the coming years will provide continued challenges and opportunities. Both quantity and quality of senior and experienced military and civilian personnel are required (especially for expeditionary operations). In the last decade-plus, this "requirement" has not been met.
From whom is it acquired? (industrial base)	A 21st-century national security industrial base should: • Be efficient, responsive, technologically advanced, and highly competitive (at all levels, including public and private sectors); • Be globalized, utilizing "best in class" (requires significant changes to U.S. export controls); • Invest in intelligence R&D and capital equipment; • Include commercial, industry and maximize dual-use facilities and workforce; and • Contain an independent systems-of-systems architecture and systems engineering firms. Merger and acquisition reviews should be based on this vision. Despite congressional resistance, all work that is not inherently governmental work should be sourced competitively (public vs. private). Government-industry communications should be encouraged once again. Finally, structural changes are required to eliminate the appearance, or reality, of conflicts of interest (regarding "vertical integration").

SOURCE: Compiled from information provided by Jacques Gansler.

To better understand threats perceived by COCOMs, Mr. Hegstrom took part in a Joint Requirements Oversight Committee session with representation by all COCOMs to identify the integrated priority lists for each. Identified areas of concern included:

- Intelligence, surveillance, and reconnaissance (ISR);
- Battlespace awareness;
- Gaps in analysis capabilities (one COCOM specifically identified that excessive collected data, without adequate resources to analyze it, was a "giant anchor");
- Restrictions on information sharing with allies;
- Human intelligence;
- Full-motion video;
- Targeting and tracking capabilities; and
- Persistent surveillance.

Mr. Hegstrom next discussed the upcoming Quadrennial Defense Review, which seeks to update long-term strategies (and budget recommendations) for the current fight and future challenges. Teams are being formed to address the following subjects:

- Irregular warfare,
- Civil support,
- High-end adversaries (for near-peer threats),
- Enablers (for processing and dissemination),
- Global posturing, and
- Business processes.

In addition to these teams, an additional "Analysis and Integration" team will synthesize results from the other teams for the FY10-FY15 budget, soon to be submitted to legislators. Related budget issues were a key concern in the final segment of the formal discussion. After the new administration entered in 2009, there has been reprioritization, and resources have been added to ISR.

Additional Discussion

During a Q&A session, the following points were among those discussed. First, in a discussion regarding the amount of time the OUSDI spent investigating foreign threats to defeat current U.S. capabilities, it was mentioned that space threats are one current focus, and that the United States is no longer assured of dominance in this area. This became evident after the Chinese anti-satellite test, which had been forewarned by some analysts but was not considered a real possibility until after the fact. Counter-threat intelligence analysis was emphasized.

Regarding the attention paid to open publication of foreign intentions in native-language publications, it was noted that OUSDI uses such publications as indicators for focusing further intelligence collection needs.

A long discussion was held on the issue of what causes surprise. Points raised included the following as contributing factors:

- **Lack of belief in outside experts.** There is a lack of coupling between the IC and outside experts.
- **Conservative analyses.** IC tradecraft and editing standards limit analysts' ability to effectively warn of potential surprises that are feasible but for which only limited intelligence data is available. This point was emphasized throughout the discussions.
- **Lack of specific, unequivocal indications and warning data.** Lack of specificity limits the ability to be conclusive, and low presumed likelihood leads to low dedication of resources.

At the end of the session, discussion ensued regarding trust issues in S&TI. Key points included the fact that data interpretation is subject to cultural biases as well as U.S. "mirror-imaging" regarding normal system or technology development timelines.

5

Underlying Themes

At the close of the symposium, the symposium committee asked the DIA/DWO representative to share what he had identified as key take-away messages from the day's discussions. These themes are summarized below. Although not intended to be comprehensive, the list highlights many of the concerns emphasized throughout the symposium.

- **Agility is essential.** Agility is difficult in a rigid structure like the DOD, but is necessary for adequate and appropriate responses to inevitable yet unexpected threats presented by adversaries.
- **Technology surprise should be defined in a standard way.** The lack of a common definition across the community of S&TI providers and users showed the DIA/DWO that neither providers nor users are adequately informed about what to look for or the risks inherent in not preparing for such surprise. Though it is not possible to anticipate all potential surprises, efforts to stay as prepared as possible are imperative.
- **The nation is not prepared to meet future science and engineering needs.** The decline in American students being trained as scientists and engineers has been noted, and the potential threat to technology surprise preparedness is profound.
- **The S&TI community lacks a central point of contact.** It is important that parties know whom to alert when either an exciting or a worrisome development has been noted.
- **Communication gaps exist within the S&TI community, between S&TI producers and consumers, and between the United States and its allies.**

Gaps in communication channels were evident when the DIA/DWO asked how symposium participants connect with people outside the community.

- **S&TI must better demonstrate the feasibility, impact, and intent of threats.** Whether a threat is possible is a consideration separate from whether or not an adversary has the motivation and intent to carry out the anticipated threat. For users of S&TI to adequately prioritize potential mid- to long-term threats, the context-specific relevance of threat must be clearly communicated.

Appendixes

Appendix A

Workshop Agenda and Panelists

AGENDA

Avoiding Technology Surprise for Tomorrow's Warfighter Symposium

The National Academy of Sciences Building
2101 Constitution Avenue NW
Washington, DC 20418

Wednesday, April 29, 2009

0800–0845	**Registration**	*Great Hall*
0845–0945	**Introduction and Setting the Scene** Dr. Ruth David, *Chair* Committee for the Symposium on Avoiding Technology Surprise for Tomorrow's Warfighter Mr. Robert Hegstrom Director, Battlespace Awareness Portfolio Office of the Under Secretary of Defense, Intelligence	*Auditorium*
1015–1030	**Introduction of Keynote Speaker** Dr. Ruth David, *Chair*	*Auditorium*

1030–1130	**Keynote Address** The Honorable Dennis C. Blair, Director of National Intelligence	*Auditorium*
1130–1230	**Panel Discussions (in Parallel)** Moderated by Members of the Committee for the Symposium on Avoiding Technology Surprise for Tomorrow's Warfighter	*Auditorium/Lecture Room*
1330–1515	**Continued Panel Discussions (in Parallel)**	*Auditorium/Lecture Room*
1545–1715	**Summaries of Panel Findings** Panel Moderators	*Auditorium*
	Committee Fact Finding and Further Discussion Dr. Ruth David, *Chair*	*Auditorium*
1800–2000	**Dinner** Dinner Speech by the Honorable Jacques S. Gansler, Director of the Center for Public Policy and Private Enterprise, University of Maryland	*Great Hall*

PANELISTS

Core panel membership was as follows.

Panel 1 (Ann Campbell and John Gannon, moderators)
- Richard Shook (USJFCOM)
- Brendan Godfrey (AFOSR)
- Patrick Jackson (USJFCOM)
- Wesley Jennings (USCENTCOM)

Panel 2 (Sharon Glotzer and James Smith, moderators)
- Rebecca Ahne (U.S. Navy)
- Thomas Carroll (USSOCOM)
- John Marshall (USJFCOM)

Appendix B

Biographical Sketches of Committee Members

Ruth A. David, NAE, *Chair,* is president and chief executive officer of Analytic Services, Inc., a nonprofit research institute focusing on national security, homeland security, and public safety issues. She initiated a corporate focus on homeland security in 1999 and established the ANSER Institute for Homeland Security early in 2001; today the corporation operates the Homeland Security Institute, a federally funded research and development center sponsored by the Department of Homeland Security, in addition to the ANSER business unit. Before assuming her current position in 1998, Dr. David was deputy director for science and technology at the Central Intelligence Agency (CIA). As technical advisor to the director of central intelligence, she was responsible for research, development, and deployment of technologies in support of all phases of the intelligence process. Dr. David is a member of the National Academy of Engineering (NAE) and currently serves on the NAE Council as well as several committees of the National Research Council (NRC); she chairs the NRC Standing Committee on Technology Insight—Gauge, Evaluate, and Review (TIGER). She is a member of the Homeland Security Advisory Council, first established to advise the president and now advising the secretary of the Department of Homeland Security. She also serves on the National Security Agency Advisory Board, the Hertz Foundation Board, and the Wichita State University Foundation National Advisory Committee and is a member of the Draper Corporation. Previously, Dr. David served in several leadership positions at the Sandia National Laboratories, where she began her professional career in 1975. Dr. David received a bachelor of science degree in electrical engineering from Wichita State University, and a master of science degree and a doctorate in electrical engineering from Stanford University.

Steven R.J. Brueck is the director of the Center for High Technology Materials (CHTM) and is a distinguished professor of electrical and computer engineering, physics, and astronomy at the University of New Mexico. As CHTM director, he manages research and education at the boundaries of two disciplines. The first, optoelectronics, unites optics and electronics and is found in CHTM's emphasis on semiconductor laser sources, optical modulators, detectors, and optical fibers. The second, microelectronics, applies semiconductor technology to the fabrication of electronic and optoelectronic devices for information and control applications. Examples of these unifying themes at work are Si-based optoelectronics and optoelectronics for Si manufacturing sensors. He is also a former research staff member of MIT Lincoln Laboratory. He is a member of the American Physical Society and the Materials Research Society and is a fellow of the Institute of Electrical and Electronics Engineers, the Optical Society of America, and the American Association for the Advancement of Science.

Ann N. Campbell is currently acting director for Sandia National Laboratories' Cyber Strategic Thrust. In this role, she provides leadership and coordination for the laboratory strategy and engagement in the national cyber challenge. Dr. Campbell received a B.S. degree in materials engineering from Rensselaer Polytechnic Institute and M.S. and Ph.D. degrees in applied physics (materials science concentration) from Harvard University. At Sandia, Dr. Campbell has served as senior manager for the Assessment Technologies Group in the Information Systems Analysis Center, where her responsibilities included leadership for a broad range of technical activities focused on vulnerability assessments and the development of national security solutions in information technology for multiple government sponsors. Most recently, she was the deputy for technical programs for Sandia's Defense Systems and Assessment Strategic Management Unit. Dr. Campbell is a senior member of the IEEE and is affiliated with the IEEE Reliability and Electron Devices Societies. She was a member of the IEEE Reliability Society Administration Committee from 1999 to 2004 and served as vice president of membership for the society. Dr. Campbell has served on the Management Committee and Board of Directors for the IEEE International Reliability Symposium.

Stephen W. Drew, NAE, holds consultancies with a variety of pharmaceutical and biotechnology organizations and is a founder and principal of Science Partners LLC. Until 2000, he worked with Merck & Company, Inc., in a series of increasingly responsible positions culminating with distinguished senior scientist. He was vice president of Vaccine Science and Technology, vice president of Vaccine Operations, and vice president of Technical Operations and Engineering. Prior to joining the Merck Manufacturing Division in 1987, he was the senior director of Biochemical Engineering in the Merck Research Laboratories (MRL), a department that he started in 1981. Dr. Drew received his Ph.D. in biochemical engineering from the Massachusetts Institute of Technology. Dr. Drew is member of

the National Academy of Engineering (NAE). He has served in several capacities within the NAE and assisted numerous National Research Council committees. He was chair of the advisory committee to the Engineering Directorate of the National Science Foundation.

John Gannon is vice president for Global Analysis, a business area within BAE Systems. Dr. Gannon joined BAE Systems after serving as staff director of the House Homeland Security Committee, the first new committee established by Congress in more than 30 years. In 2002-2003, he was a team leader in the White House's Transitional Planning Office for the Department of Homeland Security. He served previously in the senior-most analytic positions in the intelligence community, including as the CIA's director of European analysis, deputy director for intelligence, chairman of the National Intelligence Council, and assistant director of Central Intelligence for Analysis and Production. In the private sector, he developed the analytic workforce for Intellibridge Corporation, a Web-based provider of outsourced analysis for government and corporate clients. Dr. Gannon served as a naval officer in Southeast Asia and later in several naval reserve commands, retiring as a captain. He holds a bachelor's degree from Holy Cross College in Worcester, Massachusetts, and master's and doctoral degrees from Washington University in St. Louis, Missouri. He is an adjunct professor in the National Security Studies Program at Georgetown University.

Sharon C. Glotzer received her B.S. in physics from UCLA in 1987 and her Ph.D. in physics from Boston University in 1993. Under an NRC Postdoctoral Fellowship and then as a member of the technical staff, she worked at NIST as a physicist in the Polymers Division of the Materials Science and Engineering Laboratory, and co-founded and directed the Center for Theoretical and Computational Materials Science. She moved to the University of Michigan in 2001 as an associate professor with tenure and is now a professor of chemical engineering and materials science and engineering, with a courtesy appointment in physics. She also holds the titles of professor of applied physics (and serves on the executive committee) and professor of macromolecular science and engineering, and is a faculty affiliate in the University of Michigan's Center for Theoretical Physics, Center for the Study of Complex Systems, Center for Computational Medicine and Biology, the University of Michigan branch of the Institute for Complex Adaptive Matter (for which she serves on the steering committee) and the Michigan Nanotechnology Institute for Medicine and Biological Sciences (for which she serves on the executive board). Her research focuses on computational nanoscience and computer simulation of soft matter, self-assembly, and materials design and is sponsored by NSF, DOE, NASA, AFOSR, and the McDonnell Foundation. She has published more than 130 papers in such journals as *Science*, *Nature*, *Nature Physics*, *Nature Materials*, *Physical Review Letters*, *Nano Letters* and the *Proceedings of the National Academy of Sciences*, and she has presented

more than 180 invited and keynote presentations around the world, including six named lectures at universities in the United States and Canada. She has received numerous awards and honors, including the American Physical Society's Maria Goeppert-Mayer Award, Presidential Early Career Award for Scientists and Engineers (PECASE) and the Department of Commerce Bronze Medal, and she was a Sigma Xi Lecturer. Her efforts in research, teaching, and service have been recognized at the University of Michigan by the Rackham Faculty Recognition Award, College of Engineering's Monroe-Brown Foundation Research Excellence Award, and Department of Chemical Engineering's Departmental Excellence Award. She is the 2008 recipient of the Charles M.A. Stine Award from the American Institute of Chemical Engineering and is a Fellow of the American Physical Society, and is a Department of Defense National Security Science and Engineering Faculty Fellow.

Christopher C. Green is the assistant dean for Asia Pacific of the Wayne State University School of Medicine (SOM) in Beijing, China. He is also a clinical fellow in neuroimaging/MRI in the Department of Diagnostic Radiology and the Department of Psychiatry and Behavioral Neurosciences of the SOM and the Detroit Medical Center (DMC). His medical specialties are brain imaging, forensic medicine and toxicology, and neurophysiology, and his personal medical practice is in the differential diagnoses of neurodegenerative disease. He has served and continues to serve on many government advisory groups and private sector corporate boards of directors. Immediately prior to his current position, he was executive director for emergent technology research for the SOM/DMC. From 1985 through 2004 he was executive director, Global Technology Policy, and chief technology officer for General Motors' Asia-Pacific Operations. His career at General Motors included positions as head, Biomedical Sciences Research, and executive director, General Motors Research Laboratory for Materials and Environmental Sciences. His distinguished career with the CIA extended from 1969 to 1985 as a senior division analyst and assistant national intelligence officer for science and technology. His Ph.D. is from the University of Colorado Medical School in neurophysiology, and his M.D. is from the Autonomous City University in El Paso, Texas/Monterey, Mexico, with honors. He also holds the National Intelligence Medal and is a fellow in the American Academy of Forensic Sciences.

Leslie Greengard, **NAS/NAE,** is the director of the Courant Institute of Mathematical Sciences at New York University, where he is a professor of mathematics and computer science. Dr. Greengard received his B.A. in mathematics from Wesleyan University in 1979, followed by an M.D. and a Ph.D. in computer science from Yale University in 1987. He joined the faculty of the Mathematics Department at the Courant Institute in 1989. Dr. Greengard's research is largely concerned with the development of fast and adaptive algorithms for computational

problems in biology, chemistry, materials science, medicine, and physics. One such algorithm is the fast multipole method (FMM), developed during the 1980s with V. Rokhlin, which is now widely used in electromagnetics, astrophysics, molecular simulations, and fluid dynamics. He currently works on protein design, the analysis of "metamaterials," diffusion in complex geometry, and reconstruction methods for magnetic resonance imaging. Dr. Greengard has been an NSF Presidential Young Investigator and a Packard Foundation Fellow. He received the Leroy P. Steele Prize from the American Mathematical Society in 2001 and the Sokol Faculty Award in the Sciences from New York University in 2004. In 2006, he was elected to both the National Academy of Sciences and the National Academy of Engineering.

Diane E. Griffin, IOM/NAS, is professor and chair of the Department of Molecular Microbiology and Immunology and director of the Johns Hopkins Malaria Research Institute at Johns Hopkins Bloomberg School of Public Health. She earned a biology degree from Augustana College in 1962, followed by M.D. (1968) and Ph.D. (1970) degrees from Stanford University. She interned at Stanford University Hospital between 1968 and 1970, before beginning her career at Johns Hopkins as a postdoctoral fellow in virology and infectious disease in 1970. After completing her postdoctoral work, she was named an assistant professor of medicine and neurology. Since then, she has held the positions of associate professor, professor, and now professor and chair. She served as an investigator in the Howard Hughes Medical Institute from 1973 to 1979. Dr. Griffin's research interests include alphaviruses and acute encephalitis. She is also working on the effect of measles virus infection, and immune activation in response to infection, on immune responses in tissue culture and in infected humans at the University Teaching Hospital in Lusaka, Zambia. In Zambia, she and her colleagues are examining the effect of HIV infection on measles and measles virus immunization. Dr. Griffin is the principal investigator on a variety of grants from the National Institutes of Health, the Bill & Melinda Gates Foundation, and the Dana Foundation. She is a member of the National Academy of Sciences and the Institute of Medicine, the author or co-author of a more than 300 scholarly papers and articles, and the past president of the American Society for Virology, the Association of Medical School Microbiology Chairs, and the American Society for Microbiology.

J.C. Herz is a technologist with a background in biological systems and computer game design. She is the founder of Batchtags, Inc. Her specialty is massively multiplayer systems that leverage social network effects, whether on the Web, mobile devices, or more exotic high-end or grubby low-end hardware. She currently serves as a White House special consultant to the Office of the Secretary of Defense (Networks and Information Integration). Defense projects range from aerospace systems to a computer-game-derived interface for next-generation

unmanned air systems. She is one of the three co-authors of OSD's Open Technology Development roadmap. Ms. Herz serves on the Federal Advisory Committee for the National Science Foundation's education directorate. In that capacity, she is helping NSF harness emerging technologies to drive U.S. competitiveness in math and science. She was a member of the NRC Committee on IT and Creative Practice and is currently a fellow of Columbia University's American Assembly, where she is on the leadership team of the Assembly's Next Generation Project. In 2002, she was designated a Global Leader for Tomorrow by the World Economic Forum. She is a member of the Global Business Network, a founding member of the IEEE Task Force on Game Technologies, a term member of the Council on Foreign Relations, and a member of the advisory board of Carnegie Mellon's ETC Press. She graduated from Harvard with a B.A. in biology and environmental studies, magna cum laude, in 1993. She is the author of two books, *Surfing on the Internet* (Little Brown, 1994) and *Joystick Nation: How Videogames Ate Our Quarters, Won Our Hearts, and Rewired Our Minds* (Little Brown, 1997), a history of videogames that traces the cultural and technological evolution of the first medium that was born digital, and how it shaped the minds of a generation weaned on Nintendo. Her books have been translated into seven languages. As a *New York Times* columnist, she published 100 essays on the grammar and syntax of game design between 1998 and 2000. She has also contributed to Esther Dyson's *Release 1.0* and to *Rolling Stone*, *Wired*, *GQ*, and the *Calgary Philatelist*.

J. Jerome Holton is a senior systems engineer with the Tauri Group working in support of the BioWatch Systems Program Office of the Department of Homeland Security. Previously he served as senior vice president and chief technology officer for ARES Systems Group, LLC, where he focused on the fielding of information operations tools, enhancing intelligence, surveillance and reconnaissance capabilities to detect and defeat improvised explosive devices, and the development of applique armor solutions to counter explosively formed penetrators. Dr. Holton was previously an associate with Booz Allen Hamilton, where he led the technical support team for the Explosives Division within the Department of Homeland Security's Science and Technology Directorate. Prior to that, he served as the director of technical research, analyses, and communications for Defense Group, Inc., where he was responsible for the company's branding, strategic planning, and positioning in the government support sector, including policy, technology, and operations issues for weapons of mass destruction and their effects on civilian infrastructure, first responders, military forces, and tactical operations. He has been involved in defense and energy programs related to the counterproliferation of, counterterrorism/domestic preparedness for, and the detection, identification, and decontamination of chemical and biological weapons. He has provided advice and counsel to senior decision makers in the Office of the Deputy Assistant to the Secretary of Defense for Counterproliferation and Chemical/Biological Defense, the Chemical Biological Defense Directorate of the Defense Threat Reduction

Agency, and the Chemical Biological National Security Program of the Department of Homeland Security. Dr. Holton has previously served as a member of the NRC Committee on Defense Intelligence Agency Technology Forecasts and Reviews and the Committee on Alternative Technologies to Replace Antipersonnel Landmines. He earned his M.S. and Ph.D. degrees in experimental physics from Duke University.

Frederick R. Lopez had a 36-year career as an engineer with McDonnell-Douglas Aircraft Company and Raytheon Company. He is also a retired brigadier general, U.S. Marine Corps Reserve. Recently retired, he was the director of engineering for Raytheon Electronic Warfare Systems in Goleta, California. General Lopez was responsible for the management of all engineering personnel in support of operational and support programs in electronic warfare systems and for the implementation of engineering processes and process improvement activities within the engineering discipline. Highlights in his Marine Corps career include a tour of duty in Vietnam, service as an Infantry Officer with Master Parachutist Qualification, and a secondary Military Occupational Specialty of Forward Air Controller (FAC). He has held billets as company XO, company commander, battalion XO, battalion CO, FAC, and naval gunfire team leader, brigade platoon leader, ANGLICO operations officer, regimental operations officer, assistant division commander, commanding general, 4th Marine Division. He served 3 years on active duty and 28 years in the U.S. Marine Corps Reserve. General Lopez received a B.S. degree in mathematics from California State Polytechnic College and an M.S. in computer science from West Coast University, Orange, California.

Gilman G. Louie is a partner of Alsop Louie Partners, a venture capital fund focusing on the development of great technology entrepreneurs. Prior to this position he was president and CEO of In-Q-Tel, a venture capital group helping to deliver new technologies to the CIA and intelligence community. Before helping found In-Q-Tel, Louie served as Hasbro Interactive's chief creative officer and as general manager of the Games.com Group, where he was responsible for creating and implementing the business plan for Hasbro's Internet games site. Prior to joining Hasbro, he served as chief executive of the Nexa Corporation, Sphere, Inc., Spectrum HoloByte, Inc., and Microprose, Inc. As a pioneer in the interactive entertainment industry, Gilman's successes have included the Falcon, F-16 flight simulator, and Tetris, which he brought over from the Soviet Union. Louie has served on the board of directors of Wizards of the Coast, Total Entertainment Network, Direct Language, and FASA Interactive. He was an active member of the Markle Foundation Task Force on National Security and the Information Age.

Julie J.C.H. Ryan is president of Wyndrose Technical Group and an associate professor of engineering management and systems engineering at George

Washington University. She holds a B.S. degree in humanities from the U.S. Air Force Academy, an M.L.S. in technology from Eastern Michigan University, and a D.Sc. in engineering management from the George Washington University. Dr. Ryan began her career as an intelligence officer, serving the U.S. Air Force and the U.S. Defense Intelligence Agency, working in a series of increasingly responsible positions throughout her distinguished career. Her areas of interest are in information security and information warfare research, and she has conducted several research projects and written articles and book chapters in her focus area. She was a member of the National Research Council's Naval Studies Board from 1995 to 1998. Dr. Ryan is the treasurer and a member of the Board of Directors for the Colloquium on Information Systems Security Education.

James B. Smith is the international business development executive for Raytheon Integrated Defense Systems in Tewksbury, Massachusetts. Prior to this appointment, Brig Gen Smith served as vice president of government business for Raytheon Aircraft Company. Previously, he was vice president of the Precision Engagement Strategic Business Area for Raytheon in Tucson, Arizona. Before joining Raytheon, he served as the director of Navy Command and Control Systems for Lockheed Martin. Smith had a distinguished military career, retiring from the U.S. Air Force as a brigadier general in October 2002. As the deputy commander and commander of the Joint Warfighting Center, U.S. Joint Forces Command, Joint Training Analysis and Simulation Center, he was responsible for managing the joint force exercise and training development program. His aviation career includes 4,000 hours in the F-15 and T-38, including combat sorties during Desert Storm. Among his responsibilities during his military career was the command of the 94th Tactical Fighter Squadron and the 325th Operations Group. Later he served as commander of the 18th Wing at Kadena Air Base, Japan. His staff postings included a variety of joint and coalition assignments including the deputy for operations, North American Air Defense Command (NORAD), and professor of national security strategy at the National War College. Brig Gen Smith is a distinguished graduate of the U.S. Air Force Academy (B.S., military history) and Indiana University (M.A., history). He is also a distinguished graduate of Air Command and Staff College, the Naval War College, and the National War College.

Dianne S. Wiley, a Boeing technical fellow for structures and materials technology, is the innovation advocate for technology insertion into space exploration systems. She is the liaison between the Space Exploration Systems office and the Boeing Technical Fellowship. She recently left the Missile Defense National Team, where she was responsible for international coordination of Defense of Deployed Forces, Friends, and Allies. In addition to managing proposal strategy and execution for the enterprise, she also serves as the enterprise liaison to the Boeing Technical Fellowship to facilitate technology maturation and technology

transition to the space exploration systems business area. Previously, Dr. Wiley was assigned to the Missile Defense National Team, responsible for international missile defense activities for defense of friends and allies and defense of U.S. deployed forces. In her prior assignment with Boeing Phantom Works, she was the program manager for airframe technology on the NASA Space Launch Initiative Program, overseeing the development and demonstration of advanced structure and materials technology for next-generation reusable launch vehicles. Previously, she was with Northrop Grumman for 20 years, where she was manager of Airframe Technology. In that position, Dr. Wiley was responsible for research and development and technology transition in structural design and analysis, materials and processes, and manufacturing technology. During that time, she was responsible for transitioning airframe core technologies into three new business areas (space, biomedicine, and surface ships) to offset declines in traditional business. Before that, she served as a senior technical specialist on the B-2 program. Dr. Wiley was responsible for developing and implementing innovative structural solutions to ensure the structural integrity of the B-2 aircraft. Dr. Wiley's 25 years of technical experience have involved durability and damage tolerance, advanced composites (organic and ceramic), high-temperature structures, smart structures, low-observable structures, concurrent engineering, and rapid prototyping. Dr. Wiley holds a Ph.D. in applied mechanics from UCLA School of Engineering and Applied Science. She attended Defense Systems Management College (1996). She is a graduate of the Center for Creative Leadership (1995), Leadership California Class of 1998, and the Boeing Leadership Center (2002).

Appendix C

Participating Organizations

Air Force Office of Scientific Research
Air Force Research Laboratory, Wright-Patterson Air Force Base
Booz Allen Hamilton
Center for Public Policy and Private Enterprise, University of Maryland
Concurrent Technologies Corporation
Defense Advanced Research Projects Agency (DARPA)
Department of Homeland Security
Defense Intelligence Agency
Director, Operational Test and Evaluation
Georgia Tech Research Institute
Institute for Defense Analyses
Institute for the Future
Institute on Science for Global Policy, University of Arizona
Intelligence Advanced Research Projects Agency (IARPA)
Joint Transformation Command for Intelligence
Lockheed Martin Corporation
Missile Defense Agency
National Air and Space Intelligence Center
National Center for Medical Technology, U.S. Army
National Ground Intelligence Center
National Intelligence Council
National Nuclear Security Administration–Kansas City Plant
Naval Air Systems Command
Naval Surface Warfare Center
Office of Naval Intelligence

Office of the Deputy Undersecretary of Defense
Office of the Director of National Intelligence
Office of the Joint Chiefs of Staff
Office of the Secretary of Defense, Director, Defense Research and Engineering
Office of the Secretary of Defense, Networks and Information Integration
Office of the Undersecretary of Defense, Intelligence
RAND Corporation
Sandia National Laboratories
Smartronix
Stevens Institute of Technology
United States Central Command
United States Joint Forces Command
United States Naval Academy
United States Special Operations Command
United States Transportation Command
Weapons, Intelligence, Nonproliferation, and Arms Control Center, Central Intelligence Agency

Appendix D

Opening Session Charts

Prior to the symposium, the DIA/DWO distributed questionnaires to selected governmental participants to elicit their perspectives regarding key topics to be discussed during the symposium. Responses were received from the major stakeholder communities—including COCOMs, defense acquisition, defense R&D, and S&TI producers. The results were tabulated and shown graphically during the opening session to help set the scene for the subsequent panel discussions. While the sample was small and the results not statistically significant, the distribution of responses served to focus and stimulate panel discussions. Figures D-1 through D-8 in the section "Setting the Scene" in Chapter 1 were shared with symposium participants.

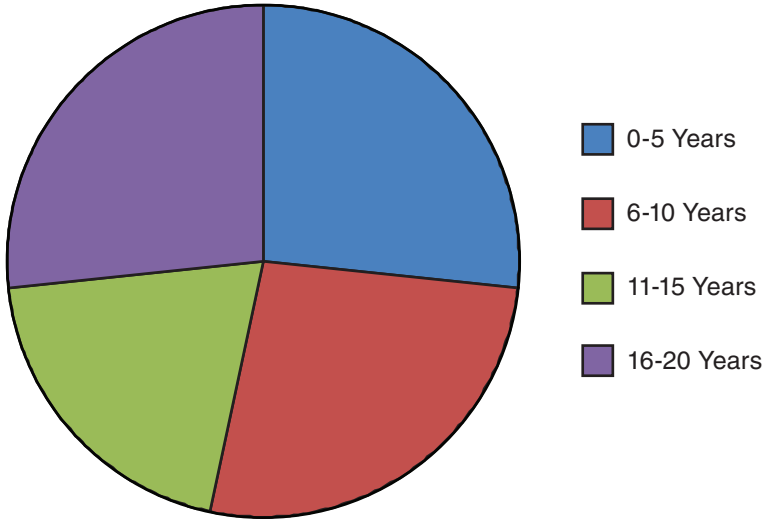

FIGURE D-1 Results in response to the question, What time horizon is your command or work unit focused on? SOURCE: Survey by DIA/DWO.

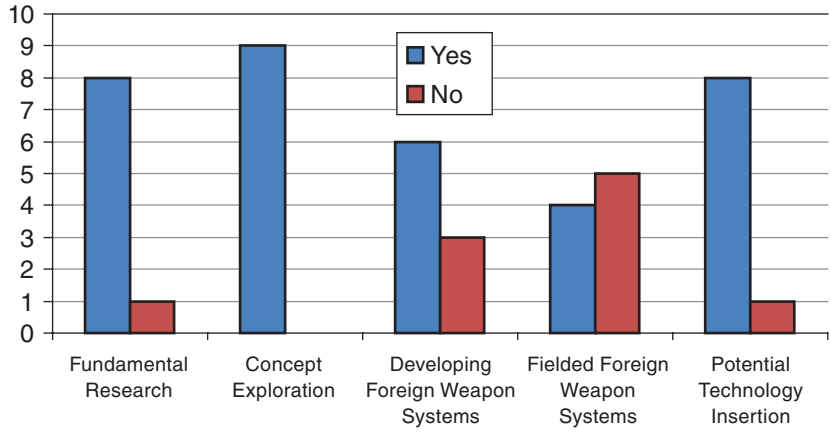

FIGURE D-2 Results in response to the question, Would you be interested in S&TI products regarding [the listed types]? SOURCE: Survey by DIA/DWO.

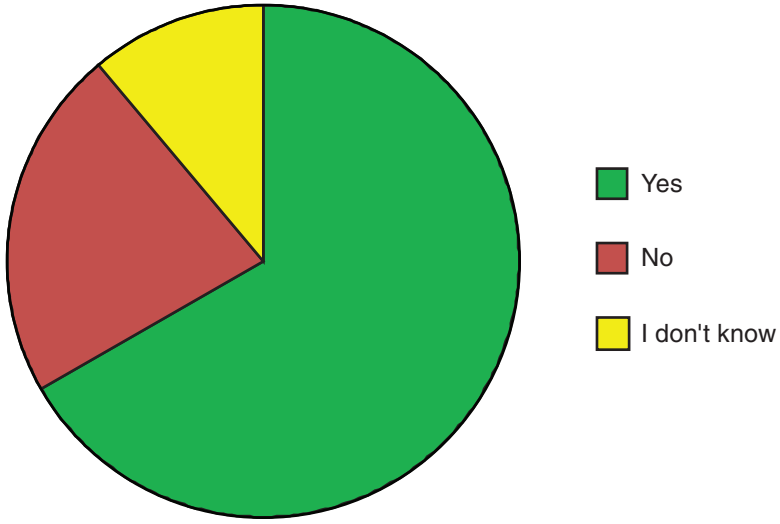

FIGURE D-3 Results in response to the question, Do you receive S&TI products on a regular basis? SOURCE: Survey by DIA/DWO.

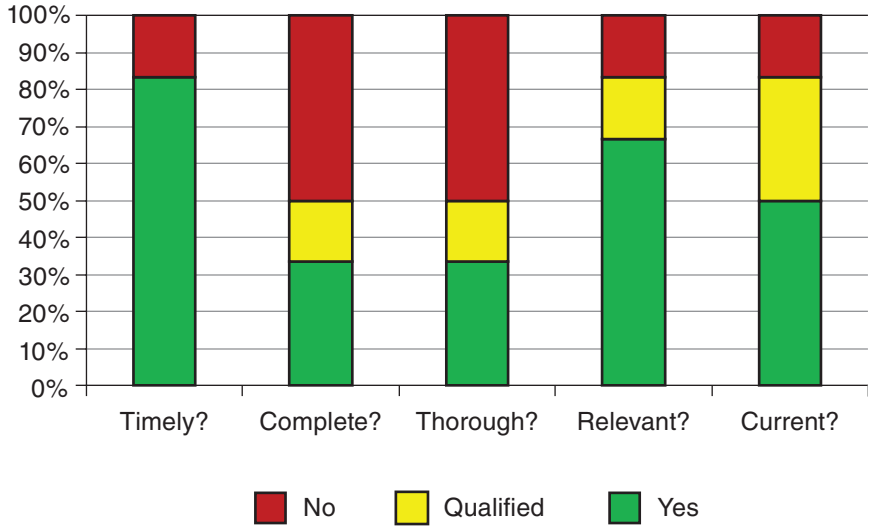

FIGURE D-4 Results in response to the question, If yes, would you say the S&TI products you receive are [timely, complete, thorough, relevant, and current]? SOURCE: Survey by DIA/DWO.

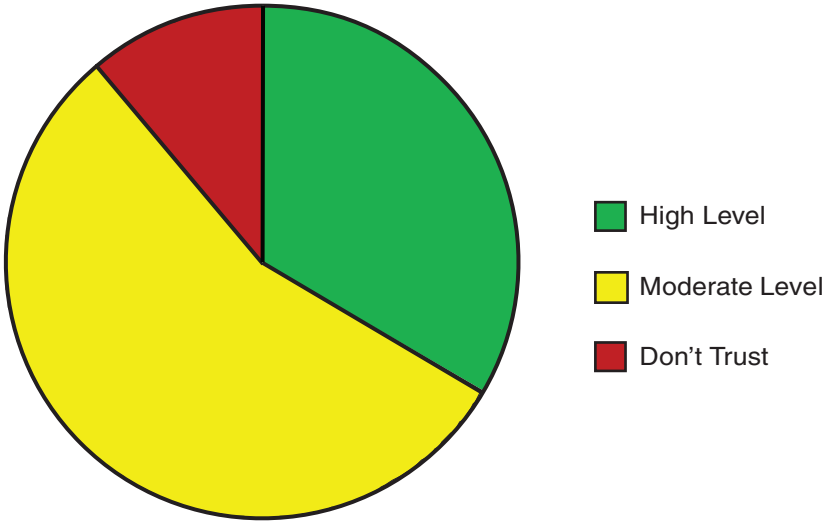

FIGURE D-5 Results in response to the question, How much do you trust the S&TI you receive? SOURCE: Survey by DIA/DWO.

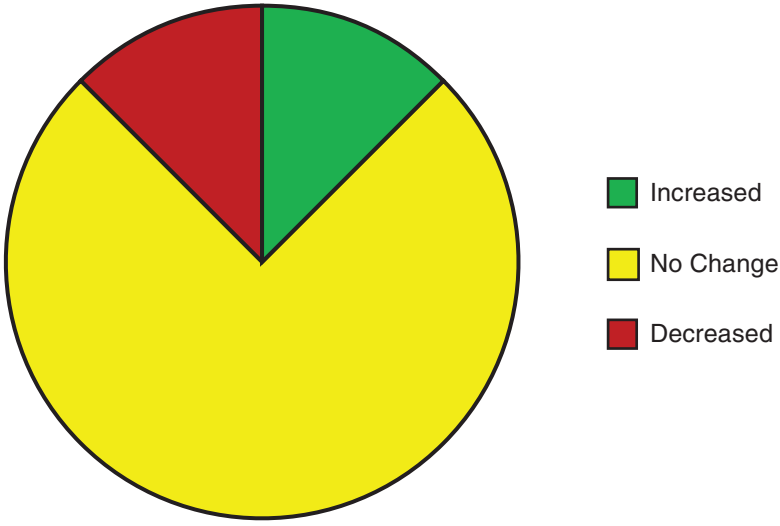

FIGURE D-6 Results in response to the question, Has your level of trust changed in the last 5 years? SOURCE: Survey by DIA/DWO.

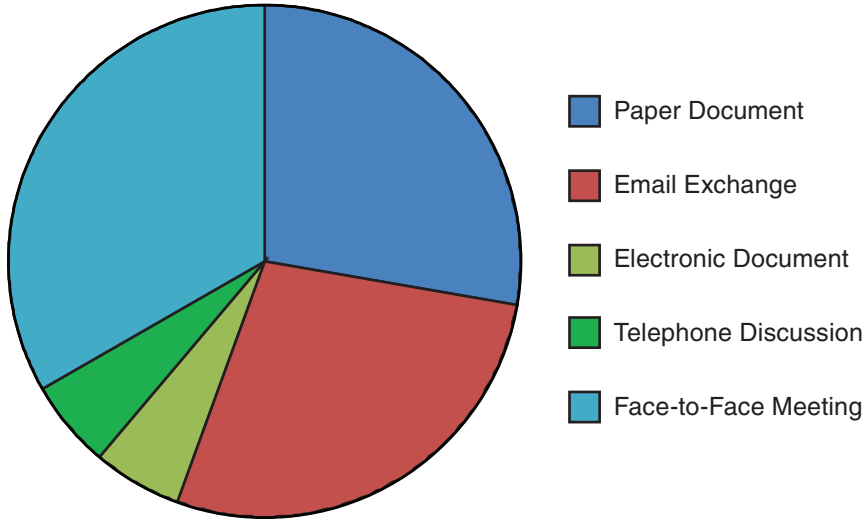

FIGURE D-7 Results in response to the question, In what form(s) do you prefer to receive S&TI information? SOURCE: Survey by DIA/DWO.

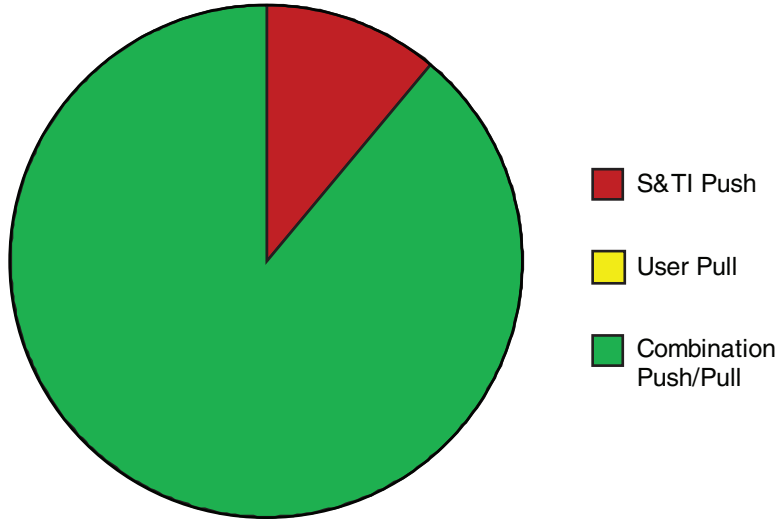

FIGURE D-8 Results in response to the question, Do you expect the IC to come to you with S&TI or primarily respond to user requests? SOURCE: Survey by DIA/DWO.

Appendix E

Questions Presented to Panels

The following questions, provided by the DIA/DWO, were posed to two parallel panel sessions in the symposium to motivate discussion by panel participants.

	Technology Surprise Problems	**S&TI (Scientific and Technical Intelligence) Solutions**
WHO	Whom do you see as future creators of technology surprise? • Can you name your top three in order of concern? *Responses may be nations, regions, transnational entities, institutions, individuals, etc.*	Whom do you go to for information on technology developments that may lead to surprise? • Whom do you formally task for S&TI? • Do you trust them to provide technically correct, balanced assessments? Why or why not?
WHAT	What are your top five technology surprise concerns? • At the strategic level? • At the operational level? • At the tactical level? What do you consider to be critical U.S. technologies that must be protected (e.g., night-vision technology)? • Where do your program managers go with questions or ideas about protecting our critical technologies?	What specific type of S&TI is most useful for your Command? • Long-term forecasts? • Technology transfer risk assessments? • Current military system capabilities? What positive action/changes have you been able to take in response to S&TI information you have received? What failures have occurred due to a lack of S&TI information?

continues

	Technology Surprise Problems	S&TI (Scientific and Technical Intelligence) Solutions
WHEN	When do you think technology surprise is most likely to occur? • What percentage of your Command's time is spent planning beyond the current conflict?	When would you like S&TI reporting to be delivered to you? • In response to requests for information? • Via IC initiative products? • Through tailored reporting based on your unique customer profile?
WHERE	Where do you think technology surprise is most likely to occur (e.g., within civil systems, military systems, on the battlefield, in space)? • Where are the greatest vulnerabilities to U.S. critical technologies?	Where should the S&TI community be focusing its effort? • Where should the responsibility for S&TI reside (e.g., at DOD, Services, Commands)?
HOW	How do you identify your S&TI needs? • How effective/useful are technology targeting risk assessments (TTRA) to program managers (are they meeting your needs)? • How proactive is your Command in seeking out S&TI?	How do you receive S&TI (e.g., in person, in hard copy, electronically)? • How would you like to receive S&TI?

Appendix F

Biographical Sketches of Invited Speakers

THE HONORABLE DENNIS BLAIR[1]

Admiral Dennis C. Blair became the nation's third director of national intelligence on January 29, 2009.

Prior to retiring in 2002, Admiral Blair served as commander in chief, U.S. Pacific Command, the largest of the combatant commands. During his 34-year Navy career, Admiral Blair served on guided missile destroyers in both the Atlantic and Pacific fleets and commanded the Kitty Hawk Battle Group. Ashore, he served as director of the Joint Staff and as the first associate director of Central Intelligence for Military Support at the CIA. He has also served in budget and policy positions on the National Security Council and on several major Navy staffs.

From 2003 to 2006, Admiral Blair was president and CEO of the Institute for Defense Analyses, one of the nation's foremost national security analysis centers. Most recently, he served as the John M. Shalikashvili Chair in National Security Studies at the National Bureau of Asian Research, and as the deputy director of the Project on National Security Reform, an organization that analyzes the U.S. national security structure and develops recommendations to improve its effectiveness.

A 1968 graduate of the U.S. Naval Academy, Admiral Blair earned a master's degree in history and languages from Oxford University as a Rhodes Scholar, and he served as a White House Fellow at the Department of Housing and Urban

[1]Information obtained from the Office of the Director of National Intelligence website on May 5, 2009; see http://www.dni.gov/blair_bio.htm.

Development. He has been awarded four Defense Distinguished Service Medals and has received decorations from the governments of Japan, Thailand, the Republic of Korea, and Australia.

THE HONORABLE JACQUES GANSLER[2]

Dr. Jacques S. Gansler, director of the Center for Public Policy and Private Enterprise and former Under Secretary of Defense for Acquisition, Technology, and Logistics, is the first holder of the Roger C. Lipitz Chair in Public Policy and Private Enterprise. As the third ranking civilian at the Pentagon from 1997 to 2001, Professor Gansler was responsible for all research and development, acquisition reform, logistics, advanced technology, environmental security, defense industry, and numerous other security programs. Before joining the Clinton Administration, Dr. Gansler held a variety of positions in government and the private sector, including deputy assistant secretary of defense (material acquisition), assistant director of defense research and engineering (electronics), vice president of ITT, and engineering and management positions with Singer and Raytheon Corporations. Throughout his career, Dr. Gansler has written, published, and taught on subjects related to his work. He is the author of *Defense Conversion: Transforming the Arsenal of Democracy*, MIT Press, 1995; *Affording Defense*, MIT Press, 1989; and *The Defense Industry*, MIT Press, 1980. He has published numerous articles in *Foreign Affairs*, *Harvard Business Review*, *International Security*, *Public Affairs*, and other journals as well as in newspapers and has provided frequent testimonies to Congress. He is a member of the National Academy of Engineering and a fellow of the National Academy of Public Administration.

MR. ROBERT HEGSTROM

Mr. Robert R. Hegstrom is the director of the Battlespace Awareness Portfolio within the Office of the Undersecretary of Defense for Intelligence, OUSD(I). In this position, he monitors, plans, and evaluates current and future intelligence programs, and he supports the undersecretary in the oversight of DOD intelligence capabilities.

Mr. Hegstrom began his career in 1989 as an intelligence analyst at the Foreign Technology Division (Wright-Patterson Air Force Base, Ohio). He published dozens of assessments on foreign space and ballistic missile capabilities. From 1996 to 2003, he worked at the Space Warfare Center (Schriever AFB, Colorado), first as the technical coordinator for modeling and simulation, and later as chief of the 25-person Wargaming and Simulation Branch. He was responsible for developing and executing the Space Warfare Center's strategic plan for modeling

[2]Information obtained from the University of Maryland's website on May 5, 2009; see http://www.publicpolicy.umd.edu/facstaff/faculty/gansler.html.

and simulation (M&S) support for DOD exercises, experiments, and wargames. He was also the game director for the highly successful Schriever 2001 wargame, the Air Force's first wargame with space as its focus.

Following senior service school at the Industrial College of the Armed Forces (ICAF) in 2003, Mr. Hegstrom completed a 30-month cross-functional assignment at the Pentagon including rotations in OSD/PA&E as a program analyst, the Joint Staff as a senior intelligence officer, and OUSD(I) as the deputy director for national collection programs. He also served as the deputy for the Intelligence, Surveillance, and Reconnaissance (ISR) team in the 2005 Quadrennial Defense Review. From 2006 to 2008, Mr. Hegstrom was the senior advisor for program analysis and evaluation within OUSD(I). He assumed his current position in August 2008.

Mr. Hegstrom is the recipient of a number of professional awards including the Air Force Decoration for Exceptional Civilian Service. He received a B.S. in electrical systems engineering, an M.S. in electrical engineering, and an M.S. in national resource strategy.