Avoiding Surprise in an Era of Global Technology Advances

Committee on Defense Intelligence Agency Technology Forecasts and Reviews, National Research Council

ISBN: 0-309-54916-7, 138 pages, 8 1/2 x 11, (2005)

AVOIDING SURPRISE IN AN ERA OF GLOBAL TECHNOLOGY ADVANCES

Committee on Defense Intelligence Agency Technology Forecasts and Reviews

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 HHM402-04-C-0015 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 views of the organizations or agencies that provided support for the project.

International Standard Book Number 0-309-09605-7

Limited copies of this report are available from:

Division on Engineering and Physical
Sciences, Room 940
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 20055
(800) 624-6242 or (202) 334-3313
(in the Washington metropolitan area)
Internet, http://www.nap.edu

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. Bruce M. Alberts 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. Wm. A. Wulf 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. Bruce M. Alberts and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON DEFENSE INTELLIGENCE AGENCY TECHNOLOGY FORECASTS AND REVIEWS

RUTH A. DAVID, *Chair*, ANSER, Inc., Arlington, Virginia
STEVEN R.J. BRUECK, University of New Mexico, Albuquerque
STEPHEN W. DREW, Science Partners, LLC, Summit, New Jersey
ALAN H. EPSTEIN, Massachusetts Institute of Technology, Cambridge
ROBERT A. FUHRMAN, Lockheed Corporation (retired), Pebble Beach, California
SHARON C. GLOTZER, University of Michigan, Ann Arbor
CHRISTOPHER C. GREEN, Wayne State University, Detroit, Michigan
DIANE E. GRIFFIN, Johns Hopkins Bloomberg School of Public Health, Baltimore, Maryland
J. JEROME HOLTON, Defense Group, Inc., Alexandria, Virginia
MICHAEL R. LADISCH, Purdue University, West Lafayette, Indiana
DARRELL D.E. LONG, University of California, Santa Cruz
FREDERICK R. LOPEZ, Raytheon Company, Goleta, California
RICHARD M. OSGOOD, JR., Columbia University, New York
STEWART D. PERSONICK, Private Consultant, Bernardsville, New Jersey
ALTON D. ROMIG, JR., Sandia National Laboratories, Albuquerque, New Mexico
S. SHANKAR SASTRY, University of California, Berkeley
JAMES B. SMITH, Raytheon Company, Tucson, Arizona
CAMILLO J. TAYLOR, University of Pennsylvania, Philadelphia
DIANNE S. WILEY, The Boeing Company, Arlington, Virginia

Staff

MICHAEL A. CLARKE, Lead Board Director
DANIEL E.J. TALMAGE, JR., Study Director
CARTER W. FORD, Research Associate
LANITA R. JONES, Senior Program Assistant

Preface

The development and writing of this report presented considerable challenges in terms of both the study schedule and the need to avoid conveying sensitive U.S. vulnerabilities to potential adversaries. Meeting both challenges has been difficult for the study committee and staff, but every effort was made to respond to the stated need of the Technology Warning Division of the Defense Intelligence Agency (DIA) for maximum openness.

I wish to express my appreciation to the members of the committee for their contributions to the preparation of this report. The committee is also grateful to the staff of the Technology Warning Division of the DIA for its sponsorship and active participation throughout the study.

The committee greatly appreciates the support and assistance of National Research Council staff members Michael Clarke, Daniel Talmage, LaNita Jones, and Carter Ford in the production of this report.

Ruth A. David, *Chair*
Committee on Defense Intelligence Agency
Technology Forecasts and Reviews

Acknowledgment of Reviewers

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

Bishnu Atal (NAS, NAE), AT&T Laboratories (retired),
Randy Katz (NAE), University of California, Berkeley,
Leslie Kenne, LK Associates,
Joshua Lederberg (NAS, IOM), The Rockefeller University,
John Lyons (NAE), U.S. Army Research Laboratory (retired),
Louis Marquet, Consultant,
S. Thomas Picraux, Arizona State University, and
Eugene Sevin (NAE), Consultant.

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 Robert Hermann, Global Technology Partners. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

Figures, Tables, Boxes, and Charts

FIGURES

TABLES

BOXES

CHARTS

Acronyms

ASIC	application-specific integrated circuit
BOLD	blood-oxygen-level dependent
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
C&C	computing and communications
CMOS	complementary metal-oxide semiconductor
COTS	commercial off-the-shelf
DARPA	Defense Advanced Research Projects Agency
DIA	Defense Intelligence Agency
DNA	deoxyribonucleic acid
DOD	Department of Defense
ECM	electronic countermeasures
EEG	electroencephalography
EMP	electromagnetic pulse
EMU	extravehicular mobility unit
EPROM	electron paramagnetic resonance oxygen mapping
ERP	event-related potential
FCS	Future Combat Systems
FLIR	forward-looking infrared
fMRI	functional magnetic resonance imaging
GDP	gross domestic product

GOTS	government off-the-shelf
GPS	Global Positioning System
IC	intelligence community
IFF	identification friend or foe
IP	Internet Protocol
IR	infrared
ISR	intelligence, surveillance, and reconnaissance
LED	light emitting diode
MANPADS	man-portable air defense system
MAV	micro air vehicle
MD-5	message-digest algorithm
MEG	magnetoencephalography
MEMS	microelectromechanical systems
MRI	magnetic resonance imaging
NIC	National Intelligence Council
NIRS	near-infrared spectroscopic imaging
NRC	National Research Council
NSF	National Science Foundation
OECD	Organisation for Economic Co-operation and Development
R&D	research and development
RCS	radar cross section
RF	radio frequency
RFID	radio-frequency identification
RPG	rocket-propelled grenade
S&T	science and technology
SAR	synthetic aperture radar
SHA	secure hash algorithm
SQUID	superconducting quantum interference device
TWI	The Welding Institute, Ltd.
UAV	unmanned aerial vehicle
UCAV	unmanned combat air vehicle
UV	ultraviolet
VTOL	vertical takeoff and landing
WMD	weapons of mass destruction

Executive Summary

The Defense Intelligence Agency (DIA) requested that the National Research Council (NRC) establish the Committee on Defense Intelligence Agency Technology Forecasts and Reviews to conduct meetings with the intelligence community (IC) in order to develop study topics relating to technology warning (see Box ES-1 for the overall statement of task for this effort).

The committee was asked to produce a report, based on its discussions with the intelligence community, that discusses capabilities upon which U.S. warfighters are dependent and to identify the potential for adversaries to threaten those capabilities through the exploitation of evolving technologies (see Box ES-2 for the report statement of task).

It is the intent of both the DIA Technology Warning Division as sponsor and the National Research Council that this first report, which is limited in scope, will establish the foundation for a long-term collaborative relationship to support the examination of technology warning issues. It is expected that such examination will be useful not only for the DIA but also for other members of the intelligence community who might need such analyses. It is intended that the current ad hoc committee be disbanded subsequent to the publication of this report and that a standing committee be formed to work with the IC to keep abreast of issues relating to technology warning and to develop specific statements of task for independent ad hoc committees of the NRC to perform.

SCOPE AND ORGANIZATION OF THE STUDY

U.S. military strength is built on a foundation of technological superiority that grew from a position of global leadership in relevant technologies and innovative capabilities. That leadership position is no longer assured. The synergistic forces of globalization and commercialization of science and technology are providing current and future adversaries with access to advanced technologies as well as the expertise needed to exploit those technologies.

The ability of the U.S. intelligence apparatus to warn of evolving technologies that, in the hands of adversaries, may threaten U.S. military preeminence is vital to the ability of the nation's leadership to make good decisions. The genesis of this report was the recognition by the DIA Technology Warning

BOX ES-1
Statement of Task

The National Research Council (NRC) will:

- Establish an ad hoc committee to provide technology analyses, both near and far term, to assist the agency to develop timelines, methodologies, and strategies for the application of identified technologies of interest to the Defense Intelligence Agency (DIA) under development within the United States and its allies and to bring to the agency's attention potentially useful technologies that DIA may not be aware of that might be of value for adaptation and consideration.
- Review information provided from government sources on technologies under development by other nations abroad and provide estimates on when these technologies may become mature to the point they could pose a threat to U.S. forces.
- Meet with the agency to discuss technology developments here and abroad of interest to DIA and to develop potential study topics and task statements for in-depth assessment of specific technical areas.
- Provide one or two short reports during the course of the first year on subjects developed in the course of meetings and as requested by the agency and approved by the NRC.

BOX ES-2
Report Statement of Task

For the first report, the National Research Council Committee on Defense Intelligence Agency Technology Forecasts and Reviews will:

- Develop, examine and review from unclassified sources evolving technologies that will be critical to successful U.S. warfighting capabilities.
- Postulate methods for potential adversaries of the United States to disrupt these technologies and discuss indicators for the intelligence community to investigate to determine if RED force elements are attempting to achieve this disruptive capability (this discussion should be generally unclassified with specific sensitive or classified information, limited to SECRET, placed in an appendix).
- Curtail its investigation to technologies consistent with the committee charter from the Defense Intelligence Agency Threat Analysis section (i.e., to exclude weapons of mass destruction (WMD) and areas of chemical/biological warfare not of specific interest to the sponsor).
- Identify and recommend specific technology areas to be pursued in greater depth, both in specificity and classification, in future reports requested by DIA.

Division, which sponsored the study, of the need to tap into new sources of information and expertise that exist in the nongovernmental scientific and technical communities.

Various lists exist that identify high-impact technologies projected to advance rapidly in the coming years. Virtually every such list contains some permutation of information technologies, biotechnologies, and nanotechnologies. From those lists it is relatively easy to identify a number of evolving technologies likely to impact national security. It is more difficult to identify those specific technologies that are potential "game-changers" in the hands of enemies of the United States, and even harder to envision potential innovations that may derive from the integration of multidisciplinary technologies to yield disruptive capabilities. These are the tasks levied on the technology warning community.

Owing to the study's time constraints, the technologies selected for inclusion in this report represent a sampling derived from the collective experience of committee members rather than from a comprehensive survey. The committee made no effort to rationalize its selection from among the broad array of evolving technologies of potential interest.

Therefore, rather than creating yet another list of potentially important technologies for the technology warning community to track, the committee chose to establish a framework that would enable ongoing identification, assessment, and prioritization of emerging technologies in terms of their potential impact on U.S. military capabilities. It is hoped that the methodology presented as a prototype in this report will provide the foundation for the ongoing collaborative relationship envisioned by the DIA Technology Warning Division.

Chapter 1 describes the challenges confronting the technology warning community, focusing on the impact of globalization and commercialization of the technology marketplace.

Chapter 2 outlines the methodology proposed by the committee. This methodology is "tested" in subsequent chapters. To provide focus, the committee's approach was anchored by the following question: *What capabilities does the United States have that, if threatened, impact U.S. military preeminence?* Subsequent steps in the methodology identify and assess emerging technologies and/or integrated capabilities that, in the hands of U.S. adversaries, could be used to defeat that U.S. military capability. The basic methodology is summarized Box ES-3.

Chapters 3 through 6 describe high-level U.S. military capabilities and potential threats to those capabilities. The focus of Chapter 3 is information superiority, which is identified in Joint Vision 2020 as a vital enabling capability (JCS, 2000). In Chapter 3, the committee identifies a number of generic vulnerabilities of information-technology-enabled systems and applications (including, in principle, those that might be used by BLUE (denoting U.S. military) forces to endeavor to maintain information superiority). These generic vulnerabilities could be attacked via evolving technologies and methodologies that, in most cases, are increasingly available to U.S. adversaries in the form of low-cost, commercial commodity products.

The committee focused specifically on potential pathways for disruption, denial, or degradation of communications and sensing capabilities. It considered system and/or network attacks as well as sensor attacks. The committee also identified, for each technology identified, potential observables that the technology warning community could use to analyze the intentions and/or capabilities of U.S. adversaries to employ these technologies and methodologies. Additional background information relating to Chapter 3 is provided in Appendix D.

Chapter 4 discusses air superiority, which underpins several of the Joint Vision 2020 operational concepts, with a focus on potential challenges in urban warfare. Future threats to U.S. airpower in urban warfare owe much to two factors—the trend toward globalization in aerospace and electronics, coupled with what has been observed to be the best way to defeat U.S. airpower: that is, not necessarily the head-to-head, platform-to-platform approach of the Cold War, but rather the exploitation of asymmetries.

BOX ES-3
Proposed Methodology for Technology Warning

Foundation	Joint Vision 2020[a] Operational Concepts and Information Superiority
• **Focus**	*What capabilities does the United States have that, if threatened, impact U.S. military preeminence?*
• **Identify**	*What are the evolving technologies that, in the hands of U.S. adversaries, might be used to threaten an important U.S. military capability?*
	What are the observables that may indicate adversarial adoption or exploitation of such technologies?
• **Assess**	*Accessibility: How difficult would it be for an adversary to exploit the technology?*
	Maturity: How much is known about an adversary's intentions to exploit the technology?
	Consequence: What is the impact on U.S. military capability should the technology be employed by an adversary?
• **Prioritize**	*Identify: What are the relative resources to be applied to each emerging technology to support the technology warning process?*
• **Task**	*Establish and assign intelligence-information-collection requirements.*

[a]SOURCE: JCS (2000).

One pillar of U.S. airpower in the past has been the capabilities of its major platforms. These sophisticated platforms now require investments of tens of billions of dollars spread over decades—investment levels that few foes can match. However, the life of the advanced technology in these platforms can now be less than the development cycle. Small, unmanned aerial vehicles (UAVs) offer a counter to large platforms; although they are much less capable than large platforms at the moment, they can have much shorter and less costly development cycles. These factors contribute to the proliferation of such vehicles around the world, especially at the smaller sizes (Munson, 1996).

The committee describes a variety of technologies that may enable adversaries to diminish the advantage currently held by U.S. airpower. The technologies are described in terms of the system characteristics that they would provide. The characteristics considered include increased range and/or reduced signature; enhanced guidance, navigation, and/or targeting; enhanced lethality; and other techniques that directly counter U.S. capabilities.

Chapter 5 discusses challenges relating to the needed ability to discriminate between friends, foes, and neutrals, as well as among various targets—key capabilities for precision engagement—and again

focuses on the urban warfare environment. The committee addresses new technology developments that might assist enemy combatants by allowing their identity and that of innocent noncombatants to be intermixed. Appropriate "spoofing" or other types of misidentification could cause the warfighter to engage a group of noncombatants, thus causing political and/or psychological damage to U.S. forces.

The committee notes that U.S. leadership can no longer be assumed for a number of the technologies discussed in Chapter 5. Japan, for example, is extremely strong in many areas of nanotechnology and in optical and electronic devices. China is, in many cases (such as photonics), the country with the best combination of high-technology manufacturing and design, and its expertise is increasingly employed by many high-technology U.S. firms. Europe has excellent research capabilities in the areas of semiconductor materials and devices; these can be and have been translated into start-up corporations.

As a result of this shift to offshore commercial vendors, important indicators of technological developments are likely to appear in open source literature, including commercial Internet sites, and at industrial fairs, particularly in Asia and Europe. Monitoring of key corporations is important. However, in many cases small or obscure start-ups are also of vital importance (suggesting that the tracking of venture capital may offer yet another set of relevant observables). In certain cases, the observation of critical manufacturing items (raw materials and/or equipment) may be useful.

Chapter 6 describes a number of prospective capabilities related to biotechnology and focuses on potential challenges to battle readiness and communications superiority. Biotechnological capabilities are rapidly expanding and becoming more and more readily available to scientists throughout the world. Emerging biotechnologies that may enable functional brain imaging, covert communications, the spread of disabling infections, and sensor spoofing are likely to affect the conduct of military operations and the status of national security in the future, as highlighted in Chapter 6.

The neuroimaging techniques of electroencephalography (EEG), magnetoencephalography (MEG), functional magnetic resonance imaging (fMRI), and near-infrared spectroscopic imaging (NIRS) provide direct measurement of brain function. The technology underlying these modalities is advancing rapidly and will allow a multitude of measurements. This technology may in the future provide a better understanding of behavior, performance, readiness, and stress that is relevant to troop readiness, the understanding of cultural differences in motivation, and prisoner interrogation.

There are many opportunities on the horizon for biology to play a role in covert communications. These include protein cube holography and bacteriorhodopsin solid-state devices for storing high-density information, and deoxyribonucleic acid (DNA) sequences as a medium for hiding covert messages.

Although infectious diseases are a continuing concern, offer opportunities for a wide range of genetic modifications, and could be deployed in many different ways, they are not a primary focus of this report. Lastly, the current emphasis on weapons of mass destruction has led to the development of sophisticated sensors that, when activated, trigger responses that can be costly in time and can limit troop responses. A release of materials that trigger the sensors while not being actual threats is one way of decreasing battle readiness in U.S. troops. The area of application of biotechnology to military purposes is currently wide ranging and will expand very rapidly over the next decade.

Chapter 7 provides general recommendations to the Defense Intelligence Agency Technology Warning Division that stem from the evolving nature of the global science and technology environment. The chapter also offers suggestions relating to the envisioned ongoing collaboration with the NRC. The committee's findings and recommendations are summarized below.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

Need for New Collaboration and Engagement

Finding 1: There is a multitude of evolving technologies for which advances are being driven by the nongovernmental, global, scientific and technical communities.

The information technology, biotechnology, microtechnology, and nanotechnology families will increasingly provide foundational building blocks for militarily relevant capabilities for RED (adversary) and BLUE (U.S.) forces alike. The fact that significant advances in these technologies will be driven largely by commercial demand—on a global scale—versus military-specific investment suggests the need for the technology warning community to establish a sustained relationship with the nongovernmental scientific and technical community in order to bolster its understanding and anticipation of technology trends.

Recommendation 1: The Defense Intelligence Agency Technology Warning Division, together with the related intelligence community components that focus on technology warning, should establish an ongoing collaborative relationship with the scientific and technical communities in the industrial and academic sectors.

The committee believes that the National Academies, through the National Research Council, provide both a window into these communities and an appropriate institutional mechanism that could assist in this endeavor.

Need for New Indicators

Finding 2: New intelligence indicators are likely to be needed to provide technology warning for the diverse spectrum of evolving technologies that are being driven by commercial forces in the global marketplace.

Traditionally, the United States has assumed that it leads the world in science and technology. This perspective leads the technology warning community to look for indications that external actors are trying to "catch up," or to exploit known technologies in new ways. Projected future trends suggest that it should no longer be automatically assumed that the United States will lead in all relevant technologies. This revised perspective imposes a new burden on the technology warning community, generating the need for it to search in different places and in different ways to be able to warn against technological surprise.

Recommendation 2: The Defense Intelligence Agency Technology Warning Division, in collaboration with the related intelligence community components that focus on technology warning, should establish, maintain, and systematically analyze a comprehensive array of indicators pertaining to globalization and commercialization of science and technology to complement and focus intelligence collection and analysis.

The committee believes that the observables identified in this report provide a useful baseline. However, it acknowledges that the first step in a more disciplined approach in technology warning should be to decompose the broad trends into potential observables more systematically and then to evaluate the utility and applicability of analytic techniques for technology warning already in use in Open Source Intelligence analysis. The committee also acknowledges that since not all relevant advances will stem from the global commercial open source environment, such an approach should complement but not supplant other collection techniques.

Need for Framework Methodology

Finding 3: The landscape of potentially important evolving technologies is both vast and diverse. A disciplined approach is thus needed to facilitate optimal allocation of the limited resources available to the technology warning community.

While it is relatively easy to create lists of technologies that will have military significance in the coming years, it is harder to identify those specific technologies that are potential game-changers in the hands of U.S. adversaries. The committee reviewed a diverse array of lists of technologies—each prioritized from a different perspective. Some lists focus on potential "disruptive" technologies that could have catastrophic consequences in the hands of adversaries, while others focus on technologies with significant commercial potential that may erode this nation's technological edge. The committee believes that the technology warning community would benefit from a disciplined approach to the identification and prioritization of the evolving technologies that may threaten U.S. military preeminence.

Recommendation 3: The Defense Intelligence Agency Technology Warning Division, in collaboration with the related intelligence community components that focus on technology warning, should adopt a capabilities-based framework within which to identify and assess potential technology-based threats.

The committee believes that a capabilities-based methodology enables a systematic approach to technology warning while reducing the tendency to focus only on advances in discrete technologies. The methodology presented as a prototype in this report was derived from the operational concepts and enablers described in Joint Vision 2020. It is offered as a starting point; the committee acknowledges that additional refinement is needed.

In Conclusion

The technology warning community, which plays a vital role in advising military leadership, is facing unprecedented challenges. BLUE force strategies are increasingly dependent upon technology-enabled capabilities assembled from building block technologies in which U.S. technological leadership is no longer assured. Foreign governments and nonstate actors are gaining access to the same building block technologies—often via the commercial marketplace. The committee applauds the Technology Warning Division's recognition that unprecedented challenges require new approaches and commends the efforts already underway.

REFERENCES

JCS (Joint Chiefs of Staff). 2000. Joint Vision 2020. Director for Strategic Plans and Policy, J5, Strategy Division. U.S. Government Printing Office, Washington, D.C. June.

Munson, Kenneth, ed. 1996. Jane's Unmanned Aerial Vehicles and Targets. Jane's Information Group, Coulsdon, Surrey, United Kingdom.

1

Technology Warning: Motivation and Challenge

INTRODUCTION

In the aftermath of the terrorist attacks of September 11, 2001, and Operation Iraqi Freedom, the U.S. populace is increasingly aware of the challenge of intelligence gathering, analysis, and forecasting. Those involved with such activities, working for the most part anonymously, are performing a service that is critical to the continuance of this nation's freedom. Recent events clearly illustrate the need for timely and accurate intelligence to aid tactical and operational planning for military operations as well as to support planning efforts related to homeland security. In this report, the committee focuses on the strategic issue of technology warning as it relates to military operations. Because U.S. military strength is built on a foundation of technological superiority, the ability of the U.S. intelligence apparatus to warn of evolving technologies that, in the hands of adversaries, may threaten U.S. military capabilities is vital to the ability of the nation's leadership to make informed decisions.

During the Cold War, the Soviet Union and its satellite nations were a central focus of the intelligence community (IC). That era seems in retrospect to have been a much simpler time with respect to the development and application of technology to national security missions. The possibility of technological surprise was always present, as evidenced by the Soviet Union's launch of *Sputnik* in 1957, but step functions in enemy warfighter capabilities were often anticipated in time to take countering steps.

That is not to say there were not enormous technological advances during the post-World War II era. Significant developments during the past 50 years that had direct implications for national security included stealth technology, improvement in target identification, precision weaponry, the information technology revolution, and the birth of the Internet. Even though the ongoing information revolution is driven primarily by the commercial marketplace and is global in scope, the U.S. military has to date successfully maintained a technological edge over its adversaries.

Rather than dealing with the relatively monolithic threat posed by the former Soviet Union, the United States now confronts a future of potential threats from many nation-states, as well as threats from extra- and transnational entities whose identities and allegiances are diffuse and complex—and whose technological prowess is enabled by globalization. These threats have also broadened in scope from conventional military threats to those also endangering civilian populations and economic targets.

The effect on the intelligence community has been dramatic. Not only must it deal with the complexity and diversity of these new threats, but it also must deal with a dynamic global environment in terms of technology development and exploitation. U.S. technological leadership cannot be assumed in the future.

STUDY ORIGIN

In full recognition of the reality that U.S. technological leadership can no longer be assumed, in the fall of 2003 the Defense Intelligence Agency (DIA) requested a series of meetings with National Research Council (NRC) staff members in the Division on Engineering and Physical Sciences to determine if a relationship was possible that would provide access not only to members of the National Academies and the nonmember technical community but also to the research community throughout the nation's universities and laboratories. The objective of the DIA was not intelligence gathering per se, but rather the development of a new source of information on burgeoning technologies and their potential for "technology surprise," with attendant military ramifications. In particular, the Technology Warning Division of the DIA recognized the potential value of ongoing engagement with the nation's technical communities in fulfilling its responsibility to "provide the earliest possible warning of technological developments that could undermine U.S. military preeminence" (DIA, 2004).

There were many issues to be overcome in order to establish the viable relationship that the DIA sought. The first concern of NRC staff members was security. It was assumed at the outset that much of the activity would necessarily be conducted at high levels of classification. The National Academies through the National Research Council can perform classified work and often does, but it is always the NRC's objective to serve the public while conducting the work of the Academies, and excessive classification can interfere with the openness sought. To the surprise of the committee chair and staff, a meeting with the director of the DIA shortly after formation of the committee dispelled the notion that the committee's work would necessarily be classified. While some activities of the committee might be classified, the director wanted the majority of the effort unclassified so as to facilitate sharing and collaboration between the intelligence community and the scientific and technical communities.

Upon receipt of a contract, the current 1-year ad hoc committee—the Committee on Defense Intelligence Agency Technology Forecasts and Reviews—was formed to conduct meetings with the intelligence community to study issues relating to technology warning. The committee was tasked to produce a report that discusses capabilities upon which U.S. warfighters are dependent and to identify the potential for adversaries to threaten those capabilities through the exploitation of evolving technologies. Technologies to be considered were to include not only those emerging from research establishments, but also potential adversarial capabilities that could arise from innovative integration or the application of existing technologies.

It was recognized from the outset that the present report would be somewhat general in nature with respect to the depth and breadth of technical analyses. It was the objective of both the DIA and the NRC that this first report would establish the foundation for a long-term relationship to support the examination of technology warning issues, not only for the DIA but also for other members of the intelligence community who might need such analyses. It is intended that the current ad hoc committee be disbanded subsequent to the publication of this report and that a standing committee be formed to work with the IC to keep abreast of issues relating to technology warning and to develop specific statements of task for independent ad hoc committees of the NRC to perform.

GLOBALIZATION IS RESHAPING THE TECHNOLOGY PLAYING FIELD

A recent report by the National Intelligence Council (NIC) observed: "We see globalization—growing interconnectedness reflected in the expanded flows of information, technology, capital, goods, services, and people throughout the world—as an overarching 'mega-trend,' a force so ubiquitous that it will substantially shape all the other major trends in the world of 2020" (NIC, 2004). While globalization has been underway for several decades, its intensity and pervasiveness have now greatly increased in magnitude and pace; the technology playing field is undergoing a massive change. Technology research and development (R&D), historically dominated by the United States, is increasingly distributed throughout the world. While the United States continued to lead the world in R&D spending in 2002, according to data from the Organisation for Economic Co-operation and Development (OECD),[1] other nations' shares are changing dramatically as they seek to boost economic performance and enhance global competitiveness. Figure 1-1 illustrates the relative shares of R&D spending in 2002 (AAAS, 2004a).

While the United States continues to dominate other nations of the world in terms of total R&D spending, comparisons of R&D spending as a ratio of gross domestic product (GDP) provide a different picture. The United States lags Japan in total R&D as a percentage of GDP (2.67 percent versus 3.12 percent in 2002) as well as in business R&D (1.87 percent versus 2.32 percent in 2002). Between 1995 and 2002, China doubled its spending on R&D when calculated as a percentage of GDP (1.2 percent in 2002). During that same period, Israel increased its spending from 2.74 percent to 4.72 percent of GDP, a ratio higher than that of any other OECD nation. Many countries have set long-term, stable targets for increasing R&D spending, with Austria aiming for 2.5 percent of GDP by 2006, Germany targeting 3 percent by 2010, and the United Kingdom targeting 2.5 percent by 2014. Canada has set a goal of being among the top five investors in R&D among OECD countries, and Korea has committed to doubling its R&D investment between 2003 and 2007 (OECD, 2004b). These trends are indicative not only of the growing importance that nations are placing on R&D but also of prospective challenges to U.S. technological leadership. The long-term commitment of other countries to basic high-technology research funding is particularly significant.

Additional indicators may be derived from the increasingly global distribution of science and engineering talent as nations increase the capacity and quality of their higher-education systems and entice their citizenry to stay home or to return from studies abroad to serve growing national economies and research enterprises. In 1999, 13 nations (United Kingdom, Finland, South Korea, Japan, Taiwan, Norway, Canada, Sweden, Netherlands, Germany, Ireland, France, Spain) outranked the United States in the ratio of first university degrees in the natural sciences and engineering to the 24-year-old population, while in 1975 the United States ranked third (NSB, 2003).

Forces relating to globalization inevitably led U.S. corporations to outsource R&D in order to take advantage of the distributed expertise, but also to help gain entry to foreign markets. In particular, U.S. companies are leveraging research capabilities in countries such as Israel, Sweden, India, and Taiwan (Bromley, 2004). Some U.S. companies take advantage of foreign research establishments, such as the Motorola collaboration with the Hong Kong Science and Technology Parks Corporation.[2] Others establish their own research facilities, such as the Microsoft Research laboratories in Beijing, China;

[1]The OECD nations are Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom, and United States.

[2]See, for example, http://www.hkstp.org/english/university/university.html. Last accessed on February 11, 2005.

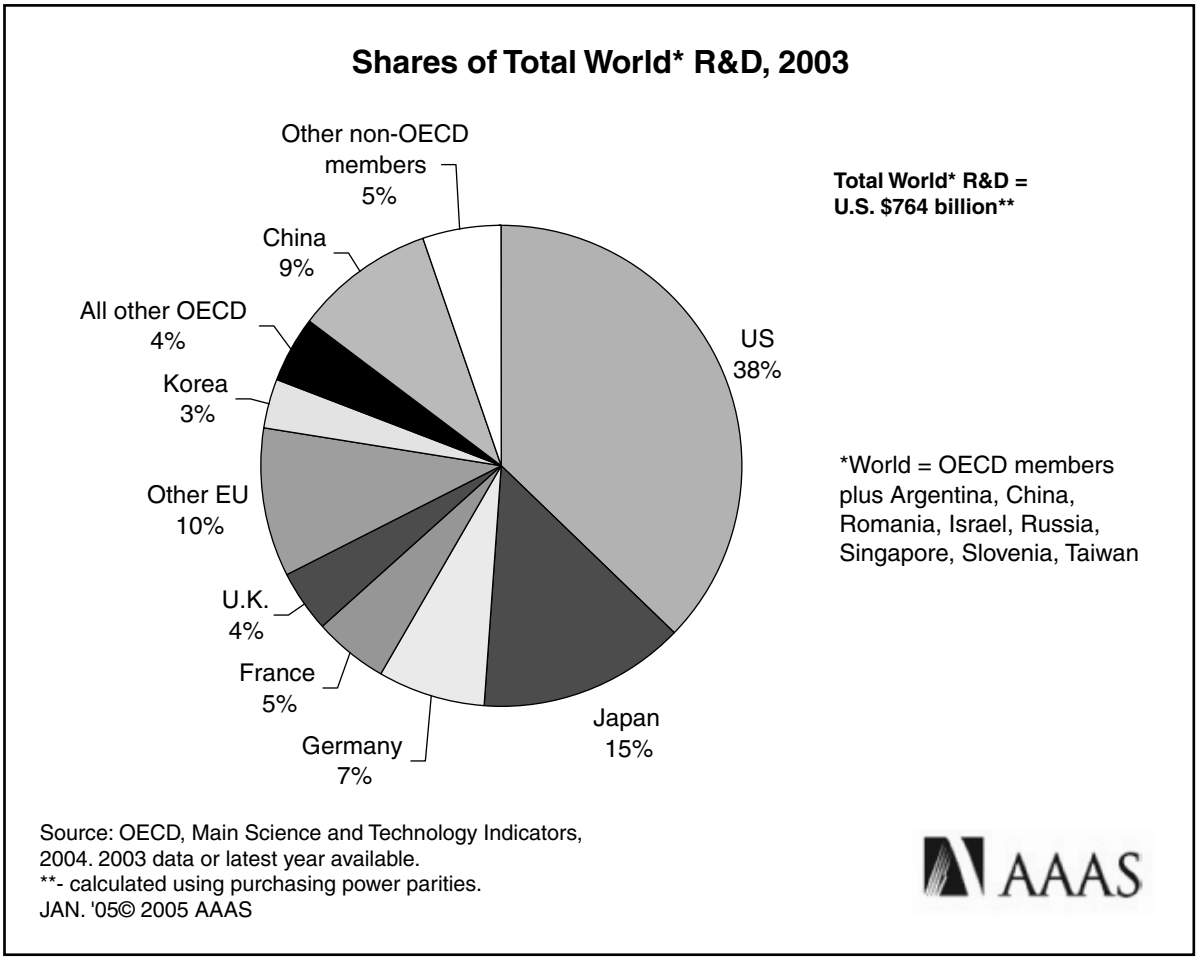

FIGURE 1-1 Shares of total world R&D, 2003 (as adapted from "Main Science and Technology Indicators: Volume 2004 Issue 2; Principaux indicateurs de la science et de la technologie: Volume 2004-2," © OECD, 2004). SOURCE: Reprinted with permission from AAAS (2004a). ©AAAS, 2005.

Bangalore, India; and Cambridge, United Kingdom (Microsoft, 2002). Based on such trends, it is clear that multinational corporations in high-technology commercial sectors will be less and less able to confine technological advances to any one nation.

COMMERCIALIZATION IS CHANGING THE TEMPO OF TECHNOLOGICAL INNOVATION

Many have observed the growing importance of commercial technologies to the defense establishment. Harvard University Professor Ashton Carter contrasted the defense technologies of the Cold War era with those of the future, as shown in Table 1-1.

A variety of factors are driving this changing nature of defense technology. The U.S. defense establishment recognized many years ago the benefits of "dual-use" technologies, and it provided

TABLE 1-1 The Changing Nature of Defense Technology

Cold War	⇒	Future
Defense Technology		*Defense Technology*
Originates in defense technology base	⇒	Originates in commercial technology base
that is embedded in defense companies	⇒	that is embedded in commercially driven companies
residing in the United States	⇒	that are global
for which defense is main driver.	⇒	for which defense is niche player.

SOURCE: Excerpted from Carter et al. (2000).

TABLE 1-2 The Nature of Innovation Is Changing

From	To
Invention	Innovation
Linear innovation model	Dynamic innovation mode
Build to forecasted demand	Sense and respond to demand
Independent	Interdependent
Single discipline	Multiple discipline
Product functions	Value to customer
Local R&D teams	Globalized 24x7 R&D teams

SOURCE: COC (2004). Reprinted with permission from the Council on Competitiveness.

funding to stimulate the development of such technologies.[3] In other areas, such as information technologies, significant drivers stem from the commercial marketplace, which, as discussed above, is increasingly global. The fact is that defense capabilities are increasingly dependent on innovations developed by commercial companies for the commercial market in many sectors, including telecommunications, aerospace, microelectronics, data processing, cryptography, special materials, biotechnology, and propulsion (DSB, 1999).

What this shift means is that the U.S. defense establishment is no longer in the driver's seat with regard to militarily relevant technological innovation. While U.S. technological advances in areas such as stealth technologies and satellite imagery once afforded multidecade military advantage, the rapid pace of technological innovation driven by the global commercial marketplace is shifting the advantage to those who rapidly adopt, exploit, and integrate evolving technologies. While defense-specific investments will continue to spawn important technological advances, U.S. technological superiority is no longer assured. Small, research-seeded start-ups are of special importance in the generation of high-technology ideas and products.

A recent report published by the Council on Competitiveness observes the acceleration of technological innovation as measured by market penetration. "It took the automobile 100 years to penetrate 50% of the global market. It took the telephone 75 years and electricity took 50 years. By comparison, the rise of cell phones, for example, has been nothing less than meteoric—faster than the personal computer—faster than the Internet" (COC, 2004). The report further observes that the nature of innovation is changing, as postulated in Table 1-2.

[3]Dual-use technologies have both military utility and sufficient commercial potential to support a viable industrial base; see, for example, http://www.dtic.mil/dust/faq.htm. Last accessed on February 11, 2005.

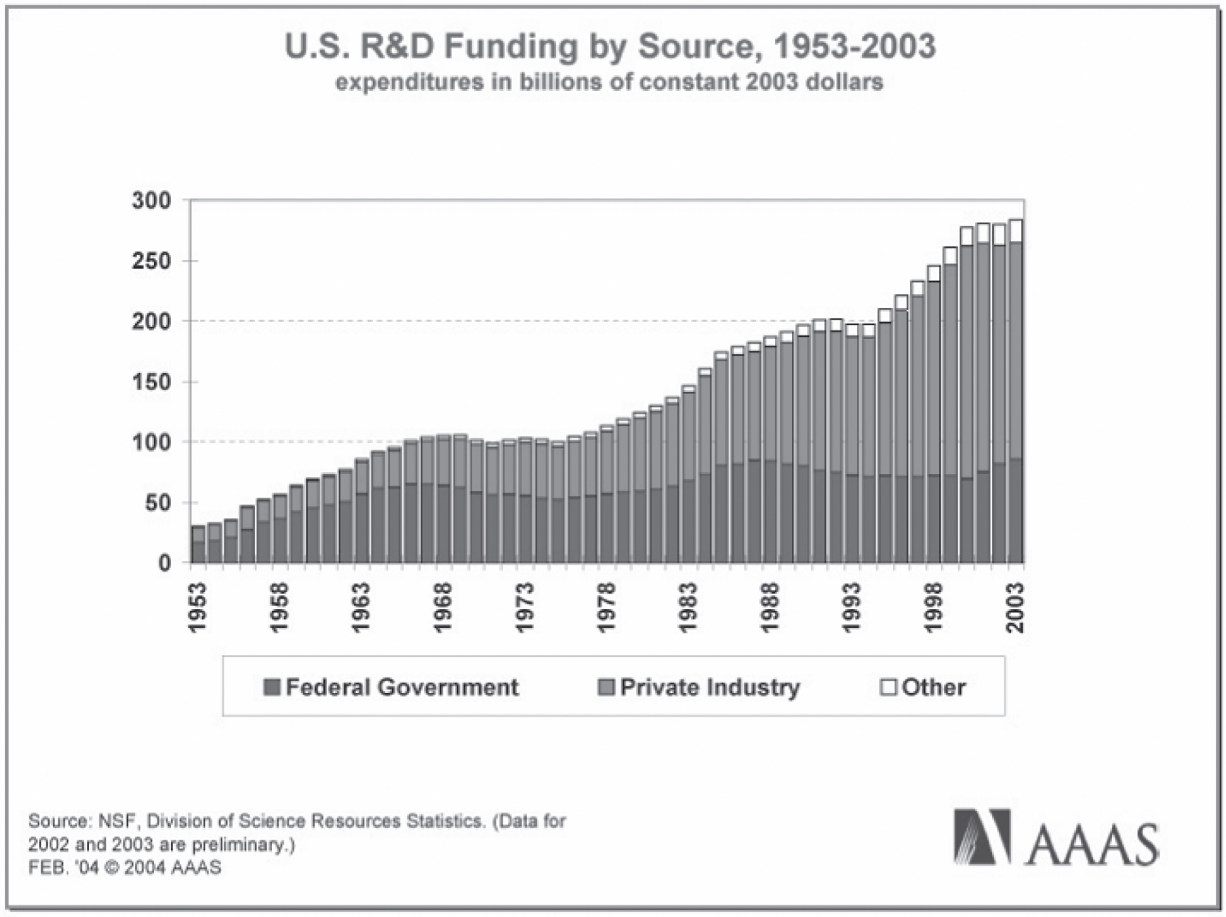

FIGURE 1-2 U.S. R&D funding by source, 1953–2003 (expenditures in billions of constant 2003 dollars). Data based on National Science Foundation's Division of Science Resources Statistics. Available online at http://www.nsf.gov/statistics/pubseri.cfm?TopID=8&SubID=6&SeriID=4. SOURCE: Reprinted with permission from AAAS (2004b). ©AAAS, 2004.

Further indication that private-sector investment is driving technological innovation is provided in Figure 1-2, which shows the relative contributions to R&D funding by the U.S. government and the private sector from 1953 through 2003. Note that private-sector investment increased sharply during the 1990s, while government funding remained relatively flat. While private-sector spending was at least partially driven by the boom in information technologies, the ratio between government and private investments remains indicative of the trend toward technology commercialization. The profit motive and the associated availability of large amounts of investment capital result in the rapid commercialization of new technologies that are perceived by investors to address unmet market needs. This leads to, among other things, a very short interval between the first appearance of an advanced-technology-enabled operational capability and the time when it is a low-cost, widely available commodity. Flat-panel displays are a recent example; cellular phones are another.

Looking to the future, the information revolution continues to fuel the synergistic trends of globalization and commercialization of technologies. As observed in a recent NIC report, "a nation's level of technological achievement generally will be defined in terms of its investment in *integrating and applying* the new, globally available technologies—whether the technologies are acquired through a country's own basic research or from technology leaders" (NIC, 2004). Thus, while patterns and trends in R&D investments provide useful indicators of the distributed research talent, the globalization of manufacturing facilities may indicate an equally important trend in distributing systems integration expertise.

THE TECHNOLOGY WARNING CHALLENGE

It is relatively easy to create a list of technologies that will have military significance in the coming years. It is far more difficult to identify those specific technologies that are potential "game-changers" in the hands of the nation's enemies. And it is even more difficult to envision potential adversaries' innovations that derive from multidisciplinary technology integration to yield disruptive capabilities. Yet this is the task levied on the "technology warning" organizations of the intelligence community.

The technology warning challenge is further complicated by the fact that adversaries are not necessarily bound by the legal, moral, and ethical standards that govern the U.S. development and application of science and technology. This is particularly true in some areas of biological and genetic research. "As deoxyribonucleic acid (DNA) manipulation becomes technologically and commercially viable, it has significant implications for both commercial and military uses that may not be pursued with equal fervor by all societies," as noted by Brown (2003). It is arguably easier to be "surprised" by an adversary who is willing to employ technology-based capabilities that this nation would not consider using.

A number of sources provide lists of technologies prioritized from different perspectives. Some lists focus on potential "disruptive" technologies that could have catastrophic consequences in the hands of U.S. adversaries, while others focus on technologies with significant commercial potential that could erode the U.S. technological edge. Three families of technologies that appear in some form on virtually every list are information technology, biotechnology, and nanotechnology. The technology warning challenge, however, is to characterize more specifically the applications of these technologies that may jeopardize U.S. military advantage.

The 2004 Strategic Planning Guidance calls for the U.S. military to better prepare for a wide range of challenges, including "irregular, catastrophic and disruptive threats." Potentially disruptive technologies include "breakthroughs in sensors, information technology, biotechnology, miniaturization on the molecular level, and cyber operations—capabilities so spectacular they would quickly give an adversary an edge" (Sherman, 2005). The threat of surprise due to disruptive technology, while not seen as a near-term threat, is viewed as one to which the United States is most vulnerable—at least in part owing to the nation's heavy reliance on technology-based military capabilities.

A 2001 study sponsored by the Central Intelligence Agency enlisted an external panel of experts that identified three tiers of technologies likely to impact national security by the 2015 time frame (OTI IA, 2001). Candidate technologies included those shown in Box 1-1. The definitions used by the panel are provided in Appendix C. The first-tier technologies, those most likely in the panel's view to have the greatest impact, include gene therapy, wireless communications, image understanding, cloned or tailored organisms, microelectromechanical systems (MEMS), and nanotechnology. Second-tier technologies, those seen as dependent upon particularly vigorous innovation, include optical communications, regenerative medicine, efficient software development, sensor webs, and advanced materials. The panel concluded that third-tier technologies are likely to remain just below the threshold of steady adoption

BOX 1-1
Candidate Technologies Likely to Impact National Security by the 2015 Time Frame, Identified by a Panel of Experts

First Tier: High-Impact Technologies
- Gene Therapy
- Wireless Communications
- Image Understanding
- Cloned or Tailored Organisms
- MicroElectroMechanical Systems (MEMS)
- Nanotechnology

Second Tier Technologies
- Optical Communications
- Regenerative Medicine
- Efficient Software Development
- Sensor Webs
- Advanced Materials

Third Tier: Below-Threshold Technologies
- Hypersonic/Supersonic Aircraft
- Next-Generation Space Shuttle System
- Alternative Energy
- Distributed Energy
- New-Generation Nuclear Power Plants
- Fuel Cells

Other Technologies Considered
- Brain-Machine Interfaces
- "Smart" Materials (organic and inorganic)
- Distributed-Grid-Based Processing Systems
- Performance-Enhancing Drugs
- Multilingual Voice Recognition
- Molecular Electronics
- Ubiquitous Water Generation
- High-Power Lasers
- Directed Energy (Microwave)

NOTE: See definitions of these technologies in Appendix C of this report.
SOURCE: OTI IA (2001).

TABLE 1-3 Challenges Identified for the National Nanotechnology Initiative

Time Frame	Strategic Challenge
Nano-now	• Pigments in paints • Cutting tools and wear-resistant coatings • Pharmaceuticals and drugs • Nanoscale particles and thin films in electronic devices • Jewelry, optical, and semiconductor wafer polishing
Nano-2007	• Biosensors, transducers, and detectors • Functional designer fluids • Propellants, nozzles, and valves • Flame-retardant additives • Drug delivery, biomagnetic separation, and wound healing
Nano-2012	• Nano-optical, nanoelectronics, and nanopower sources • High-end flexible displays • Nano-bio materials as artificial organs • NEMS-based devices • Faster switches and ultra-sensitive sensors

NOTE: NEMS, nanoelectromechanical systems.
SOURCE: NAE (2004).

absent unforeseen market potential or government assistance; technologies in this category include hypersonic military and supersonic commercial aircraft, next-generation space shuttle system, alternative energy, distributed energy, new-generation nuclear power plants, and fuel cells (OTI IA, 2001).

A recent National Academy of Engineering report (NAE, 2004) identifies a list of "breakthrough" technologies and/or applications that engineers will be expected to contend with by 2020. The list includes biotechnology, nanotechnology, materials science and photonics, information and communications technology, the information explosion, and logistics (NAE, 2004). Advances in nanotechnology will be driven at least in part through government investment in the U.S. National Nanotechnology Initiative, which budgeted nearly $1 billion in research and funding for fiscal year 2004. Strategic challenges identified for the National Nanotechnology Initiative are shown in Table 1-3.

Yet another perspective is provided by a Web-based survey conducted by *R&D Magazine* in which readers were asked to choose five technologies that are expected to see rapid growth and high investments in 2005 (Studt, 2005). According to the survey, the top three technologies are fuel cells, nanotechnology, and antibioterrorism devices. More than 225 readers responded to the survey; in a separate question, nearly 60 percent of the respondents revealed that they had some involvement in the technologies that they selected (Studt, 2005).

While derived from disparate sources, these lists of important technologies (as well as other lists shown to the committee) bear remarkable similarities in terms of the underlying technological foundations. So rather than creating yet another list of potentially important technologies for the technology warning community to track, the committee chose to establish a framework that would lend itself to the ongoing identification and prioritization of technologies in terms of their potential impact on the U.S. military's operational capabilities. The committee's framework and methodology are discussed in Chapter 2 of this report. Chapters 3 through 6 contain the committee's initial assessments within specific technology areas, and Chapter 7 provides general recommendations and suggestions for the path ahead.

LIMITATIONS OF THIS STUDY

Although a 1-year contract was established to support the work of this ad hoc committee, only three 2-day meetings were convened. This schedule provided limited time for committee members to develop a common understanding of the DIA Technology Warning Division's needs as well as to discern what the division already knows with respect to technologies of potential interest. Thus, this report contains some "tutorial" information, as well as commentary, relating more specifically to the technology warning challenge.

In addition, due to the limited time available for analysis, committee members tended to address technologies with which they were personally familiar rather than attempting to rationalize selections from among the broad array of technologies of potential interest. This report therefore focuses on a few specific technologies and applications rather than attempting to provide a "complete" or prioritized list of important evolving technologies.

Furthermore, the Technology Warning Division asked that the committee specifically exclude technologies relating to adversarial threats posed by weapons of mass destruction, since that topic is outside the division's scope of responsibilities. It was acknowledged that such issues may be the subject of future studies, but in this report the coverage is, as requested, only notional.

It is the committee's intent that this report provide the framework and basis for an ongoing collaborative relationship between the intelligence community's technology warning community and the National Research Council. Committee members are, however, mindful of the caution expressed by the United States Commission on National Security/21st Century, which concluded that "U.S. intelligence will face more challenging adversaries, and even excellent intelligence will not prevent all surprises" (USCNS, 1999).

REFERENCES

AAAS (American Association for the Advancement of Science). 2004a. U.S. Leads World in R&D Spending, China Moves to 3rd Place. Guide to R&D Funding Data—International Comparisons. Available online at http://www.aaas.org/spp/rd/guiintl.htm. Last accessed on February 8, 2005.

AAAS. 2004b. Guide to R&D Funding Data—Total U.S. R&D (1953-2003). Available online at http://www.aaas.org/spp/rd/guitotal.htm. Last accessed on February 8, 2005.

Bromley, D.A. 2004. Technology policy. Technology in Society 26(2/3):455-468.

Brown, Michael E., ed. 2003. Grave New World: Security Challenges in the 21st Century. Georgetown University Press, Washington, D.C. ISBN 0-87840-142-3.

Carter, Ashton B., with Marcel Lettre and Shane Smith. 2000. Keeping the technological edge, pp. 127-162 in Keeping the Edge: Managing Defense for the Future. Ashton B. Carter and John P. White, eds. MIT Press, Cambridge, Mass. ISBN 0-9705414-0-6.

COC (Council on Competitiveness). 2004. 21st Century Innovation Working Group. Innovation: The New Reality for National Prosperity: 21st Century Innovation Working Group Recommendations, Version 2.1. December 15. Available online at http://www.compete.org/docs/pdf/NII_21st_Century_Innovation%20Report.pdf. Last accessed on April 8, 2005.

DIA (Defense Intelligence Agency). 2004. Fact Sheets on Intelligence Agency Components. Washington, D.C.

DSB (Defense Science Board). 1999. Final Report of the Defense Science Board Task Force on Globalization and Security. Office of the Under Secretary of Defense for Acquisition and Technology, Washington, D.C. Available online at http://www.acq.osd.mil/dsb/reports/globalization.pdf. Last accessed on February 8, 2005.

Microsoft Corporation. 2002. Meeting of the Minds: Microsoft Research Asia Conference Spurs Collaboration Among Region's Researchers. Beijing, China. Available online at http://www.microsoft.com/presspass/features/2002/oct02/10-17msrasia.asp. Last accessed on February 8, 2005.

NAE (National Academy of Engineering). 2004. The Engineer of 2020: Vision of Engineering in the New Century. The National Academies Press, Washington, D.C.

NIC (National Intelligence Council). 2004. Mapping the Global Future. Government Printing Office, Pittsburgh, Pa. ISBN 0-16-073-218-2.

NSB (National Science Board). 2003. The Science and Engineering Workforce—Realizing America's Potential. Available online at http://www.nsf.gov/nsb/documents/2003/nsb0369/nsb0369.pdf. Last accessed February 7, 2004.

OECD (Organisation for Economic Co-operation and Development). 2004a. Main Science and Technology Indicators: Vol. 2004, Issue 2; Principaux indicateurs de la science et de la technologie: Vol. 2004-2.

OECD. 2004b. OECD Countries Spend More on Research and Development, Face New Challenges. Available online at http://www.oecd.org/document/2/0,2340,en_2649_201185_34100162_1_1_1_1,00.html. Last accessed on February 7, 2005.

OTI IA (Office of Transnational Issues, Intelligence Analysis). 2001. Global Technology Scenarios Through 2015: America's Game to Lose. OTI-IA 2001-083. CIA Analytic Report. November.

Sherman, Jason. 2005. More cuts to major weapons programs could be on the way in 2005 QDR. Inside the Air Force 16(1): 16-17.

Studt, Tim. 2005. R&D's hot technologies for 2005. Reed Business Information. Available online at http://www.rdmag.com/ShowPR.aspx?PUBCODE=014&ACCT=1400000100&ISSUE=0412&RELTYPE=PR&ORIGRELTYPE=CVS&PRODCODE=00000000&PRODLETT=BZ. Last accessed on February 7, 2005.

USCNS (United States Commission on National Security/21st Century). 1999. New World Coming: American Security in the 21st Century, Major Themes and Implications: Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century, Washington, D.C. Available online at http://govinfo.library.unt.edu/nssg/Reports/NWC.pdf. Last accessed on April 8, 2005.

2

Committee Methodology

With the context and scope of its assignment established, the committee turned its attention to defining a robust methodology for technology warning that would be suitable for the diverse inquiries likely to stem from ongoing engagement between a standing committee of the National Research Council (NRC) and the intelligence community's (IC's) technology warning components. The proposed methodology is described in this chapter and tested through application in subsequent chapters.

KEY FEATURES OF THE METHODOLOGY

A robust methodology for technical inquiry should have four key features. First, to be accepted, it must be presented in a lexicon and structure appropriate for the user's culture—in this case, for the culture in which the Defense Intelligence Agency (DIA) Technology Warning Division (the sponsor of this study) operates. Any communication of findings, conclusions, or recommendations offered by the committee must be expressed accordingly. The division makes use of weather-forecasting terminology (Futures, Watch, Warning, Alert)[1] in the issuance of technology assessments, making the overall warning message regarding all products readily interpretable by any reader. The committee adopted and adapted the DIA's vocabulary to characterize the relative status—and recommended action—for each technology.

The second key feature is that, to be relevant, the study methodology must be tied in a fundamental way to top-level Department of Defense (DOD) strategies. For example, the committee reviewed Joint Vision 2020 (JCS, 2000) to validate its selection of the technology topics addressed in this report. In future studies, to facilitate integration into the larger body of intelligence materials, the committee proposes that technology selections be derived through a more disciplined, RED team[2] review of top-

[1]The definitions used by the DIA for these terms are as follows: Futures—Create a technology roadmap and forecast; identify potential observables to aid in the tracking of technological advances. Technology Watch—Monitor global communications and publications for breakthroughs and integrations. Technology Warning—Positive observables indicate that a prototype has been achieved. Technology Alert—An adversary has been identified and operational capability is known to exist.

[2]"RED" is used in this report to denote the adversary or an adversarial perspective (e.g., "RED team").

level strategy documents (e.g., Joint Vision 2020) with an eye to identifying technologies that could be used to deny a BLUE[3] capability deemed critical to U.S. military success.

The third key feature is that, to maintain focus and ensure timeliness, the study methodology must yield assessments built on a solid understanding of the technical feasibility of potential technology-based threats. This requirement leads to a capability-based approach for investigating and categorizing candidate technologies. Furthermore, the technical peer review process to which all NRC reports are subjected provides additional assurance of the technical quality of committee assessments.

Lastly, to be enduring, the methodology should accommodate evolving realities of science and technology (S&T) leadership, driven by the synergistic trends of globalization and commercialization described in Chapter 1. Traditionally, the United States has assumed that it leads the world in S&T. This perspective leads the technology warning community to look for indications that external actors are trying to "catch up," or to exploit known technologies in new ways. Projected trends suggest that it should no longer automatically be assumed that the United States will lead technological advances in all relevant technologies. This reality imposes a new burden on the technology warning community, generating the need for it to search in different places and in different ways for the information needed to warn against technology surprise.

FOUNDATION OF THE METHODOLOGY

The committee believes that the Technology Warning Division can most effectively prioritize its limited resources by utilizing a capabilities-based approach with respect to assessing technologies. The landscape of potentially important emerging technologies is both vast and diverse. Ideally, the division should assess whether a given technology has the potential to pose a viable threat prior to commissioning in-depth analyses. Since the division is keenly interested in when specific technologies may mature to the point that they pose a threat to U.S. forces, a functional decomposition from an adversarial, or RED, perspective is most useful. The methodology defined by the committee begins with the following focus question: *What capabilities does the United States have that, if threatened, impact U.S. military preeminence?*

In general, U.S. capabilities could be threatened either through direct denial of or disruption of BLUE capabilities or via RED capabilities that negate or significantly diminish the value of BLUE capabilities (e.g., improvised explosive devices (IEDs) being employed by insurgent forces in Iraq).

Joint Vision 2020 was used to define the basic framework for U.S. military capabilities deemed vital to sustained success (JCS, 2000). The overarching focus of this vision is Full Spectrum Dominance—achieved through the interdependent application of four operational concepts (Dominant Maneuver, Precision Engagement, Focused Logistics, and Full Dimensional Protection) and enabled through Information Superiority, as illustrated in Figure 2-1 (JCS, 2000). The committee selected the four operational concepts, together with Information Superiority, as the foundation for its assessment methodology. Joint Vision 2020 provides the definitions presented in Box 2-1.

The committee also noted the importance of technology warning with respect to the "Innovation" component of Joint Vision 2020 shown in Figure 2-1, since "leaders must assess the efficacy of new ideas, the potential drawbacks to new concepts, the capabilities of potential adversaries, the costs versus benefits of new technologies, and the organizational implications of new capabilities" (JCS, 2000).

From this foundation the committee then identifies specific capabilities in accordance with the

[3]"BLUE" is used in this report to denote U.S. military forces.

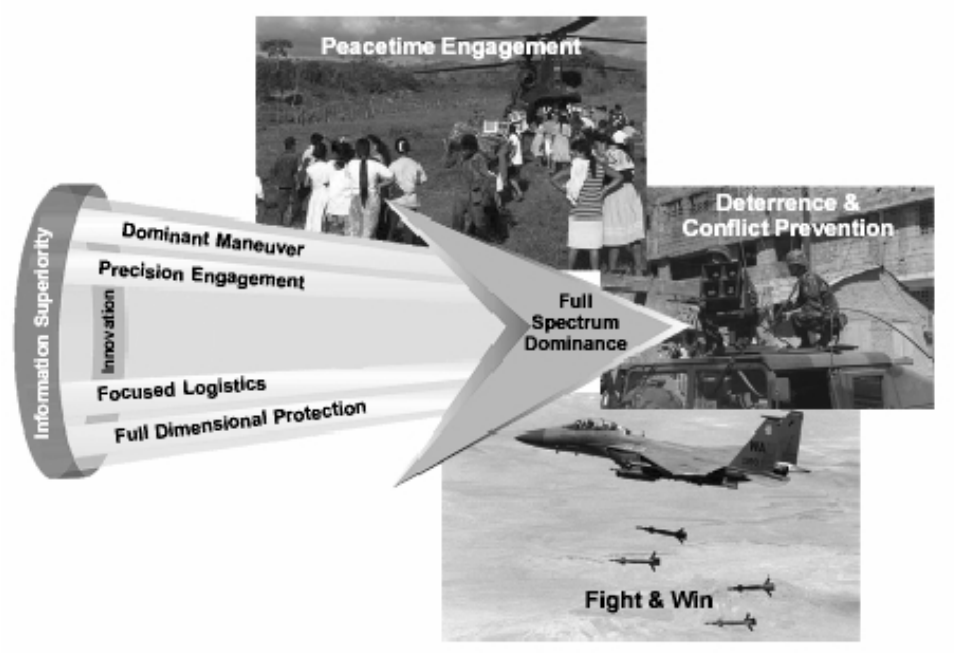

FIGURE 2-1 Concepts constituting the basic framework for U.S. military capability as defined by Joint Vision 2020. (See Box 2-1.) SOURCE: JCS (2000).

previously defined focus question—*What capabilities does the United States have that, if threatened, impact U.S. military preeminence?*

While the U.S. military has devoted significant time to the definition of vital capabilities in alignment with Joint Vision 2020, the committee made no effort in this first report to synchronize its derivations or definitions, or to provide a complete decomposition of the operational concepts and enablers into their underlying capabilities. Rather, committee members selected a few evolving technologies and assessed the potential for those technologies to threaten important U.S. capabilities. Given that the committee's proposed basic methodology is adopted, future studies will analyze more comprehensively the threats to a taxonomy of U.S. military capabilities that derives from the operational concepts envisioned by Joint Vision 2020. The basic methodology developed by the committee is summarized in Box 2-2 and is described in greater detail in subsequent sections.

IDENTIFY

The next step of the proposed assessment methodology is performed from the RED perspective. The central question here is as follows: *What are the evolving technologies that, in the hands of U.S. adversaries, might be used to threaten an important U.S. military capability?* A corollary question is, What technologies, if rapidly exploited by the U.S. military, are likely to yield sustained technological superiority? However, this issue was addressed only peripherally, given the division's focus on technology warning.

Having identified a technology of potential interest, the next challenge becomes the derivation of "indicators" or "observables" that may suggest adversarial adoption or exploitation of that technology.

BOX 2-1
Relevant Definitions from Joint Vision 2020 Serving as Foundation for Assessment Methodology

Information Superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority is achieved in a noncombat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives.

Dominant Maneuver is the ability of joint forces to gain positional advantage with decisive speed and overwhelming operational tempo in the achievement of assigned military tasks. Widely dispersed joint air, land, sea, amphibious, special operations and space forces, capable of scaling and massing force or forces and the effects of fires as required for either combat or noncombat operations, will secure advantage across the range of military operations through the application of information, deception, engagement, mobility and counter-mobility capabilities.

Focused Logistics is the ability to provide the joint force the right personnel, equipment, and supplies in the right place, at the right time, and in the right quantity, across the full range of military operations. This will be made possible through a real-time, web-based information system providing total asset visibility as part of a common relevant operational picture, effectively linking the operator and logistician across Services and support agencies.

Precision Engagement is the ability of joint forces to locate, surveil, discern, and track objectives or targets; select, organize, and use the correct systems; generate desired effects; assess results; and reengage with decisive speed and overwhelming operational tempo as required, throughout the full range of military operations.

Full Dimensional Protection is the ability of the joint force to protect its personnel and other assets required to decisively execute assigned tasks. Full dimensional protection is achieved through the tailored selection and application of multilayered active and passive measures, within the domains of air, land, sea, space, and information across the range of military operations with an acceptable level of risk.

SOURCE: JCS (2000).

Although targeted intelligence-collection methods remain important, in this report the committee focuses on observables that may be derived from open source analysis—leveraging the effects of the information revolution and acknowledging that the twin forces of globalization and commercialization provide new sources of relevant information. At the same time, however, the committee recognizes the difficulty of discerning when technological advances portend emerging threats rather than societal benefits.

A sample chart—Chart 2-1—exemplifies how each technology is assessed.

BOX 2-2
Proposed Methodology for Technology Warning

Foundation Joint Vision 2020[a] Operational Concepts and Information Superiority

- **Focus** *What capabilities does the United States have that, if threatened, impact U.S. military preeminence?*
- **Identify** *What are the evolving technologies that, in the hands of U.S. adversaries, might be used to threaten an important U.S. military capability?*

  What are the observables that may indicate adversarial adoption or exploitation of such technologies?
- **Assess** *Accessibility: How difficult would it be for an adversary to exploit the technology?*

  Maturity: How much is known about an adversary's intentions to exploit the technology?

  Consequence: What is the impact on U.S. military capability should the technology be employed by an adversary?
- **Prioritize** *Identify: What are the relative resources to be applied to each emerging technology to support the technology warning process?*
- **Task** *Establish and assign intelligence-information-collection requirements.*

[a]SOURCE: JCS (2000).

CHART 2-1 Example of Technology Assessment Chart

Technology		Observables
Brief description of technology		Brief description of observables.
Accessibility	**Maturity**	**Consequence**
Level 1, 2, or 3	Technology Futures Technology Watch Technology Warning Technology Alert	Short characterization.

ASSESS

The committee's assessment methodology involves characterization of a technology in terms of three variables: Accessibility, Maturity, and Consequence. Priorities for more detailed analyses may derive from any individual variable or any combination of the three.

Accessibility

The Accessibility variable focuses on the question, *How difficult would it be for an adversary to exploit the technology?* It addresses the ability of an adversary to gain access to and exploit a given technology. This assessment is divided into three levels:

- *Level 1*. The technology is available through the Internet, being a commercial off-the-shelf item; low sophistication is required to exploit it.
- *Level 2*. The technology would require a small investment (hundreds of dollars to a few hundred thousand dollars) in facilities and/or expertise.
- *Level 3*. The technology would require a major investment (millions to billions of dollars) in facilities and/or expertise.

In general, Level 1 technologies are those driven by the global commercial technology environment; they are available for exploitation by a diverse range of potential adversaries. Level 3 technologies, by contrast, are typically accessible only to state-based actors. The indicators likely to be of value in determining an adversary's actual access to a given technology vary by level as well as by the type of technology.

Maturity

The Maturity variable focuses on the question, *How much is known about an adversary's intentions to exploit the technology?* It integrates what is known about an adversary's actions, together with an evaluation of the state of play with respect to the technology of interest. At the highest level, called Technology Alert, an adversary has been identified and an operational capability has been observed. At the lowest level, Technology Futures, the potential for a technology-based threat has been identified, but no positive indicators have been observed. The Maturity assessment is divided into four categories: the first two (the lower levels) suggest further actions for the technology warning community; the other two indicate the need for immediate attention by military leadership:

- *Futures*. Create a technology roadmap and forecast; identify potential observables to aid in the tracking of technological advances.
- *Technology Watch*. Monitor (global) communications and publications for breakthroughs and integrations.
- *Technology Warning*. Positive observables indicate that a prototype has been achieved.
- *Technology Alert*. An adversary has been identified and operational capability is known to exist.

Given the potential for disruptive advances through technological breakthroughs or innovative integration, as well as the difficulty of identifying and tracking meaningful indicators, any particular technology is unlikely to progress sequentially through the various categories of Maturity listed above.

As indicated at the beginning of this chapter, the committee adopted and adapted the DIA's terminology in defining these categories. The definitions are likely to evolve as the process matures. The committee sees significant value in this basic approach, however, since it divorces the challenge of technology warning from the discrete time lines associated with "prediction," which are almost invariably inaccurate.

Consequence

Characterization of a technology in terms of the Consequence variable involves addressing the question, *What is the impact on military capability should the technology be employed by an adversary?* It involves assessing the impact of the postulated RED technology on the capability of BLUE forces. This impact can range from denial or negation of a critical capability to the less-consequential level of annoyance or nuisance. A corollary assessment may be made as to the locus of impact—that is, whether the technology affects a single person, as in the case of an assassination, or creates a circumstance of mass casualty and attendant mass chaos.

PRIORITIZE

The objective of the prioritization step of the methodology is to respond to the question, *What are the relative resources to be applied to each emerging technology to support the technology warning process?* This step is intended to harmonize the distinct nodes of observed capability, demonstrated intent, resources available, and the inherent cost of inaction. Prioritization is key to the technology warning methodology, since the Technology Warning Division lacks the resources to fully analyze every conceivable evolving technology. It is equally important to recognize that prioritization is an integral part of each methodology parameter. The prioritization of individual parameters is based on the levels of change detection and potential impact. By prioritizing the parameter, the division can focus subsequent analyses over a smaller subset of an assigned change detection domain. Priority assignment is essential to enable the focusing of more sophisticated information-gathering tools and analytic techniques on the areas of highest potential concern.

The prioritization methodology lends itself to any number of commercially available tools and techniques designed for assistance in establishing and maintaining a logical and consistent focus as well as the flexibility to react to the dynamics of technology change and country-of-interest variability. During the prioritization process, it will be important to establish measures of performance to allow critical analysis as well as change management in order to improve the overall process. The end result of the prioritization process is to provide for actionable awareness with which to influence analysis and tasking, the last of the methodology parameters.

The committee envisions that prioritization would be accomplished in close consultation with the technology warning community. It made no attempt to further develop the prioritization process in this report.

TASK

The Technology Warning Division will inevitably have unmet needs for additional information and/or intelligence relating to the prioritized list of evolving technologies. Although some needs may be met through division-chartered research, others will require the assistance of the broader intelligence community.

The task step—*Establish and assign intelligence-information-collection requirements*—involves the dissemination of collection requirements to other IC components and subordinate agencies. Such requirements must provide sufficient specificity to enable interpretation by collectors who are not necessarily literate in the specific technology. The requirements may include general instructions for accomplishing the mission. It is envisioned that some of the observables postulated in the Identify step of the methodology will provide a useful basis for such tasking.

The results from collection efforts will be integrated back into the assessment step in order to refine, reprocess, and update the division's understanding of a given technology. This analysis may stimulate the issuance of a new report to the division's customers to inform them of changes in the assessed maturity of that technology.

USING THE METHODOLOGY IN THIS REPORT

To test the robustness of the proposed technology warning methodology, the committee applied it in order to assess four key areas in this initial report. It should be noted that this initial exercise was necessarily circumscribed by the domain expertise represented in the committee members and by the shortness of time for broader outreach to the technical community at large. Furthermore, since the methodology emerged in parallel with the committee's technology assessments, the approaches taken were not entirely consistent.

The foundation provided by Joint Vision 2020 and augmented by the military and professional backgrounds of committee members was used to select the following four key capabilities to assess:

- Information superiority (Chapter 3),
- Air superiority (Chapter 4),
- Discrimination between friends/foes/neutrals (Chapter 5), and
- Battle readiness and communications superiority (Chapter 6).

Chapters 3 through 6 each address the "Identify" activity with examples of evolving technologies that may threaten the capability and potential indicators that such technology development is underway. The "Assess" activity then examines opportunity and motivation for adversarial technology development and/or employment, posits change detection relative to the indicators, and assesses likely impact. Preliminary characterizations of accessibility, maturity, and consequence are provided for most evolving technologies, although the level of specificity is variable.

Subsequent steps (i.e., "Prioritize" and "Task") of the proposed methodology require customer inputs and actions and are left to future study efforts.

REFERENCE

JCS (Joint Chiefs of Staff). 2000. Joint Vision 2020. Director for Strategic Plans and Policy, J5, Strategy Division. U.S. Government Printing Office, Washington, D.C. June.

3

Challenges to Information Superiority

The importance of accurate, timely information in warfare is self-evident. The enormous advantage that superior access to such information can provide to adversaries on either side of a conflict has been recognized by warfighters for thousands of years. *The Art of War* by Sun Tzu says the following (Giles, 1910):

> All warfare is based on deception.
>
> Attack him where he is unprepared, appear where you are not expected.
>
> Fighting with a large army under your command is nowise different from fighting with a small one: it is merely a question of instituting signs and signals.
>
> The quality of decision is like the well-timed swoop of a falcon which enables it to strike and destroy its victim.
>
> Though the enemy is stronger in numbers, we may prevent him from fighting. Scheme so as to discover his plans and the likelihood of their success.
>
> Hence the experienced soldier, once in motion, is never bewildered; once he has broken camp, he is never at a loss.
>
> Hence the saying: If you know the enemy and know yourself, your victory will not stand in doubt; if you know Heaven and know Earth, you may make your victory complete.

The vision of 21st century warfighting strategy, as articulated at the highest levels of U.S. military leadership, is critically dependent on the ability of BLUE forces to obtain and rapidly act on a highly accurate, detailed, and timely picture of the battlespace, and to deny RED forces the ability to do so. In Joint Vision 2020, "Information Superiority" is identified as a key enabler that cuts across all four of the

envisioned operational concepts (JCS, 2000). That is, achieving information superiority enables BLUE forces to outmaneuver RED forces (the Dominant Maneuver operational concept); to concentrate BLUE forces quickly and accurately on selected RED targets (Precision Engagement); to react opportunistically to attack newly discovered, prospective RED targets; and to rapidly repurpose resources (Focused Logistics) to protect BLUE forces from attacks by RED forces (Full Dimensional Protection).

Conversely, if an adversary can penetrate, infiltrate, contaminate, and/or neutralize the BLUE communications systems, computing systems, and/or the information that they contain, it can inflict serious damage on the BLUE force. This damage can range up to and including the defeat of the BLUE force that otherwise would have prevailed. Furthermore, the vulnerability of the BLUE force to significant reductions in its ability to operate effectively—as a result of disruptions in its ability to communicate and access information securely and in a timely manner—increases as the BLUE force implements new or significantly modified concepts of operation that increasingly depend on information superiority.

MAINTAINING INFORMATION SUPERIORITY IN THE FACE OF GLOBALIZATION AND COMMERCIALIZATION

The information technology revolution is on par with the Industrial Revolution in terms of bringing in new and disruptive technologies that drive societal change through their ubiquity and pervasiveness. Since computing and communications go hand in hand, this confluence of technologies is often referred to as C&C.[1]

A current C&C vision would almost certainly include sensors (i.e., computing, communications, and sensors) because many existing and emerging commercial and military applications are critically dependent for their success and value on the availability of sensors that generate information needed for situational awareness. See, for example, the recent coverage in the popular press and in investment publications regarding the many applications of networked radio frequency identification (RFID) tags.

The Industrial Revolution began in the United Kingdom and Germany and gradually spread to the rest of the world. In contrast, the C&C revolution has taken root throughout vast areas of the world, and a number of the newest technologies of the 1970s, 1980s, and 1990s are commodity technologies of today. Examples that quickly come to mind are high-performance personal computers, personal digital assistants, two-way pagers, video-camera-enabled cellular telephones, virtual-reality-based multiplayer games, and high-bandwidth networking. The vast majority of these devices and systems were developed in the United States initially, under sponsorship of the Department of Defense (DOD) (largely the Defense Advanced Research Projects Agency [DARPA]). They then were sponsored through cross-agency Presidential Initiatives on High Performance Computing and Communications (now having become the National Coordination Office for Information Technology Research and Development).

It is not difficult to see that a variety of benefits resulted from the strategy of using national security "surprise prevention" priorities to seed and then nurture the C&C engine of economic productivity and growth in the late 1990s and early 21st century. The benefits include the following:

- The level of current superiority in U.S. military systems incorporating information technology,
- A very high societal return on investment (i.e., well beyond the domain of defense applications), and
- A vibrant commercial sector, which can deliver systems to the DOD as commercial off-the-shelf (COTS) products (and integrations thereof); these are much less expensive than traditional, one-

[1]See, for example, www.smartcomputing.com/editorial/dictionary/detail.asp?guid=&searchtype=1&DicID=16593&RefType=Encyclopedia. Last accessed on April 1, 2005.

of-a-kind government off-the-shelf (GOTS) systems that had previously been the norm in DOD procurements of platforms and systems.

As a result of these successes, this strategy has been studied by several foreign governments and is being emulated by the European Union nations and by Singapore, China, and other nations. Additionally, while the virtues of COTS over GOTS products are indisputable and numerous, a by-product of the "seeding and nurturing" strategy to date has been the acceleration of the commoditization of C&C technologies.

A national response to these developments to date could fall into one of two categories:

1. An added emphasis on a classification regimen to protect the newest advances in C&C and a return to a more traditional model of development favored in earlier generations of DOD procurement of platforms and systems. (It is unlikely that such a strategy would succeed in slowing down the commercial emergence significantly, if at all, of many of the enabling technologies over which the DOD might wish to keep control.)
2. A recognition that, while the constituent technologies comprising C&C have been commoditized, their integration into complex, secure, useful, usable, survivable systems that benefit the DOD can indeed be a competitive advantage if the nation maintains sufficient leadership in the relevant systems integration skills.

Other nations as well have recognized the advantages of a strong research enterprise. A number are devoting increasing fractions of their national resources to basic and early applied research in many emerging areas, while the United States is at best maintaining a steady level of funding for its research agenda (although the amount of funding is still quite large in absolute, inflation-adjusted dollars) (Roco et al., 1999; Chan et al., 2004). The end result is that the United States can be assured of neither the first and the best technology results nor a first mover's advantage in applying COTS to military systems. This situation compounds the difficulties faced by the technology warning community. That is, not being in a leadership position in creating and applying the technology makes it much harder to know what to look for and more difficult to understand the implications of the complex array of things observed.

With this background, Chapter 3 focuses on providing the beginnings of a roadmap to help the technology warning community identify, analyze, and prioritize developments in the international exploitation of C&C technologies in several key areas. These areas are trusted software; trusted hardware and foundries; supercomputing; ubiquitous sensing, computing, and communications systems; and the fusion of C&C with other novel technologies.

Trusted Software

Software today plays the role of a universal system. The key to achieving the marriage of "new- and old-economy" technologies is the development of new software-based technologies for the integration of complex systems. The competitor who is more adept at designing, implementing, and operating large, complex, software-based systems will be at a distinct advantage in 21st-century operations that are increasingly dependent on information superiority. These systems of course need to be secure and trustworthy (i.e., they need to do what is expected and only what is expected).

One often hears a somewhat-undeserved comment about the state of current software development (particularly in the context of large, software-based systems): that is, current software is just poor

enough to slow down the impressive gains made to date in computer hardware—poor enough to keep the performance improvement of systems modest. There are numerous examples of cost overruns caused by failed projects involving software-based system development (especially embedded software) in procurements. These examples include the Crusader artillery system, the Comanche helicopter, the Space-Based Infrared System-High satellite, the F/A-22 airplane, the Future Combat System, and unmanned combat aerial vehicles (the Joint Unmanned Combat Aerial System). This phenomenon is not exclusively a management problem.

Competent program managers with experience in large, software-based system development are in short supply and high demand. Their needed multidisciplinary skills are largely honed through on-the-project experience, and they are subject to the natural selection processes of a competitive business environment. They cannot be easily "cloned" through educational programs.

With the growth of large software-development centers in India, Israel, and Eastern Europe, the technology warning community should be carefully tracking the work on techniques for the development of trusted software systems, especially trusted embedded software systems. New techniques for the metamodeling of embedded systems, aspect-based programming, and model-based integration of embedded systems should be closely monitored.

A related point is the need for new methods for the development of trusted software for civilian infrastructures. The huge market created by the expanding use of wireless embedded systems in physical infrastructures, and the associated commercial requirements for the trustworthiness of those systems, afford the possibility of generating a cyber infrastructure that is secure and trusted—and available worldwide to allies and adversaries alike.

Trusted Hardware and Foundries

BLUE force technological superiority relies on the development and manufacturing of trusted and, it is hoped, tamperproof hardware components. Therefore, it is important to pay attention to trends in semiconductor manufacturing to determine the relative maturity and directions of U.S. and foreign semiconductor fabrication facilities. To date, the United States remains the world leader in processor fabrication and in the production of application-specific integrated circuits (ASICs). However, emerging foundries in South Korea, Taiwan, and China are poised to take a leading market share in semiconductors.

Additionally, technology trends point to the emergence of a number of interesting new nano-technologies and materials that will be used alongside complementary metal-oxide semiconductor (CMOS) technologies and methods. While CMOS is the dominant electronics technology of today, alternatives—nanotubes (e.g., carbon and silicon), molecular electronics, quantum dots, and others—are rapidly being developed. Eventually they are likely to complement and perhaps even supplant CMOS as the electronics benchmark. It will be important to monitor, with a worldwide perspective, the development of these electronics technologies (DSB, 2005).

Supercomputing

The greatest supercomputing threat today does not come from fourth-generation computers but rather from the use of grid computing involving the concept of "networks of workstations" to connect commodity personal computers (PCs).[2] Such grid computing is already being used by the Search for

[2]See, for example, http://www.eecs.berkeley.edu/ and http://webs.cs.berkeley.edu. Last accessed on April 26, 2005.

Extraterrestrial Intelligence (SETI) Institute to conduct signal analysis of multiband extraterrestrial signals, by astronomers for basic exploration of cosmic background radiation, and for climate modeling. Superiority in this area is achieved through advanced models for distributed programming and infrastructures for supporting high-performance scientific computing. High-performance scientific computing is an important dual-use technology with diverse applications, including cryptology, signal processing and climatic modeling, geological event detection, and intracellular and intercellular interaction modeling (so-called systems biology). The network of workstations is a commodity entity, but the distributed software is the key element of differentiation.

Ubiquitous Sensing, Computing, and Communications Systems

With the convergence of computing and communications technologies, there is now an emergence of sensor webs of smart dust, networks of cameras, networks of unmanned "X" vehicles (UXVs), networks of microsatellites, and other networked embedded systems. The sensing, computing, and communications hardware that goes into these systems is commodity. However, the exploitation of distributed sensor networks for applications ranging from civilian infrastructure to intelligence-gathering activities in a secure and trusted fashion is once again conditioned on the use of superior techniques for embedded software development for networked embedded systems. Thus, from a technology warning perspective, the investment in systems building for secure cyber infrastructures and other networked embedded systems is an important arena for identification, assessment, and prioritization. More detailed information on ubiquitous sensing, computing, and communications systems is provided in Appendix D in this report.

Fusion of Computing and Communications with Other Novel Technologies

C&C has been the paradigm-shifting information-technology-based engine of change over the past 30 years. All indications are that in the future it will, for many applications of great importance to the DOD, be leveraged via a fusion of C&C with biotechnologies, information technologies, and nanotechnologies in such a way that the best of the potential capabilities of nano- and biotechnologies are harvested on a C&C substrate. An example of how C&C technologies in ubiquitous sensing and communications systems can be combined with other technologies addressed in this report is the use of video-enabled disposable cellular phones in microair vehicles to provide networked monitoring and surveillance.[3] Another example is the use of C&C technologies with DNA computing methods to produce synthetic biological systems.[4]

POTENTIAL OBSERVABLES THAT MAY INDICATE EMERGING THREATS

Many of the technologies that pose potential threats to the communications capabilities of BLUE forces are readily available in the global marketplace. Thus, it is possible to postulate a variety of other observables that may be of value. Table 3-1 summarizes potential observables and potential sources of information for each. For example, the areas that foreign graduate students choose to study may be an indicator of the desire of a foreign government to develop capabilities in that area. In retrospect, it is

[3]For additional information, see, for example, http://robotics.eecs.berkeley.edu/bear/. Last accessed on April 1, 2005.
[4]See, for example, information on the Biobricks project at http://parts.mit.edu/. Last accessed on April 20, 2005.

TABLE 3-1 Potential Observables and Sources of Information on Potential Threats to Communications Capabilities

Observables	Potential Source[a]
Movement of graduate students between countries and fields	National Science Foundation Science and Engineering Indicators http://www.nsf.gov/sbe/srs/seind04/c0/c0s1.htm
	National Science Foundation Survey of Graduate Students and Postdoctorates in Science and Engineering http://www.nsf.gov/sbe/srs/sgss/
	Organisation for Economic Co-operation and Development (OECD) Education and Skills http://www.oecd.org/topic/0,2686,en_2649_33925_1_1_1_1_37455,00.html
Import and export of critical technology items (volume, type, etc.)	U.S. Government Export Portal http://www.export.gov/tradestatistics.html
Business travel to and from the United States from select countries correlated to export of certain technologies	Travel Industry Association of America http://www.tia.org/default.asp
Relevant publications and patents from select foreign countries	OECD Work on Patent Statistics http://www.oecd.org/document/10/0,2340,en_2649_34451_1901066_1_1_1_1,00.html
U.S. patents and publications	U.S. Patent and Trademark Office (Patent Statistics Available for Viewing) http://www.uspto.gov/web/offices/ac/ido/oeip/taf/index.html
Workforce migration and mobility	OECD Science and Technology Working Papers http://www.oecd.org/findDocument/0,2350,en_2649_33703_1_119684_1_1_1,00.html
Labor productivity trends	OECD Productivity Statistics http://www.oecd.org/topicstatsportal/0,2647,en_2825_30453906_1_1_1_1_1,00.html
Global diffusion of information technologies	OECD Information and Communication Technologies http://www.oecd.org/topic/0,2686,en_2649_37409_1_1_1_1_37409,00.html
Foreign industrial performance	OECD Measuring Industrial Performance http://www.oecd.org/document/15/0,2340,en_2649_34445_1895503_1_1_1_1,00.html

[a]All sites were last accessed on April 1, 2005.

clear that Middle Eastern interest in studying certain areas of engineering, particularly nuclear engineering, was an indicator of a desire to develop a nuclear capability.

Another indicator of emerging or existing capability is the return of foreign expatriates to their country of origin. In many cases their return could simply evidence a desire for wealth in a rapidly growing market and would be considered a natural by-product of the global economy. However, the return of foreign expatriates could also indicate that desired information had been obtained in the United States and could now be put to use by foreign entities.

Another indicator that should be watched is an increased interest in low-power electronics. Such interest could be indicative of developments in the areas of sensors and sensor networks. Similarly, an increased interest in low-power radio-frequency communication may be indicative of developments in sensor networks. Since much of the expertise for sensor networks is the same as that for mobile telephone networks, this behavior may also simply be a natural outgrowth of the increasingly ubiquitous telecommunications environment. The committee believes that it nonetheless bears attention.

Advances in cryptography and computer security often appear in the open literature. Increasingly, these advances are the work of foreign researchers. Recently a French researcher broke SHA (secure hash algorithm)-0 (replaced by SHA-1 in 1994), and Chinese researchers have broken message-digest algorithm 5 (MD-5) (Randall and Szydio, 2004; Wang et al., 2004). Israeli researchers have successfully attacked a 40-round version of SHA-1. SHA-1 is the foundation of many security protocols. The National Institute of Standards and Technology believes that SHA-1 remains secure, but has decided to phase it out in favor of hash functions that it believes are stronger, such as SHA-256 and SHA-512 (NIST, 2002).

It is difficult to gauge the strength of government efforts in cryptography and computer security since the results are unlikely to be published in the open literature. The analysis of such activities is likely to have to rely more on targeted intelligence collection. A possible indicator is that of hiring patterns of foreign intelligence agencies. The hiring of mathematicians and computer scientists could be a strong indicator that such agencies are developing a capability in cryptography or computer and communications security.

An indicator that is often missed is silence. During World War II, leading nuclear physicists prevailed on their colleagues and scholarly journals to refrain from publishing their results. This was interpreted correctly by the Soviets to signify that work of consequence was occurring, since it was very unlikely that the leading physicists of the day would simply stop publishing. If it was noticed that foreign researchers who had been publishing in, say, cryptography suddenly stopped or switched areas, it would be a strong indicator that increased attention should be paid to activities in that area by that government.

Areas of industrial investment can also be indicators. Anecdotal discussions indicate that Cisco now considers Huawei Technologies, based in Shenzhen, China, to be its greatest competitor. According to a recent news article (The Economist, 2005), Huawei, China's leading telecommunications equipment manufacturer, now ranks 8th among wireline-equipment suppliers, up from 18th last year (Cisco ranks first). Former People's Liberation Army (PLA) officer Ren Zengfei heads Huawei Technologies. Huawei is of particular interest because approximately 40 percent of its employees are in research and development, which contrasts sharply with current commercial practice in the United States.[5]

Earlier in this chapter it was observed that silence may also be a useful observable. With that idea in mind, some of the areas identified in Table 3-1 (e.g., publications and patents) should be monitored for abrupt pattern changes. A cautionary note with respect to the observables postulated above is that the committee made no assessment regarding policy or other issues that may limit such analysis. Furthermore, the committee acknowledges that many of the observables that it identified may be routinely analyzed by the technology warning community.

BASIC WAYS TO DEGRADE OR NEUTRALIZE INFORMATION SUPERIORITY

An adversary could impact BLUE force information superiority in a number of ways, including exploitation, corruption, disruption, or destruction of U.S. information systems. Virtually any component

[5]See, for example, http://company.monster.com/huaweihk/. Last accessed on February 11, 2005.

of the information environment is a potential target—that is, the aggregate of individuals, organizations, and systems that collect, process, and disseminate information, including the information itself (JCS, 2000). In this section, the committee provides a "tutorial-level" overview of several of the more commonly used methods of attack.

Exploitation

If an adversary gains access to protected information, the system has been exploited. Intercepting battle plans and moving assets out of harm's way are perhaps the most classic examples of battlefield information exploitation. Most commonly, exploitation is associated with voice or data transmission among forces or between forces and command authorities. In the modern battle environment, however, other information can be exploited. Intercepting the communications between a sensor and the next point in the communications stream, or between a weapon and its launch platform, are examples of modern exploitation. Intercepting a wireless or wired signal, "bugging" a node or facility in the system, or emplacing a human agent are all methods of information exploitation.

Encryption is perhaps the most effective way to prevent the loss of information through signal interception. "Bugging" may be prevented (or detected) by the application of suitable scanning technology, but doing so may be expensive and tedious. The "spy," especially an insider threat, may be the most difficult to counter. History is replete with stories from classical times to the present of spies upsetting even the best-laid battle plans.

Corruption

If an adversary gains access to the information environment and is able to alter information, that information has been corrupted. Means of corrupting information are many—ranging from "spoofing," which means changing the content of information collected and transmitted, to deception, which is simply creating bad information. Being able to flip 1's and 0's in a data stream so that a weapon hits a wrong target is an example of spoofing. Passing on false information so that a wrong target is attacked constitutes deception.

The level of maturity of technology required to spoof electronic information is relatively advanced, probably beyond the inherent capability of an insurgent but well within the capability of a state actor. However, insurgents with sufficient money could buy the technology and the capability to use it on the black market or from some less-than-scrupulous state actors. One must have the means to intercept, alter, and then retransmit information, or one must be able to compromise a sensor or to compromise data-processing or data-transmitting hardware. Deception, especially involving human sources, is notoriously easy.

Using encryption to ensure the integrity of data that are transmitted is a well-known technique that should be implemented. It is extremely difficult for even a peer adversary to alter the contents of an encrypted data stream in an undetectable fashion. It is much easier to alter the data at the source before it is encrypted (e.g., altering the values returned by a sensor).

Disruption

Preventing the movement of information constitutes a disruption. The jamming of a signal, either wired or wireless, is an example; the flooding of communications channels with extraneous messages could also disrupt the movement of useful information; cutting a communications link is another

example. The destruction of a single node on a system may disrupt the functioning of the system, although it would not destroy the system itself. For example, blowing up a communications tower or shooting down an unmanned aerial vehicle (UAV) could be disruptive of the entire system without destroying it.

State actors, whether through indigenous or purchased capability, are the adversaries most likely to acquire weapons to jam U.S. systems. In the early days of Operation Iraqi Freedom, Iraq attempted to use purchased Global Positioning System (GPS) jammers to interfere with GPS precision-guided munitions of the United States (Trimble, 2003).

Destruction

Taking down an entire information system for an extended period of time effectively constitutes the destruction of that system. The most extreme example would be through the use of an electro-magnetic pulse (EMP) system (Foster et al., 2004). Potential adversaries have no doubt watched U.S. methodology in Iraq and elsewhere and realize that such a strike might gravely damage this nation's ability to wage warfare.

Only a major state actor would be capable of such a strike today over an entire theater. However, lesser state actors and insurgents might, with a lucky hit, be able to destroy a major command center and significantly interfere with the U.S. ability to conduct operations. One major threat from a nuclear-capable, lesser state actor would be to detonate a weapon at high altitude; the resulting EMP might well destroy the electronics in ground assets as well as nearby space assets. If the attacker were so fortunate as to "pump" the Van Allen belts, the number of space assets at risk would rise dramatically (Foster et al., 2004).

Analogies in Non-Warfighting Scenarios

The BLUE force's increasing dependence on information superiority has related analogies in non-warfighting scenarios. New and emerging information technologies and their associated applications are recognized as being the engine of productivity growth in developed countries. Conversely, the disruption of widely used services and applications that employ information technologies can have widespread and major consequences. For example, disrupting the capabilities of average U.S. citizens to send and receive e-mail, to make and receive cellular telephone calls, and/or to access Web sites causes a major disruption in their abilities to do their jobs effectively and to conduct their personal business effectively. This is the case today even though e-mail, cellular telephones, and the World Wide Web were not used by average citizens only 15 years ago. Businesses and individuals will become increasingly dependent on applications of information technology that employ sensors (GPS receivers, RFID tags, and so on). Given that dependence, even perceived disruption (e.g., spoofing) could diminish users' confidence in the underlying information networks and, in effect, degrade the services that the networks would otherwise deliver.

COMMITTEE FOCUS: COMMUNICATIONS AND SENSING SYSTEMS

Joint Vision 2020 acknowledges the transitory nature of information superiority as well as the fact that it alone does not guarantee victory (JCS, 2000). Rather, information superiority serves as an essential enabler for the operational concepts. In general terms, a distributed BLUE force needs the following:

- To know where it is (information about the locations of relevant BLUE forces);
- To know where the adversary is (information about the locations of relevant RED forces and RED systems, which will often be obtained from distributed, networked BLUE sensors);
- To decide where it wants to be at specific times in the future;
- To know how to safely get where it wants to be (using networked BLUE sensors to detect threats);
- To know what to do when it gets there;
- To respond to emerging opportunities and threats (which will often be detected by networked BLUE sensors); and
- To be able to do so more quickly and more effectively than the adversary.

The ability to communicate over distance with low latency relies on superb communications and rapid, controlled accessibility to relevant information, which are core capabilities of any modern fighting force (MITRE, 2004). Such capabilities become increasingly important as the military moves toward implementation of the operational concepts articulated in Joint Vision 2020. The recognition of the importance of these capabilities has led to programs such as the Joint Tactical Radio System, which seeks to rationalize the disparate communications systems of the armed forces under a standard, interoperable architecture. The importance of such efforts is underscored in programs such as the Future Combat System, which relies on excellent communications and the superb (but controlled) accessibility of relevant information in order to achieve unprecedented situational awareness, coordination, and reaction times. If the abilities of the soldiers and other systems to communicate reliably and/or to access dependable information are substantially disrupted, the effectiveness of the forces that rely on information superiority to accomplish their missions will be substantially reduced.

Potential Pathways for Disruption, Denial, or Degradation of Communications and Sensing Capabilities

As a result of the highly distributed nature of communications systems, the interdependencies inherent to network architectures, and the fact that BLUE forces increasingly rely on commercially available technologies, innumerable vulnerabilities exist (many of them are well documented in open literature). Below, the committee summarizes some potential pathways that could impact the nation's ability to maintain information superiority. These pathways include the following:

- Causing physical damage to wireless handheld appliances and using embedded wireless subsystems to destroy or degrade the ability of BLUE forces to communicate (e.g., using EMP generators to destroy electronic components or to cause significant changes in stored data);
- Jamming of communications capabilities (e.g., using strong radio signals to overload the wireless receivers in wireless systems and subsystems);
- Performing a denial-of-service attack on communications capabilities by overloading networks with bogus communications (e.g., injecting packets into a network to cause congestion, preventing BLUE force packets from reaching their destinations);
- Performing a denial-of-service attack by revoking the access privileges of legitimate users and systems (e.g., by attacking the authentication databases, making it impossible for legitimate soldiers to authenticate themselves to systems that they wish to access);
- Disrupting network servers so the information that they contain is not accessible to legitimate users of those servers (e.g., by overloading the servers with bogus requests for information, as in a distributed denial-of-service attack on a commercial Web server);

- Accessing information that should not be available to the party accessing it (e.g., using a spy with access privileges to obtain information—a form of "insider" attack);
- Breaking cryptographic systems to read encrypted messages in transit, to read encrypted stored files, or to obtain passwords and cryptographic keys;
- Spoofing sensors—that is, causing false readings, resulting in misinformation that causes the BLUE forces to misinterpret situations in which accurate situational information is critical (e.g., causing a sensor to mistakenly identify noncombatants as RED forces);
- Evading sensor detection (stealth) by employing technologies that mask the physical attributes that are being sensed (e.g., clothing that employs a combination of insulation and surface cooling to evade detection by infrared sensors); and
- Jamming sensors—that is, employing "signals" that overload sensors and/or prevent sensors from discriminating between "noise" and signals of significance (e.g., attempting to overload or damage acoustic sensors with inexpensive, high-power acoustic noise generators).

IDENTIFICATION AND ASSESSMENT STEPS OF THE COMMITTEE METHODOLOGY

A variety of technologies and tactics may be employed to degrade the information superiority of BLUE forces. Several techniques were discussed in the previous section. Here the committee identifies a few specific technologies and postulates observables that may suggest adversarial intent to develop such capabilities. Two broad categories are considered: system/network attacks and sensor attacks.

System/Network Attacks

Electromagnetic Pulse Generators

The combination of a sufficiently high energy electromagnetic pulse (EMP) generator with a suitable antenna could be used by an adversary to achieve a disruptive capability (see Charts 3-1 and 3-2).

CHART 3-1 Technology Assessment: Electromagnetic Pulse Generators

Technology	Observables	
Electromagnetic Pulse (EMP) Generators: Non-nuclear, transportable generators of electromagnetic pulses that are sufficiently powerful (and rich in high-frequency content) to be used to damage electronic components or to induce data changes in electronic memories within BLUE force handheld appliances and/or embedded systems.	Research and development activities related to high-energy EMP generators (which have no apparent commercial purpose, other than for testing equipment for EMP vulnerability or, perhaps, for certain types of precision welding processes).	
Accessibility	**Maturity**	**Consequence**
Level 2	Watch	Destroy electronic components or degrade stored data.

Radio-Frequency Jammers

Low-cost radio-frequency jammers may be procured commercially or assembled from commercially available subsystems and components (see Chart 3-3).

Modular Network Nodes

The basic capability of modular network nodes can be readily obtained by using commercially available local area networking products, perhaps with some modifications of the associated software plus the associated capability to obtain the necessary passwords and/or encryption keys (see Chart 3-4).

CHART 3-2 Technology Assessment: Electromagnetic Pulse Generators

Technology		Observables
EMP Generators		Covert or overt research and development activities to develop adaptations of commercial off-the-shelf electronic components that operate at higher voltages, or that employ higher band-gap materials (i.e., so that the adversary can disable BLUE force equipment, without disabling RED force equipment).
Accessibility	**Maturity**	**Consequence**
Level 3	Watch	Asymmetric advantage to adversary.

CHART 3-3 Technology Assessment: Radio-Frequency Jammers

Technology		Observables
Radio-Frequency (RF) Jammers: Low-cost, transportable, high-power RF jammers employing adaptive antennas to achieve directional (pointing) capabilities that enable them to direct more of their total power on their targets.		Emerging commercial capabilities.
Accessibility	**Maturity**	**Consequence**
Level 2	Warning	Disrupt information flow.

CHART 3-4 Technology Assessment: Modular Network Nodes

Technology		Observables
Modular network nodes: Low-cost, small nodes (modules) that can generate bogus traffic that can be used to overload networks (once the necessary network access passwords and/or encryption keys have been obtained).		Emerging commercial products used in wireless local area networking applications.
Accessibility	**Maturity**	**Consequence**
Level 1 for basic capability; difficulty is in gaining access.	Watch	Disruption of communications.

Malicious Code

Small groups of talented computer scientists can produce potent malicious code. The insertion of undetectable malicious code into well-protected military systems may require access to the systems by persons with system administration privileges. However, this could also be accomplished by adversaries employed by software-development organizations that develop the software used by BLUE forces. The activation of the malicious code by an adversary during an actual operation would probably require the adversary to employ BLUE force insiders with sufficient access privileges (see Chart 3-5).

Sensor Attacks

Sensor attacks can generally be classified into jamming (overloading the sensory input to degrade the sensor system either temporarily or permanently), signature reduction (camouflage), and spoofing (injecting false signals into the sensor stream either at the sensor or at the network or computation or communication level). While any of these tactics can be effective in specific instances, there is a general hierarchy of impact. While jamming can deny the BLUE forces the use of their sensors, it leaves no doubt that the RED forces are making an assault on the sensor suite, and tracing the source of the jamming leaves RED forces vulnerable to counterattack. Signature-reduction strategies degrade situational awareness without providing an obvious indication of enemy presence or providing any directions for response. Spoofing can degrade BLUE force capabilities by diverting resources into unproductive directions.

BLUE forces exploit a diverse and expanding spectrum of sensor modalities, as illustrated in Table 3-2. Additional related information is provided in Appendix D in this report. It should be noted, however, that the information in this report is not comprehensive in terms of either modalities or their potential applications.

CHART 3-5 Technology Assessment: Malicious Code

Technology	Observables
Malicious code (e.g., executable software hidden within an application loaded onto a BLUE system) that lies dormant and can be activated by a trigger that is injected by the actions of an insider. The activation of this malicious code causes essential servers and essential communications networking assets (e.g., routers) to become unusable or to perform incorrectly.	Covert projects employing computer scientists to develop undetectable malicious code, and the associated methods for inserting it into BLUE systems; virus, worm, etc., attacks, conducted as experiments to test different types of malicious code (e.g., how long does it take to be detected? How fast does it spread among the target systems in a network of systems?); persons employed by adversaries, with computer system expertise who have infiltrated BLUE organizations and attempted to gain significant access privileges via job assignments.

Accessibility	Maturity	Consequence
Level 1 for basic capability; difficulty is in gaining access.	Watch	Could enable exploitation, corruption, or disruption of information environment.

TABLE 3-2 Examples of Sensor Modalities and Their Potential Utility

Sensor Modality	Illustrative Applications
Terahertz sensors	Potential ability to see through walls and under clothes.
Infrared spectrum	Enabling operations in dark and nighttime environments.
Visual spectrum	Optical imaging.
Acoustic and seismic sensors	Identification of certain classes of targets and target bearing.
Image/spectroscopy	Spatial/spectral resolution of a target.
Chemical sensors	Detection of presence of chemical agents (e.g. nerve agents).
Ionizing radiation	Detection of presence of radiological/nuclear materials.

NOTE: See Appendix D in this report for additional information on sensor modalities.

Sensor attacks are typically targeted to specific sensor modalities. Here the committee has not provided a complete assessment, instead discussing only general approaches that may threaten BLUE sensor suites, together with potential observables. A discussion of a few specific technologies is provided in subsequent chapters (e.g., see the subsection entitled "Sensor Spoofing" in Chapter 5).

Jamming

In general, sensors are designed to detect weak signals and to filter out extraneous signals without degrading the signals of interest. In most cases, radio-frequency (RF), terahertz (THz), infrared (IR) radiation, optical, ultraviolet (UV), acoustic, chemical, and biological detectors can be readily overwhelmed by the deliberate introduction of large levels of artificial signals into the theater of operations. Undoubtedly the best defense is redundancy—of sensors and of sensing modalities. Reliance on a single sensor of a single observable is an inherently risky strategy that allows an adversary to exploit a single set of vulnerabilities. Hardening of single sensors is usually expensive and most often degrades the sensitivity and/or selectivity of the sensor. Distribution of wide-area networked sensors operating across a range of modalities provides an inherent immunity (see Chart 3-6).

CHART 3-6 Capability Identification: Sensor Jamming

Capability	Potential Observables
Sensor jamming	In some cases, such as infrared countermeasures for heat-seeking missiles, there are national programs to develop appropriate sources and packaging. Clearly, these need to be monitored. More difficult to detect are strategies that employ low-technology sources, e.g., acoustic generators, to confuse appropriate sensors. On the state level, both the jamming sources and the hardening of each state's own sensor suite provide potential observables.

Camouflage

Signature reduction is a time-honored military tradition. One specific area of great importance is the reduction of infrared signatures—attempting to reduce the benefit of IR sensors to BLUE forces. There is a long history of signal manipulation and reduction by using advanced coatings (e.g., stealth), improved thermal isolation, and so on. Recently, there has been much activity reported in the open scientific literature in the related fields of photonic crystals, plasmonics, and metamaterials. While the goals are many and span the range from fundamental optical interactions with matter, to improved telecommunications and signal processing systems, to quasi-optical interconnects in next-generation integrated circuits, all of these areas have a potential impact on infrared signatures and sensing (see Chart 3-7).

Spoofing

There are as many possible targets for the use of spoofing as there are sensors. One category of increasing importance is chemical and biological sensors. Ground forces are significantly hampered by protective gear to defend them against these threats. Thus, RED forces gain significant leverage if BLUE forces must defend against a threat that does not exist while RED forces can operate unencumbered (see Chart 3-8).

SUMMARY

In Joint Vision 2020, Information Superiority is identified as a key enabler that cuts across all four of the envisioned operational concepts (JCS, 2000). In the future, the United States can be assured neither of being the first to have access to all of the best information technologies nor of having a first mover's advantage in applying COTS products to military systems. As a result, it is much harder to know what to look for and much more difficult to recognize the implications of the complex array of achievements in information technology and undertakings in development and applications that will be possible to observe.

The committee identified a number of generic vulnerabilities of information-technology-enabled systems and applications (including, in principle, those that might be used by BLUE forces to endeavor to maintain information superiority). These vulnerabilities could be attacked via emerging technologies and capabilities that, in most cases, are increasingly available to U.S. adversaries in the form of low-cost, commercial commodity products. The emerging technologies and capabilities that might attack these vulnerabilities include (but are not limited to) the following:

- Causing physical damage to wireless handheld appliances and embedded wireless subsystems;
- Jamming of communications capabilities;
- Performing a denial-of-service attack on communications capabilities by overloading networks with bogus communications;
- Performing a denial-of-service attack by revoking the access privileges of legitimate users and systems;
- Spoofing sensors (i.e., causing false readings that result in the dissemination of misinformation);
- Evading sensor detection (stealth) by employing technologies that mask the physical attributes that are being sensed; and
- Jamming sensors (i.e., employing "signals" that overload sensors and/or prevent sensors from discriminating between "noise" and signals of significance).

CHART 3-7 Capability Identification: Camouflage

Capability	Potential Observables
Camouflage (signature reduction)	This is an active area in the open literature, with many papers being presented at international scientific meetings and published in the archival literature. It is important to monitor this activity and to seek to apply developments to BLUE systems to better understand the capabilities of these newly emerging capabilities. The usual phenomenon of active research groups going silent is a potential indicator of state activity. Monitoring the commercial development of these technologies will be especially important because of the strong efforts in Europe and Asia-Pacific.

CHART 3-8 Capability Identification: Sensor Spoofing

Capability	Potential Observables
Sensor spoofing particularly relating to chemical and biological agents.	Development of simulants for toxic agents. Testing against commercial sensors. This is again a very active area of investigation, with much of the literature open and available. Just as for low-observable research, it will be important to monitor not just research directed specifically at sensor spoofing, but more generally at improved sensors for chemical/biological agents for homeland defense, and for commercial as well as military applications.

The committee also identified for each of the emerging technologies or capabilities listed above, potential indicators that the technology warning community could employ to attempt to determine the actual intentions and/or capabilities of U.S. adversaries to employ these technologies and methodologies.

REFERENCES

Chan, Felix, Dora Marinova, and Michael McAleer. 2004. Trends and volatilities in foreign patents registered in the USA. Applied Economics 36(6):585-592.

DSB (Defense Science Board). 2005. Task Force on High Performance Microchip Supply. Office of the Under Secretary of Defense, Washington, D.C. February. Available online at http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf. Last accessed on April 12, 2005.

The Economist. 2005. See Huawei run. March 5-11 issue. pp. 60-61.

Foster, John S., Earl Gjelde, William R. Graham, Robert J. Hermann, Henry "Hank" M. Kluepfel, Richard L. Lawson, Gordon K. Soper, Lowell L. Wood, Jr., and Joan B. Woodard. 2004. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Available online at http://www.globalsecurity.org/wmd/library/congress/2004_r/04-07-22emp.pdf. Last accessed on April 1, 2005.

Giles, Lionel, translator. 1910. Sun Tzu on the Art of War, The Oldest Military Treatise in the World. Translated from the Chinese. Available online at http://www.chinapage.com/sunzi-e.html. Last accessed on February 4, 2005.

JCS (Joint Chiefs of Staff). 2000. Joint Vision 2020. Director for Strategic Plans and Policy, J5; Strategy Division. U.S. Government Printing Office, Washington, D.C.

MITRE Corporation. 2004. Horizontal Integration: Broader Access Models for Realizing Information Dominance. MITRE Corporation, McLean, Va. Available online at http://www.fas.org/irp/agency/dod/jason/classpol.pdf. Last accessed on April 1, 2005.

NIST (National Institute of Standards and Technology). 2002. Announcing the Secure Hash Standard. Available online at http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf. Last accessed on April 1, 2005.

Randall, James, and Michael Szydio. 2004. Collisions for SHA0, MD5, HAVAL, MD4, and RIPEMD, but SHA1 Still Secure. August 31. RSA Laboratories. Available online at http://www.rsasecurity.com/rsalabs/node.asp?id=2738. Last accessed on April 1, 2005.

Roco, M.C., R.S. Williams, and P. Alivisatos, eds. 1999. Nanotechnology Research Directions, IWGN Workshop Report. September. Available online at http://www.wtec.org/loyola/nano/IWGN.Research.Directions/. Last accessed on April 1, 2005.

Trimble, Stephen. 2003. In Iraq, GPS is surviving jamming threat, Pentagon says. Aviation Week. March 25. Available online at http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/gps.xml. Last accessed on April 1, 2005.

Wang, Xiaoyun, Dengguo Feng, Xuejia Lai, and Hongbo Yu. 2004. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. Revised on August 17, 2004. Available online at http://eprint.iacr.org/2004/199.pdf. Last accessed on April 1, 2005.

4

Future Threats to U.S. Airpower in Urban Warfare

INTRODUCTION

For the past 50 years, the United States has enjoyed air dominance in all of its conflicts. No U.S. warfighter died from attack by an enemy aircraft during that time. In addition, in several recent conflicts, U.S. aircraft have been consistently able to penetrate hostile airspace, attack targets with unprecedented accuracy, and return to base with few or no losses. What technologies have led to this unprecedented success, and how much longer will the United States continue to enjoy these advantages? The answers to these questions form the basis for new research to maintain current U.S. advantages and a search for new technologies to allow it to stay a step ahead of developments elsewhere.

Several technologies have been responsible for this U.S. supremacy. The first that merits discussion is radar stealth. In the 1970s it became obvious that, through the use of special coatings and aircraft shape management, the radar cross section (RCS) of an aircraft could be reduced enormously, thereby enabling operations within hostile airspace with relative protection from gun-laying and missile-tracking radars. Aircraft such as the B-2 and the F-117 were developed employing these technologies. Their success has been spectacular.

Getting to a target undetected, however, is only half the challenge. Once there, an aircraft must identify the target and destroy it. Technologies for precision all-weather target strike were developed that reduced target-miss distance to just a few feet. Probably most important to this achievement were the invention and deployment of the Global Positioning System (GPS) for positioning and munition guidance, laser target designation, and enhanced aircraft avionics systems.

Underlying all of these aspects of U.S. air dominance is the infrastructure that supports them—an infrastructure that is difficult for others to replicate owing to the resources required. Besides the quality of the aircraft themselves and the highly trained aircrews who fly them, the primary enabler is the tanker fleet that allows long-range strike to anywhere in the world from the United States. This capability is best exemplified by the 30-hour missions flown by the B-2 in recent conflicts. Even forward-based aircraft need tanker support to reach many targets or to loiter before being called in.

While U.S. air dominance is unlikely to be jeopardized by symmetric means, particularly in the near term, technology trends in commercialization and globalization suggest that new types of threats may be

on the horizon. The United States has long since lost the lead in the manufacture of electronics (the technology of which is driven by worldwide commercial and consumer concerns rather than by aerospace, as was the case in the 1950s and 1960s). Now, the United States is also no longer dominant in the manufacture of commercial aircraft in terms of either manufacturing or technology. In addition to competition from foreign producers, U.S.-"produced" aircraft are assembled from parts largely made overseas. Even U.S.-"made" subsystems and assemblies are increasingly assembled from parts engineered and produced in areas where costs are lower, such as China, India, and the former Eastern bloc. Large U.S. aerospace and electronics companies have set up research organizations in these regions for economic reasons. This offshore sourcing is having the effect of building up research, development, and manufacturing capability in other countries in aerospace and related fields.

One pillar of U.S. airpower in the past has been the capabilities of its major platforms. These sophisticated platforms now require investments of tens of billions of dollars spread over decades, investment levels that few foes can match. However, the life of the advanced technology in these platforms can now be less than the development cycle. Small unmanned aerial vehicles (UAVs) offer a counter to large platforms—while much less capable than the large platforms at present, they can have much shorter and less costly development cycles. These factors contribute to the proliferation of such vehicles around the world, especially at the smaller sizes (Munson, 1996).

The new technologies delineated above combined with the globalization of the aerospace and electronics businesses imply that current U.S. aerospace supremacy will face new classes of challenges from new adversaries—a few of which are described below.

Obviously, negating radar stealth must be high on the list of technologies for RED forces to pursue. The antidote to this nation's stealth advantage takes two forms—direct and indirect. To negate U.S. radar stealth advantages directly requires the development of radars with different and improved characteristics. For example, the power of the radar can be increased to illuminate even small RCS targets. Changes in frequencies and radar-emanation management can also help. On an indirect basis, other sensors could be perfected that can precisely track aircraft, such as improved infrared (IR) or optical sensors. All of these require a high degree of sophistication to invent, but they can be sold to and used by relatively unsophisticated buyers with hostile intentions.

The difficulty of GPS interference has been the subject of great conjecture. Suffice to say that RED forces could profit enormously if the system could be shut down or biased in such a way as to interfere with weapons accuracy.

Other ways to interfere with or reduce the advantages of U.S. airpower include the use of electromagnetic pulse (EMP) radiation to shut down onboard targeting systems, the spoofing of targeting systems, the burying or hardening of high-value targets, population shielding (urban targets), the use of laser absorption material, and many more.

The scope of this report does not allow delving into all of these possibilities. Thus, to make the task manageable, the complex challenge of successfully attacking urban targets is discussed as an example of one mission scenario. This scenario was selected in part because the committee believes that it represents a current as well as an enduring challenge, with particular relevance to the global war on terrorism.

AIRPOWER IN URBAN WARFARE

In general, the current use of U.S. airpower in urban warfare can be grouped into the following four broad categories that underpin the operational concepts delineated in Joint Vision 2020 (the concepts are Dominant Maneuver, Precision Engagement, Focused Logistics, and Full Dimensional Protection) (JCS, 2000):

- Intelligence, surveillance, and reconnaissance (ISR);
- Transport of personnel and material;
- Strike (the destruction of pre-identified targets); and
- Close air support (strike in close cooperation with and in support of troops on the ground).

The urban environment is the arena in which U.S. airpower is currently the least effective and decisive. Masking from urban clutter can be severe, greatly reducing the field of view and utility of most airborne sensor systems. Transport is restricted to rotary-wing or vertical-takeoff-and-landing (VTOL) aircraft, since landing areas are small and such vehicles are under severe threat at low altitude from small arms, rocket-propelled grenades (RPGs), and so on. Strike and close air support with precision munitions can be effective when ground troops identify targets, but the effects of current weapons can be on a larger scale than is desirable (e.g., destruction of buildings rather than rooms) and differ little from those of precision artillery.

Historically, ISR, transport, strike, and close air support have been executed by manned, fixed-wing and rotary aircraft, to and from which information flows through other aircraft or space assets (which are not discussed further in this chapter). The definition and nature of airpower are changing, however. Within the past decade, UAVs such as the Global Hawk and Predator have taken over some ISR missions. UAV strike missions that have been demonstrated in combat with existing aircraft and experimental unmanned combat air vehicles (UCAVs) designed specifically for strike are now flying (the X-45 and X-47). While unmanned, these UAVs of the U.S. Air Force and U.S. Navy, respectively, are as large as manned aircraft. As part of its Future Combat System (FCS), the U.S. Army plans to adopt relatively large, automated, fixed- and rotary-wing vehicles as well (Gabbert, 2004). However, the U.S. Army and U.S. Marine Corps also plan to field much smaller aerial vehicles—down to a few inches in wingspan—which can be carried and deployed by individual soldiers (Tousley, 2004). Indeed, a motivation for these so-called micro air vehicles (MAVs) is urban warfare, in which bird- or even insect-sized vehicles could be of use for surveillance and reconnaissance in the cluttered urban environment, even within buildings.

The committee believes that the ability of RED forces to field large forces of MAVs developed with commercial off-the-shelf (COTS) products represents a significant threat to U.S. air dominance—particularly in the area of surveillance and reconnaissance in urban environments. Given trends in the global commercial marketplace, future adversaries will have low-cost options that could negate the advantage held by today's BLUE forces.

Assessments of future threats to U.S. airpower must take into consideration the full range of future airpower—including U.S. and adversary air assets ranging from large, manned platforms at medium and high altitudes, to low-flying rotary aircraft, to MAVs flying among and inside buildings. In the following sections, the committee discusses some challenges to U.S. airpower, describing the high-level characteristics of RED systems that could constrain or defeat this power and technology developments that may enable such systems.

CHALLENGES TO U.S. AIRPOWER

A major objective of U.S. airpower is to enable access to the battlefield for U.S. ground, sea, and air forces while denying that access to an adversary. Such access forms a foundation upon which U.S. military plans are constructed and has been achieved with little serious challenge for the past five decades. The advantages of this access are readily apparent to the world's military organizations, and antiaccess strategies and tactics are a major focus of military planners. Evolving and disruptive tech-

nologies, used with innovative tactics, may offer the potential to challenge and disrupt U.S. airpower as currently envisioned.

An adversary can potentially challenge, reduce, or even negate the impact of U.S. airpower in many ways. These approaches can be characterized as either offensive or defensive:

- Offensive
  - —Threaten, disable, or destroy aircraft (manned or unmanned);
  - —Disrupt targeting (jam GPS, compromise "identification friend-or-foe" [IFF], regulate proximity of restricted facilities); and
  - —Disrupt information flow (jam communications, disrupt asset management within network-centric operations, disrupt sensors, and so on).

- Defensive
  - —Disperse forces geographically, and
  - —Hide (camouflage, spoof, bury or harden structures, disrupt sensors).

Offensive Techniques That May Be Employed by an Adversary

Threatening, damaging, or destroying aircraft are obviously effective techniques for constraining U.S. airpower. These can be manifested as traditional air-to-air threats (fighters and air-to-air missiles), traditional surface-to-air threats (guns and ground-to-air missiles), and high-technology worries yet to be seen on the battlefield (such as electromagnetic pulse [EMP] weapons, lasers, stealth aircraft detection, and chemical and biological threats to the aircraft). While to an adversary, threatening a U.S. aircraft may not be as satisfying as destroying it, a threat can be effective in denying the access that U.S. forces need. The results of such threats may be (1) to force vulnerable U.S. assets (such as tankers or ISR aircraft) back from the battlefront, (2) to force attack aircraft up to altitudes at which they are less effective, (3) to funnel aircraft into specific corridors, (4) to constrain or prevent aerial resupply, and (5) to constrain the types of aircraft that the United States is willing to employ to those of which it has very few (such as stealthy and electronic countermeasures [ECM] aircraft). These outcomes can all serve to reduce the effectiveness of U.S. airpower to a significant degree, given an imposing threat.

Another technique for countering U.S. airpower is to disrupt targeting (deny Precision Engagement). In this case, while the United States has located a target, the opponent has taken action to reduce the ability or willingness of the United States to destroy it. Increasingly, facilities are deeply buried to reduce their vulnerability to conventional weapons (this also makes them more difficult to locate or identify precisely). A related approach is to position a facility so that geographic masking combined with the kinematics of missile and bomb dynamics frustrates weapons trajectories. The previous two cases are examples of reducing the U.S. ability to destroy a target.

Often as effective, and much cheaper than reducing the *ability* of the United States to destroy a target, is positioning a target so as to reduce U.S. *willingness* to destroy it. This includes target placement within, under, or near such civilian structures as schools, hospitals, marketplaces, and houses of worship (an approach well suited to urban environments). These are passive, low-technology approaches to frustrating U.S. targeting. Active approaches are possible as well. They might include foiling of the systems that the United States uses to identify its forces on the battlefield (so-called IFF and BLUE force tracking technologies). Compromising or spoofing these systems can permit a foe to masquerade as U.S. forces or to introduce uncertainty and fear of friendly fire. Even more active techniques involve the jamming of precision-guided weapons GPS and electro-optical navigation guidance systems. Such

active techniques require sophisticated knowledge of precision-guided weapons technologies, can be sensitive to counter-countermeasures, and so are of most value when used with tactical surprise.

Defensive Techniques That May Be Employed by an Adversary

Airpower is most effective when the adversary masses its forces. Historically, it is least effective when the enemy disperses. Operation Strangle in World War II (again in Korea) and Rolling Thunder in Vietnam are historical examples in which interdiction has been shown to be ineffective when the enemy disperses its forces. Likewise, during the air war over Serbia, when the Serbs dispersed their tanks and did not move them, U.S. airpower was relatively ineffective against their armor. Many will argue that tank killing was not a primary mission, but in fact an enemy dispersed creates a situation that reduces airpower's effectiveness. Similarly, in the current operations in Iraq, the ability of the enemy to remain dispersed, but to be able to mass in time and at a place to achieve limited tactical advantage has proven to be a unique challenge for the U.S. military, despite tactical superiority.

If this historical trend continues, there is every reason to assume that future adversaries will migrate away from force-on-force situations whenever possible, because whenever they mass, they become vulnerable. The unique challenge for airpower in the future is to become effective against an adversary that disperses, in order to be able to provide the intelligence regarding enemy positions and intent before the enemy masses at the tactical level. For the future enemy, the challenge will be to acquire technologies that allow it to remain hidden, communicate at will with dispersed forces, then form at the time and place of its choosing.

While dispersion is a tactic as old as warfare, advanced technology can enhance an adversary's capability to disperse, remain hidden, and coalesce when the time is right. Technologies that aid dispersion include the following:

- *Secure communications*. Secure communications, especially low-cost military or commercial implementations, enable rapid force dispersal and constitution. There are many aspects to communications security, including security of the waveform (spread spectrum, temporal compression, and so on), security of the information (encryption), and security of fixed infrastructure. As commercial and consumer users become more concerned with communications security, commercially available strong encryption and the incorporation of such encryption into low-cost cellular phones, walkie-talkies, and personal digital assistants will enhance an adversary's dispersal capabilities.
- *Low-cost, portable stealth technologies*. These technologies would enhance a dispersed foe's ability to hide assets such as vehicles. Specifically, the development of lightweight, flexible multispectral (light/radio frequency [RF]) "camouflage netting" would reduce the effectiveness of many advanced U.S. airborne and spaceborne sensors.
- *Advanced, low-cost multispectral decoys*. These decoys would reduce the effectiveness of many advanced U.S. airborne and spaceborne sensors, require the expenditure of additional (and perhaps expensive) munitions, and mislead the United States as to the effectiveness of its activities.

Traditional air superiority combined with precision munitions (Precision Engagement) has given the United States the capability to destroy almost any target that it can locate. Thus, hiding from U.S. forces is an attractive counter for adversaries to use. Hiding can take many forms, such as traditional camouflage (netting, hiding under foliage, and so on), burying or submerging targets, or actively disrupting sensors (RF or optical jamming). Notwithstanding its sophisticated sensors, the United States has yet to demonstrate on the battlefield that hard problems such as tanks under trees and decoy discrimination

have been solved. Nevertheless, as the sophistication of U.S. sensors increases, so must the art of hiding: camouflage must be multispectral; burying must account for infrared (IR) perturbations; and acoustic, magnetic, and electromagnetic signatures must be reduced.

COMMITTEE FOCUS: SYSTEMS THAT CAN DEGRADE U.S. AIRPOWER

The system-level performance criteria of a new technology determine how and to what degree it can challenge U.S. airpower. These system-level parameters can then be devolved into specific engineering requirements that new technologies must meet in order to be effective. Clearly, this can be a very large set. Here the committee chooses to list a few specific examples of particular relevance to urban warfare:

- Increased effectiveness of man-portable air defense systems (MANPADSs);
- User-friendly, smart weapons;
- Acoustic/RF mines;
- Shrinking of the systems listed above in size and/or cost;
- Micro systems with the effectiveness of large ones; and
- Exploitation of commonly available devices.

Two illustrative examples are presented below. The first example, involving man-portable air defense systems, illustrates the evolution of an existing threat class. The second example, involving micro air vehicles and missiles, illustrates the emergence of a new class of threats.

Man-Portable Air Defense Systems

MANPADSs are antiaircraft missiles small enough to be carried and launched by one or two people. These are currently a major threat to low-altitude aircraft. The nature of the threat ranges from short-range, low-accuracy rocket-propelled grenades to sophisticated guided weapons with cooled, multiband sensors and ranges of several kilometers. The importance of the threat stems from MANPADSs' relatively low cost (and so, ready availability and proliferation), lack of prelaunch warning cues (such as radar illumination), and the low level of training and logistics support required.

The effectiveness of a particular missile design is a strong function of the performance of its seeker and vehicle kinematics. Here, "seeker" refers to the combination of the sensor and guidance system. The seeker performance determines the target acquisition range, the aspect of the target that can be attacked, the resistance of the missile to countermeasures, and target closure accuracy. The vehicle dynamics set the missile range and maneuver performance.

Technology trends are already making such missile systems easier to support, deploy, hide, and use. Improved system characteristics such as those described below may further increase the effectiveness of MANPADSs, and thus the seriousness of their threat.

Increased Range and/or Reduced Signature

- *Increasing range*. Improving this characteristic would increase the threat footprint; threaten mid- and high-altitude aircraft, including ISR assets; and increase the slant range so that, for example, transports that stay within an airport perimeter would be at risk from remote launch sites.
- *Low-optical-emission propulsion*. Many aircraft missile countermeasure systems use the optical emission from the missile launch to queue the defense. Thus, no signature, no warning, no

defense. Extending the definition of reduced optical emission to include smoke helps to mask the launch location and thus increase the tactical utility of the missile.

Enhanced Guidance, Navigation, and/or Targeting

- *Multimode seekers*. This improved technology would reduce or eliminate the effectiveness of countermeasures or permit non-line-of-sight launches. In addition to multiple optical bands (an approach currently popular), this might include acoustic or RF cues to allow a missile launch against a target not in sight from the launch position. With sufficient range and RF seeker performance, large radar and battle management aircraft can be placed under threat.
- *Increased accuracy guidance*. The warhead size of a man-portable missile is of the order of a kilogram. Thus, it must detonate very close to a critical location to be effective. Increased guidance accuracy, along with any necessary increase in maneuverability, will improve the lethality of these small missiles, especially against large aircraft.

Enhanced Lethality

- *Autonomous launch*. With sufficiently capable sensors, automated decision making, and hardening, these small missiles can act as aerial mines, threatening any aircraft that flies within range. Remote queuing could increase the effectiveness of such systems.
- *Expanded mission capability*. By integrating relatively simple GPS guidance, laser capability for precise geolocation, and data link capability, an adversary could transform a MANPADS from a surface-to-air weapon into one that can also perform precision engagement missions in the ground-to-ground role in a wide variety of mission areas.

The interaction among the system characteristics described above is a complex topic beyond the scope of this discussion. Simply put, some of these factors are synergistic, some antagonistic, but they are all quite technologically challenging. Realizing such a system is even more challenging when cost is introduced as a prime consideration. Many weapons owe their effectiveness not to their performance or capabilities but rather to their ubiquitousness. An advanced MANPADS threat is a combination involving cost and performance.

An advanced threat with a potential impact similar to, or more serious than, that of the advanced MANPADS discussed above would be the non-nuclear electromagnetic pulse generator, as discussed in Chapter 3. The urban environment in particular is rich in opportunities to conceal such weapons.

Milli to Micro Air Vehicles and Missiles

Milli to micro air vehicles and missiles[1] are generally defined as aerospace systems massing a few kilograms or less. The confluence of microelectronics, GPS, and microelectromechanical systems (MEMS) now make it feasible to engineer very small UAVs and missiles, the capabilities of which will evolve as the enabling technologies advance. The U.S. Army and the Defense Advanced Research

[1]Micro UAVs were defined by DARPA to be less than 6 inches in any dimension, but now the Army has been using the term for 12 to 18 inch vehicles. DARPA has been trying to define "nano" as under 2 inches (insect size), despite opposition. The committee believes that practical working definitions are as follows: micro = bird sized; nano = insect sized; milli = larger than the largest bird but smaller than a Piper Cub.

Projects Agency (DARPA) have been sponsoring work on many small air vehicles, and there is considerable interest around the world on size classes down to a few inches, so-called micro UAVs (Davis et al., 1996; Grasmeyer and Keennon, 2001).

The United States anticipates using very small UAVs for reconnaissance and surveillance. In urban warfare, perch-and-stare applications are receiving attention. Of course, these capabilities are of use to a foe as well. Such capabilities may be particularly advantageous to an adversary who cannot overcome large U.S. aircraft at medium and high altitudes.

Advantages for small vehicles include very low cost, covertness, maneuverability in a complex urban environment, and freedom from extensive logistics requirements. Conceptually, these small vehicles can be armed and thus be employed as antipersonnel and anti-emitter weapons—in effect, three-dimensional mines. Vehicles at this size add a new dimension to the concept of air superiority and may be especially applicable in an urban environment.

Small vehicles need not be short-ranged. Eleven-pound aircraft powered by model-airplane engines have flown the Atlantic, navigating to a precise landfall with GPS (Wicks, 2004). Attempts are now underway by amateurs to fly the Pacific. Hundred-pound intercontinental ballistic missiles have been designed (Francis, 1999). Both aircraft and missiles of these sizes have inherently low signatures and so will be difficult to locate and track. These ranges imply that U.S. logistics and staging areas can be put at risk. The payloads of these small vehicles are concomitantly small, a few pounds, but are sufficient to represent a significant threat if carrying chemical, biological, or radiological payloads. Given sufficient precision, even conventionally armed attacks on rear areas may have more than nuisance or political value. These factors combine to create a potential RED force capability that could diminish the advantage provided by U.S. airpower. In particular, counters to these weapons may consume disproportionate U.S. resources compared to those expended by the attackers.

The micro air and space vehicles are enabled by several emerging technologies, the evolution of which will pace the vehicles' utility as weapons systems. Several examples, again grouped by the system-level capabilities enabled, are described below.

Increased Range and/or Reduced Signature

- *Quiet, efficient micro air-breathing propulsion systems*. Such systems include very small piston and gas turbine engines with fuel economy approaching that of larger engines; they range in power from a few kilowatts down to the watt level.
- *Micro bipropellant liquid rocket engines*. These engines use storable propellants with fuel economy and power density of the best large engines; their sizes range from a hundred pounds down to pounds.

Enhanced Guidance, Navigation, and/or Targeting

- *Micro guidance and navigation systems*. These systems consist of capable, chip-sized GPS receivers, MEMS gyros and accelerometers, and low-power processors.
- *Large geographic databases*. Such databases provide precise, GPS-compatible maps of large regions of the world, including habitation and economic data, for non-time-critical targeting information.
- *Micro digital storage devices to hold large databases*. These devices are sufficiently compact that large, target databases can be deployed with the micro vehicles.

- *Integrated GPS communications systems*. These systems are for timely updates keyed to geographic databases.

All of the enablers listed above exist now at various levels of performance. Their continued development and integration could yield extremely capable micro flight vehicles, well suited to mounting a low-cost challenge to aspects of U.S. air dominance, especially in an urban environment.

IDENTIFICATION AND ASSESSMENT STEPS OF COMMITTEE METHODOLOGY

The preceding discussion focuses on the system level. Here the committee considers individual technologies, which, if realized and integrated into a system, can result in significant challenges to U.S. airpower. The technologies are again grouped according to the system-level capabilities enabled (increased range and/or reduced signature; enhanced guidance, navigation, and/or targeting; and enhanced lethality); in addition to the previously described categories, a "counter-BLUE" category has been added.

Given the time available for this task, the examples presented reflect the expertise and experience of the committee members rather than representing the result of a systematic, comprehensive study. In each case the committee identifies the technology and the capability that it may enable, and postulates open source indications and motivators for domestic or foreign researchers to work in this direction.

Increased Range and/or Reduced Signature

The signature of a vehicle's propulsion system is a major contributor to the overall vulnerability of the vehicle. The propulsion system and its fuel make up 40 to 90 percent of the initial mass of powered-flight vehicles, while the payload is usually only 10 to 20 percent (even less for launch vehicles, at 1 to 2 percent). Thus, small changes in the performance or characteristics of the propulsion system can have a large impact on the payload, range, maneuverability, or vulnerability of an aircraft or missile. Technological advances considered here (see Charts 4-1 through 4-6) include propulsion systems as well as other techniques that could extend the range or reduce the signature of air vehicles.

Enhanced Guidance, Navigation, and/or Targeting

The technologies described in this subsection (see Charts 4-7 through 4-12), which are likely to emerge in the global commercial marketplace, provide improved performance for guidance and navigation or targeting systems.

Enhanced Lethality

The evolving technologies described in Charts 4-13 through 4-19 may serve to enhance the lethality of RED force capabilities.

Counter-BLUE

The technologies described in Charts 4-20 through 4-23 could be used to negate the BLUE force advantage.

CHART 4-1 Technology Assessment: Jet Engines

Technology	Observables
Jet engines: Very small (1 to 50 lb thrust), low-cost jet engines.	Small turbojet engines of appropriate size now sold internationally for the hobby market (Wilkinson, 2003) (see also www.wren-turbines.com/specifi.htm; last accessed on April 8, 2005); a Defense Advanced Research Projects Agency project to improve the performance of such small engines by a factor of 4 (see also www.darpa.mil/baa/baa04-12mod8.htm; last accessed on April 8, 2005); a robust research community in the United States, Europe, and Asia (Gerendas and Pfister, 2000).

Accessibility	Maturity	Consequence
Level 2	Warning	Negate man-portable air defense system (MANPADS) launch warning; greatly extend MANPADS range; extend unmanned aerial vehicle range (to thousands of kilometers) and speed.

CHART 4-2 Technology Assessment: Storable Liquid Propellant and Micro Rocket Engines

Technology	Observables
Storable liquid propellant, micro rocket engines	Microelectromechanical system research papers in the United States (London et al., 2001), Europe (Miotti et al., 2004), Asia (Takahashi, 2004); Missile Defense Agency-sponsored work in the United States for kinetic kill vehicles.

Accessibility	Maturity	Consequence
Level 3	Warning	Negate man-portable air defense system (MANPADS) launch warning; extend MANPADS range; antisatellite interceptors; micro intercontinental ballistic missile or launch vehicles.

CHART 4-3 Technology Assessment: Higher-Performance Small Rocket Engines

Technology		Observables
Higher-performance small rocket engines		New players entering business motivated by X Prize, perceived commercial opportunities, micro satellite enthusiasm.
Accessibility	**Maturity**	**Consequence**
Level 3	Watch	Small intercontinental ballistic missiles and space launchers.

CHART 4-4 Technology Assessment: Nanoscale Surface Machining

Technology		Observables
Nanoscale surface machining		Thermophotovoltaics, university research (Sai et al., 2003).
Accessibility	**Maturity**	**Consequence**
Level 2	Watch	Optical/IR stealth.

CHART 4-5 Technology Assessment: Electronically Tuned Surface Coatings

Technology		Observables
Electronically tuned surface coatings		Cancelled university programs in electro-optics, smart paper development (Lu et al., 2001; see also www.eink.com/technology/index.htm; last accessed on April 8, 2005).
Accessibility	**Maturity**	**Consequence**
Level 2	Warning	Optical/infrared stealth.

CHART 4-6 Technology Assessment: Negative Index of Refraction Materials

Technology		Observables
Negative index of refraction materials		University engagement of the technology (Wiltshire, 2001; Shelby et al., 2001).
Accessibility	**Maturity**	**Consequence**
Level 2	Watch	Improved infrared, optical, and radio-frequency stealth.

CHART 4-7 Technology Assessment: Low-Cost, Uncooled, Low-Noise Infrared Detector Arrays

Technology		Observables
Low-cost, uncooled, low-noise infrared (IR) detector arrays (especially mid-wave infrared (MWIR) and long-wave infrared (LWIR))		Automotive market, Defense Advanced Research Projects Agency programs, microelectromechanical system bolometers (see also www.xenics.com/Products/Lwir.php); last accessed on April 8, 2005), nano machining.
Accessibility	**Maturity**	**Consequence**
Level 2	Warning	Improved capability and range in man-portable air defense systems.

CHART 4-8 Technology Assessment: Narrowband, Tunable Frequency Agile, Imaging Infrared Optical Filters

Technology		Observables
Narrowband, tunable frequency agile, imaging infrared optical filters		Microelectromechanical system, commercial and weapons of mass destruction sensors, (example, monochrometer).
Accessibility	**Maturity**	**Consequence**
Level 2	Warning	Improved capability, countermeasure robust man-portable air defense systems.

CHART 4-9 Technology Assessment: High-Accuracy Microelectromechanical Systems Gyros and Accelerometers

Technology		Observables
High-accuracy microelectromechanical systems gyros and accelerometers		Automotive market, military investments.
Accessibility	**Maturity**	**Consequence**
Level 3	Warning	Very long range small unmanned aerial vehicles, missiles, and launch vehicles.

CHART 4-10 Technology Assessment: Automated, Ad Hoc, Cellular Phone/Computer Systems

Technology		Observables
Automated, ad hoc, cellular phone/computer systems		Commercial integration of cellular phones and computers, Web-based distributed computing.
Accessibility	**Maturity**	**Consequence**
Level 1	Alert	Remote queuing/targeting for man-portable air defense systems and mines; large, informal sensor and/or computer arrays for antistealth.

CHART 4-11 Technology Assessment: High-Speed Processor Chips and Mega-Flash Memories

Technology		Observables
High-speed processor chips and mega-flash memories		Security violations among algorithm-developer institutions.
Accessibility	**Maturity**	**Consequence**
Level 2	Warning	Targeting and/or discrimination algorithms.

CHART 4-12 Technology Assessment: Large Geographic and Economic Web Databases

Technology		Observables
Large geographic and economic Web databases		Economics, disaster management (see also http://www.nytimes.com/pages/world/worldspecial4; last accessed on April 8, 2005), Global Positioning System receivers in cellular phones.
Accessibility	**Maturity**	**Consequence**
Level 1	Warning	Low-cost targeting of U.S. assets.

CHART 4-13 Technology Assessment: Increased Energy Density or Slow-Burning Energetic Materials

Technology		Observables
Increased energy density or slow-burning energetic materials		New Defense Advanced Research Projects Agency program; warheads for small unmanned aerial vehicles, foreign research (Talawar et al., 2005).
Accessibility	**Maturity**	**Consequence**
Level 2	Watch	Extend man-portable air defense systems range; increase lethality.

CHART 4-14 Technology Assessment: High-Power, Low-Cost Microwave Radio-Frequency Chips and Arrays

Technology		Observables
High-power, low-cost microwave radio-frequency (RF) chips and arrays		Security violations among identified state-of-the-art RF chip manufacturers; export of this technology as embedded in Future Combat Systems.
Accessibility	**Maturity**	**Consequence**
Level 3	Warning	Frequency agility command detonation devices; antifuse system.

CHART 4-15 Technology Assessment: Very Low Cost Radio-Frequency Proximity Fuses

Technology		Observables
Very low cost radio-frequency proximity fuses		Commercial radar detectors, U.S. Army Research Laboratory demonstrations (Caito, 2004).
Accessibility	**Maturity**	**Consequence**
Level 2	Warning	Aerial mines; smart improvised explosive device.

CHART 4-16 Technology Assessment: Increased-Speed Digital Signal Processor and Processor Chips

Technology		Observables
Increased-speed digital signal processor and processor chips		U.S. success with antifuse systems, improved-capability video games.
Accessibility	**Maturity**	**Consequence**
Level 3	Warning	Antifuse systems.

CHART 4-17 Technology Assessment: Very High Pulse Power Systems

Technology		Observables
Very high pulse power systems (also see Chapter 3 in this report)		U.S. vulnerability and dependence on microelectronics, Soviet legacy.
Accessibility	**Maturity**	**Consequence**
Level 2	Warning	Non-nuclear electromagnetic pulse.

CHART 4-18 Technology Assessment: Bioagents

Technology		Observables
Bioagents (which attack aviation lubricants, fuels, transparencies, or composites)		Foreign military use of nonoptimal elastomers, fuel additives, literature on bioenvironmental cleanup.
Accessibility	**Maturity**	**Consequence**
Level 2	Futures/Watch	Neutralization of U.S. aviation.

CHART 4-19 Technology Assessment: Tactical Nuclear Electromagnetic Pulse

Technology		Observables
Tactical nuclear electromagnetic pulse		Foreign experimentation with nuclear devices; export of high-speed video games with gigahertz-speed processors; atomic research laboratory security violations and missing material (hardware, software, plans), U.S. government concerns on domestic infrastructure vulnerability.
Accessibility	**Maturity**	**Consequence**
Unknown	Unknown	Disabling of aircraft while in flight or on the ground; disabling of most of U.S. military.

CHART 4-20 Technology Assessment: Very Low Cost, Compact Near-Infrared Images

Technology		Observables
Very low cost, compact near-infrared images		Automotive market.
Accessibility	**Maturity**	**Consequence**
Level 3	Watch	Inexpensive, pen-sized laser illuminator warning receivers, trackers.

CHART 4-21 Technology Assessment: Wireless Technology, Frequency Modulation Techniques, Global Positioning System Crypto Capture

Technology		Observables
Wireless technology, frequency modulation techniques, Global Positioning System (GPS) crypto capture		The maturing of commercial wireless technologies and power sources focused in the $1^{1}/_{2}$ gigahertz range (available today). Attempts to capture GPS element with crypto gear along with attempts to imitate dynamics of the GPS satellite constellation.
Accessibility	**Maturity**	**Consequence**
Jamming: Level 1 Spoofing: Level 3	Alert Watch	Improved, low-cost GPS jammers and spoofers.

CHART 4-22 Technology Assessment: Multistatic Systems

Technology		Observables
Multistatic systems		Foreign military demand.
Accessibility	**Maturity**	**Consequence**
Level 2	Warning	Mitigate current radio-frequency stealth technologies.

CHART 4-23 Technology Assessment: Strong Commercial Encryption for Personal Digital Assistants and Cellular Phones

Technology		Observables
Strong commercial encryption for personal digital assistants and cellular phones		Global commercial marketplace.
Accessibility	**Maturity**	**Consequence**
Level 3	Warning	Force dispersion.

SUMMARY

Future threats to U.S. airpower in urban warfare owe much to two factors—the trend toward globalization in aerospace and electronics, coupled with what has been observed to be the best way to defeat U.S. airpower: that is, not necessarily the head-to-head, platform-to-platform approach of the Cold War, but rather the exploitation of asymmetries.

This chapter discusses in broad terms the threats posed by advanced MANPADSs and milli to micro air vehicles and missiles, considering system-level characteristics such as increased range and reduced signature; enhanced guidance, navigation, and/or targeting; and enhanced lethality. For each area, technologies that may enable such RED force capabilities are identified and assessed. Finally, several technologies that may enable RED forces to counter BLUE forces—either directly or indirectly—are identified and assessed.

Although U.S. air dominance is unlikely to be jeopardized in the near term by symmetric means, the committee believes that global technology trends suggest new types of threats that may be on the horizon.

REFERENCES

Published

Davis, W.R., B.B. Kosicki, D.M. Boroson, and D.F. Kostishack. 1996. Micro air vehicles for optical surveillance. Lincoln Laboratory Journal 19(2):197-213.

Francis, R. 1999. A System Study of Very Small Launch Vehicles. Master's Thesis. Massachusetts Institute of Technology.

Gerendas, M., and R. Pfister. 2000. Development of a Very Small Aero-Engine. Paper presented at ASME Turbo Expo, Munich, Germany.

Grasmeyer, Joel M., and Matthew T. Keennon. 2001. Development of the Black Widow Micro Air Vehicle. Reston, Va.: American Institute of Aeronautics and Astronautics. Available online at http://www.aerovironment.com/area-aircraft/prod-serv/bwidpap.pdf. Last accessed on February 8, 2005.

JCS (Joint Chiefs of Staff). 2000. Joint Vision 2020. Director for Strategic Plans and Policy, J5. Strategy Division. U.S. Government Printing Office, Washington, D.C. June

London, A.P., A.H. Epstein, and J.L. Kerrebrock. 2001. A high pressure bipropellant microrocket engine. Journal of Propulsion and Power 17(4):780-787.

Lu, Yunfeng, Yi Yang, Alan Sellinger, Mengcheng Lu, Jinman Huang, Hongyou Fan, Raid Haddad, Gabriel Lopez, Alan R. Burns, Darryl Y. Sasaki, John Shelnutt, and C. Jeffrey Brinker. 2001. Self-assembly of mesoscopically ordered chromatic polydiacetylene/silica nanocomposites. Nature 410(6831):913-917.

Miotti, P., M. Tajmar, C. Guraya, F. Perennes, B. Marmiroli, A. Soldati, M. Campolo, C. Kappenstein, R. Brahmi, and M. Lang. 2004. Bi-propellant Micro-Rocket Engine. Paper presented at CANEUS 2004-Conference on Micro-Nano-Technologies, Monterey, Calif.

Munson, Kenneth, ed. 1996. Jane's Unmanned Aerial Vehicles and Targets. Jane's Information Group, Coulsdon, Surrey, United Kingdom.

Sai, Hitoshi, Yoshiaki Kanamori, and Hiroo Yugami. 2003. Selective Emitters for Thermophotovoltaic Generation by Means of Metallic Surface Microstructures. Power MEMS 2003. Kyoto, Japan.

Shelby, R.A., D.R. Smith, and S. Schultz. 2001. Experimental verification of a negative index of refraction. Science 292(5514):77-79.

Takahashi, Koji. 2004. Micro Thruster For Miniaturized Space Systems—Need and Perspective. Power MEMS. Kyoto, Japan.

Talawar, M.B., C.N. Divekar, P.S. Makashir, and S.N. Asthana. 2005. Tetrakis-(4-amino-1,2,4-triazole) copper perchlorate: A novel ballistic modifier for composite propellants. Journal of Propulsion and Power 21(1):186-189.

Wicks, Frank. 2004. A model mission. Mechanical Engineering 126(12):44-46.

Wilkinson, T. 2003. SIMJET'S 1200 turbojet on test. Simply Excellent: pp. 18-21. Available online at http://www.simjet.com/Simjet1200.pdf. Last accessed on February 8, 2005.

Wiltshire, M.C.K. 2001. Bending light the wrong way. Science 292(5514):60-61.

Unpublished

Caito, Steve. 2004. Full Spectrum Active Protection Close in Layered Shield. Presentation to the Board on Army Science and Technology, June 8.

Gabbert, LTC Jeff, Product Manager, Medium Altitude Endurance UAV Systems. 2004. Army UAV Systems Overview. Presentation to the Board on Army Science and Technology, December 17.

Tousley, Brad. 2004. Update for MAV ACTD and OAV2 for the BAST. Presentation to the Board on Army Science and Technology, December 17.

5

Combatant Identification in Urban Warfare

INTRODUCTION

This chapter addresses new technology developments that might assist enemy combatants by allowing their identity and that of innocent noncombatants to be intermixed. Appropriate "spoofing" or other types of misidentification could cause the warfighter to engage a group of noncombatants, thus causing political and/or psychological damage to U.S. forces.

The type of combat situation—urban warfare—addressed here is a scenario in which the United States is increasingly engaged. This chapter describes potential techniques for sensor spoofing and for hiding RED forces, as well as some enabling technologies.

The enemy engaging in this type of warfare is often technologically nimble but unable to afford or even consider large weapons systems. Commercial technology of superior quality and capability that may be readily available from non-U.S. suppliers is a likely source of components for adversary systems. The synergistic trends of globalization and commercialization of science and technology are creating an environment in which U.S. forces may unexpectedly find themselves vulnerable. One example of offshore technology strength is the infrared (IR) laser-diode technology, which is effective in IR-thermal source spoofing. This technology was initially developed in the United States and is now manufactured and sold commercially in Switzerland.[1]

KEY FEATURES OF FOREIGN URBAN WARFARE

Modern urban warfare has been described extensively in connection with many wars over the past 50 to 75 years. Instances of such warfare include German/Soviet combat in Stalingrad, U.S. combat in Somalia and Iraq, and Russian combat in Chechnya (Beevor, 1998; Bowden, 1999). This type of combat has several distinct characteristics, including the following:

[1]For more information, see, for example, http://www.alpeslasers.ch/. Last accessed on April 1, 2005.

- *Complex "terrain."* Heavy combat in cities and large towns generates a chaotic artificial terrain. The lack of a clear line of combat as well as the presence of dust and smoke can make identification of combatants difficult or impossible. Combatants can easily remain hidden until detailed searches, lasting many days, are completed.
- *Short line of sight.* Urban combat occurs in an environment of extremely short lines of sight. Intense firefights between neighboring rooms in a housing unit, for example, are characterized by short range and a common element of surprise. Reaction time is very short, and positive identification may be possible only ex post facto.
- *Intermixing of noncombatants (noncombatants) and combatants.* When population densities are high, it is impossible to rule out the presence of significant numbers of noncombatants. In many cases these people are the most vulnerable of the former population, since it is hardest for them to leave the combat zone quickly. This situation makes it difficult for troops to engage enemy troops without fear of incurring casualties among noncombatants.
- *Need for precision delivery of weapons.* Because of the short distances, complex terrain, and mixing of targets, urban combat requires the ability to deliver ordnance with precision so that collateral damage is minimized. This capability is compromised if noncombatant or RED team identification is spoofed.

COMMITTEE FOCUS: CAPABILITY TO DISCRIMINATE BETWEEN ENEMY COMBATANTS AND NONCOMBATANTS

One form of misidentification relates to the issue of fratricide, which in itself is very challenging and has been addressed in other studies. A report from the Office of Technology Assessment entitled *Who Goes There: Friend or Foe?* discusses the Persian Gulf War and the problem of fratricide. During that conflict, 24 percent of U.S. combat fatalities were due to friendly fire (U.S. Congress, OTA, 1993). There is an optimal level of antifratricide measures beyond which more stringent measures could lead to increased losses from enemy fire owing to slow reaction times. The four pillars of fratricide prevention are doctrine, training, rules of engagement, and technology, as viewed from a BLUE force perspective (Armstrong, 1999). While related to the topic at hand, the avoidance of fratricide is not the central focus of the committee in this chapter; its focus instead is on the capability of discriminating between enemy combatants and noncombatants.

Rules of engagement from a RED force perspective include causing confusion, hiding among the noncombatant population in areas not necessarily designated as combat zones, jamming electronic devices, and moving so that prior reconnaissance or mapping by the BLUE force is of limited utility. When cast in the context of urban warfare, the scenarios become even more complex, if only because noncombatants must also be positively identified to avoid harming them.

The techniques for the identification of noncombatants in combat areas are stressed to the limit in urban warfare, principally because of the short timescale of combat and the possibility that large numbers of noncombatants might be present. Spoofing of sensors, including both visual and electronic imaging systems, compromises the BLUE force's ability to carry out precision engagements and may endanger noncombatants. Recent examples of urban combat have included the use of noncombatants as shields by enemy combatants. Finally, ground-to-ground combat even under the best of circumstances is prone to error; the fratricide rate during Desert Storm was 69 percent attributable to ground-to-ground combat (U.S. Congress, OTA, 1993). Urban environments further exacerbate the challenge relating to the discrimination of combatant forces.

IDENTIFICATION AND ASSESSMENT STEPS OF THE COMMITTEE METHODOLOGY

This section considers potential implications of emerging technologies that may be exploited by the enemy to degrade BLUE force capabilities relating to identification of friend or foe (IFF) and, more specifically, to discrimination between enemy combatants and noncombatants. Enemy combatants may leverage technological advances available in the global marketplace to develop methods of causing false identification of noncombatant parties as combatants. This situation could lead to the BLUE force's inflicting of casualties among the noncombatants and thus cause serious psychological damage to the BLUE forces and/or divert attention from the central BLUE force combat mission. Such events inevitably lead to political damage to the United States as well. Below, the committee describes three techniques that may be employed by RED forces to degrade the ability of BLUE forces to discriminate enemy targets.

Misdirected Target Designation

BLUE forces wish to engage only RED forces and related enemy targets. Currently, laser-designation technology is used to enable the precision guidance of weapons. RED forces' acquisition of inexpensive commercial laser systems, misleading designation and hence misleading weapons guidance parameters, could lead to the misdirection of munitions onto politically or psychologically sensitive targets. Such technology is accessible to RED forces in the form of rapidly advancing, low-cost, diode-laser technology. The state-of-the-art small, compact, diode-driven solid-state lasers are currently in the hands of overseas manufacturers that in many cases are the dominant manufacturer of these systems. These systems can be used to misdirect weapons, either by blinding the weapon or by retargeting it, so as to cause substantial noncombatant casualties.

An important technology in target designation is the use of wavelength tuning to prevent detection of the designating laser system. This can be an effective technique, since narrowband filters decrease the detection wavelength "bandwidth" and hence prevent out-of-band spoofing. At present there are a number of low-cost IR laser devices, which can be made wavelength agile (tunable). At the other end of the spectrum, an example of high-cost and advanced IR laser technology is the "quantum cascade" laser, which emits throughout the near and medium infrared.

Sensor Spoofing

Another method of IFF sensor spoofing by RED forces relies on the BLUE forces' use of sensor technology to identify military targets and to distinguish these from related civilian or noncombatant entities. For example, if an IR sensor has sufficient resolution or can use a feature such as spectral signature to discriminate among targets, it can be used as a reliable method for IFF. One example, which does use spectral-sensitive signatures, is an active forward-looking infrared (FLIR) system. As described below, these same technologies may be used by RED forces to spoof BLUE force sensors.

Tunable Lasers

The National Research Council report entitled *Opportunities in Biotechnology for Future Army Applications* further analyzes the possibilities for RED force spoofing of BLUE force identification measures. As stated in that report, "Because humans, tanks, and other military structures have a significantly different reflectivity than plants and trees, the enemy can easily identify military targets with

inexpensive infrared lasers with wavelength-scanning capability" (NRC, 2001). If, on the other hand, the RED force were to possess such tunable lasers, it could rapidly mimic the key spectral ingredients in various targets and use this knowledge to spoof civilian targets in a way that could cause them to be erroneously identified as bona fide RED targets. For military structures, because a small fraction of the "target would be observable because of its distinctive spectral properties it may be possible to develop paints with terahertz and infrared reflectivity identical to trees or grass, possibly using genetically engineered plant protein as the active medium" (NRC, 2001). See Chart 5-1.

False Radio Frequency Identification Signals

Radio-frequency (RF) sensors are also vulnerable to spoofing. Radio-frequency identification (RFID) is a technology that uses various RF bands to probe a transponder carried by BLUE forces or a friendly noncombatant. The transponder then responds to this probe, using either onboard (battery) energy or power from the interrogating beam to cause a coded reply, which can be read by the interrogator. The market for this technology is expanding rapidly, because RFID is useful for a wide variety of commercial applications such as merchandise identification, automatic toll payment, animal identification and tracking, and so on. Since the heart of the technology is microchips and advanced microwave devices, it can be expected to advance further in sophistication and availability over the next decade.

For the same reasons that RFID will continue to develop, "false tag" methods will also grow in capability. These methods could enable RED forces to "masquerade" as friendly forces, thus diminishing BLUE forces' confidence in RFID. See Chart 5-2.

CHART 5-1 Technology Assessment: Tunable Lasers

Technology		Observables
Tunable lasers		These lasers were invented and developed in the United States, but they are now manufactured overseas. They are an extremely powerful source for placing an intense infrared signal at the position of the pointed laser beam. This laser is now readily available overseas, and suppliers are accessible via the Internet.
Accessibility	**Maturity**	**Consequence**
Level 1	Warning	Spoofing of BLUE sensors by changing/determining key spectral components in targets.

CHART 5-2 Technology Assessment: False Radio-Frequency Identification Signals

Technology		Observables
False radio-frequency identification (RFID) signals		There are a number of suppliers of RFID technology. Detailed information is available at a Web site of the U.S. Department of Energy's Pacific Northwest Laboratory.
Accessibility	**Maturity**	**Consequence**
Level 1	Warning	Diminished trust in BLUE RFID.

Projection of Realistic-Looking Real-Time Optical or Infrared Images

Realistic-looking false-image projection will grow with the increasing availability of low-cost lasers and holographic images. In urban warfare, reaction time is very short, and the sudden appearance of any image may immediately elicit a response—for example, a programmed false image could provoke firing at an inappropriate target. The ingredients for this technology are powerful personal computers, advanced lasers, and real-time holographic media. All of these are advancing rapidly, owing in large part to demands from the commercial marketplace.

While the examples provided below may seem farfetched for a warfare environment, the committee believes that there is some value in tracking such emerging technologies, since they may spawn RED force tactics that could be difficult to counter. It should be noted that the committee did not have time to separate "marketing hype" from actual capabilities in the examples below.

Figure 5-1 shows the result of a system in which a "microscopic pattern of particles [is] suspended in a transparent medium that simultaneously diffracts, reflects and transmits all wavelengths of light. Through this proprietary process the TransScreen displays a projected image as well as allows you to see beyond the image floating in space."[2]

Figure 5-2 illustrates HoloMirror technology that:

> generate[s] the illusion of a hologram by projecting specially created video images that are projected and focused to a point in space in front of the kiosk. Even though the projection source is within the kiosk housing, the image appears out in front of the display. In pictures below you will see hands pointing at or near the projected image. To the person viewing the HoloMirror they are really seeing their hand passing through the object or they are seeing the 3D image hovering above or below their hand. It is impossible to show the true 3D effect here in photographs. But these pictures will give you a bit of an idea of what happens when you experience a HoloMirror in person. Laser Magic offers two types of HoloMirror 3D Volumetric Projectors.[3]

Figure 5-3 illustrates a life-size hologram. According to the manufacturer's Web site:

> There is nothing like the magic of a real hologram. It's like a window into another world. View it from one angle and a crystal clear 3D image is clearly visible. Step to the side and the image disappears without a trace. As you walk back and forth in front of a hologram, the image moves and you can see around it as if it were really there.[4]

Projection of a programmed false image could provoke BLUE forces to fire on an inappropriate target. The committee has considered scenarios in which such capabilities may become more accessible to RED forces as materials suitable for projecting and showing the images are commercialized and adapted in consumer and fashion marketing. See Chart 5-3.

Hiding of Targets

Another potential method of inducing erroneous noncombatant targeting stems from the following fact, as discussed in the National Research Council (NRC) report *Opportunities in Biotechnology for Future Army Applications*:

[2]See http://www.laser-magic.com/transscreen.html. Last accessed on April 25, 2005.
[3]See http://www.laser-magic.com/HoloMirror_Pictures.html. Last accessed on April 25, 2005.
[4]See http://www.laser-magic.com/holograms.html. Last accessed on April 25, 2005.

FIGURE 5-1 TransScreen, power holographic projection creates the illusion of life-size, holographic images. SOURCE: Reprinted with permission. © by Laser Magic Productions.

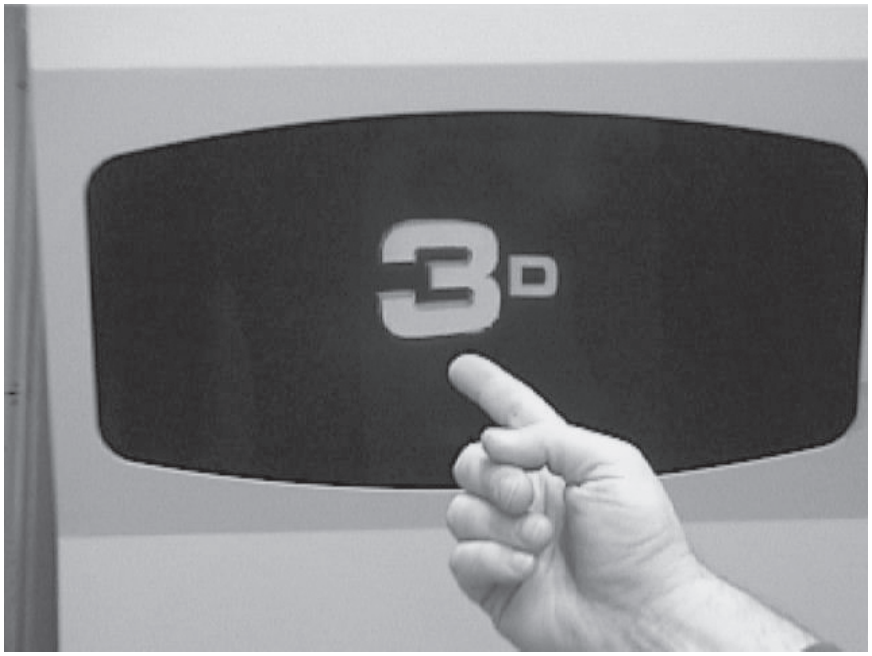

FIGURE 5-2 Example of a projected three-dimensional image that appears to be floating above the hand. SOURCE: Reprinted with permission. © by Laser Magic Productions.

FIGURE 5-3 Life-size hologram. SOURCE: Reprinted with permission. © by Laser Magic Productions.

CHART 5-3 Technology Assessment: Projection of Realistic-Looking, Real-Time Optical or Infrared Images

Technology		Observables
Projection of realistic-looking, real-time optical or infrared images		Rock concerts; entertainment industry (markets that may drive technological advances in holographic imagery).
Accessibility	**Maturity**	**Consequence**
Level 2	Watch	Spoofing visual sensors.

> Biological systems can also be mimicked for the next generation of soldier camouflage uniforms. One [example of this approach] uses mimicking of the mechanical chromatic effects that birds and fruits use. The exquisite color patterns on the feathers of birds are the result of the intricate structural pattern of each feather that enables it to diffract light. This phenomenon, mechanical chromatophores, is also exhibited by some varieties of fruits. Another natural phenomenon that might be valuable for camouflage is the biochromatic behavior of some reptiles. The chameleon, for example, can change color and patterns in accordance with the environment. Camouflage with this property would automatically change to blend with the environment, such as snow-covered terrain, desert sand, dense and light vegetation, daylight and darkness (NRC, 2001).

Prominent research centers in the United States and elsewhere are working on adaptive materials—in particular, exploiting polymers, biomimetic structures, and nanotechnology. Both the Defense Advanced Research Projects Agency and the U.S. Army support research in this area, advances in which could eventually lead to capabilities that enable RED force hiding.[5,6] Acquisition of such technology by RED forces would enable them to spoof BLUE forces by camouflaging their appearance and making themselves harder to detect. See Chart 5-4.

New types of stealth could become available in the form of coatings that consist of microwave-absorbing paint (see Chart 5-5), or interactive displays of the type described above. BLUE force development of an intelligent surface coating that is readily apparent for night vision, or, conversely, that neutralizes night vision in a manner that could redirect ordnance, could become a RED force advantage if the technology is redirected to spoof night vision. Advances in IR-absorbing coatings (proteins), temperature-noncombatant materials, and heat-emitting coatings could enable such capabilities.

The availability of IR-absorbing coatings may be a near-term possibility. Commercial development of a coating used to weld textile fabrics is based on this principle. Clearweld®, a process patented by The

CHART 5-4 Technology Assessment: Adaptive Materials

Technology		Observables
Adaptive materials		Literature reports of wearable displays integrated into common clothing and electronic ink are available on the Internet. At least one Web site reports that a wearable display is under development in Japan and is described as optical camouflage.[a]
Accessibility	**Maturity**	**Consequence**
Level 2	Watch	Camouflage automatically changes to blend with the environment.

[a]See for example, http://smh.com.au/cgi-bin/common/popupPrintArticle.pl?path=/articles/2004/08/13/1092340452457.html. Last accessed on April 8, 2005. See also, http://www.star.t.u-tokyo.ac.jp, which presents research by international researchers. Last accessed on April 8, 2005.

[5]For additional information see, for example, Massachusetts Institute of Technology's Institute for Soldier Nanotechnologies, http://web.mit.edu/isn/. Last accessed on April 25, 2005.

[6]For additional information see, for example, http://www.darpa.mil/dso/thrust/matdev/matdev.htm. Last accessed on April 25, 2005.

CHART 5-5 Technology Assessment: Bacteriorhodopsin

Technology		Observables
Bacteriorhodopsin (and other infrared-absorbing coatings)		Biocatalogs and Web sites for textile manufactures.
Accessibility	**Maturity**	**Consequence**
Level 3	Watch	New types of stealth to enable RED forces to hide from BLUE force sensors.

Welding Institute, Ltd., is being commercialized by Gentex Corporation.[7] Commercially available lasers and a colorless IR-absorbing medium, used in place of a carbon black absorber, enables clear plastics to be welded. The IR-absorbing medium is printed or painted onto one surface of the joint, encompassed into the bulk plastic, or produced in the form of a film that can be inserted into the joint. The medium absorbs IR laser light, allowing an almost invisible weld to be produced between materials that are required to be clear or have a predetermined color.

The NRC (2001) report also discusses biological methods that may be employed by RED forces to evade detection:

> Biological means might also be useful for avoiding radar detection. Some biomolecules have long been known to be strong microwave absorbers. For example, bacteriorhodopsin has strong microwave absorptivity (3 GHz to 40 GHz). Scientists are investigating the use of chemically, and possibly genetically, modified bacteriorhodopsin protein as the active medium in microwave-absorbing paint for both tanks and planes. The absorption mechanism appears to be associated with the motion of monovalent and divalent metal cations within channels, e.g., Mg(II), Ca(II). If this theory is correct, proteins could be engineered to have precise microwave absorption bands and then fine tuned for anticipated threats in a given theater of operation. Microtubules, which are also excellent microwave absorbers, may be even better microwave absorbers and more easily fine tuned. Because much of the research in this area is classified, the committee was not able to make recommendations in this area (NRC, 2001).

Is a protein with the appropriate optical and physical properties a possibility in the near future? According to the NRC (2001):

> From 1975 to 1995, scientists in the former Soviet Union participated in a government-sponsored program to leapfrog the West in computer technology by exploring protein-based bioelectronics. Many of the anticipated applications were military and may therefore be important to the U.S. Army, but details remain classified. One of the best-known accomplishments of the Soviet project was the development of biochrome, a real-time photochromic and holographic film based on chemically modified polymer films containing bacteriorhodopsin (Vsevolodov and Poltoratskii, 1985; Bunkin et al., 1981). The published photochromic and holographic properties of bacteriorhodopsin stimulated the international research that continues today. The protein bacteriorhodopsin is representative of the potential that proteins may have for future Army applications (NRC, 2001).

[7]For more information, see, for example, www.twi.co.uk/j32k and www.gentexcorp.com. Last accessed on February 11, 2005.

CHART 5-6 Technology Assessment: Transgenic Crops

Technology		Observables
Transgenic crops		Seed companies.
Accessibility	**Maturity**	**Consequence**
Level 1	Watch	Ability to grow materials and/or toxins.

INEXPENSIVE SUPPLY OF RAW MATERIALS FOR CAMOUFLAGE

An impediment to RED or BLUE forces' implementation of technology such as that described above is the availability of materials in sufficient quantities to be useful. To overcome this barrier, agricultural biotechnology might be used for the large-scale production of some new materials. For example, "the protein from soybeans can be refined and sold for only pennies per pound of protein, substantially less than the cost of manufacturing equivalent synthetic polymers" (NRC, 2001). In addition, "genetically engineered crops (transgenic crops) could potentially deliver recombinant proteins directly with the food or feed products in which they are found" (NRC, 2001). When it is considered further that such crops could be cultivated in caves ("underground agriculture"), the production, using relatively low technology, of some types of materials that have the capability of obfuscating the identification of noncombatants or a RED force is a remote possibility. See Chart 5-6.

SUMMARY

The committee notes that U.S. leadership in research or manufacturing can no longer be assumed in a number of the technologies discussed in this chapter. Japan, for example, is extremely strong in many areas of nanotechnology and in optical and electronic devices. China is, in many cases (such as photonics), the country with the best combination of high-technology manufacturing and design, and Chinese capabilities are increasingly employed by many high-technology U.S. firms. Europe has excellent research capabilities in the areas of semiconductor materials and devices; these can be and have been translated into start-up corporations.

As a result of this shift to offshore commercial vendors, important indicators are likely to appear in open source literature, including commercial Internet sites, and at industrial fairs particularly in Asia and Europe. The monitoring of key corporations is important. However, in many cases small or obscure start-ups are also of vital importance (suggesting that the tracking of venture capital may offer yet another set of relevant observables). In certain cases, the observation of critical manufacturing items (raw materials and/or equipment) may be useful, since the global marketplace, together with Internet-accessible "directions," is empowering friend and foe alike.

REFERENCES

Armstrong, Steven E. 1999. Fratricide: Fact or Fiction? Naval War College, Newport, R.I. Available online at http://handle.dtic.mil/100.2/ADA370683. Last accessed on February 9, 2005.

Beevor, Antony. 1998. Stalingrad. Viking, New York, N.Y.

Bowden, Mark. 1999. Black Hawk Down: A Story of Modern War. Atlantic Monthly Press, New York, N.Y.

Bunkin, F.V., A.B. Druzhko, B.I. Mitsner, A.M. Prokhorov, V.V. Savranskii, T.B. Shevchenko, N.W. Tkachenko, and N.N. Vsevolodov. 1981. Diffraction efficiency of bacteriorhodopsin and its analogs. Soviet Technical Physics Letters 7:630-631.

NRC (National Research Council). 2001. Opportunities in Biotechnology for Future Army Applications. National Academy Press, Washington, D.C.

U.S. Congress, OTA (Office of Technology Assessment). 1993. Who Goes There: Friend or Foe? OTA-ISC-537. U.S. Government Printing Office, Washington, D.C. Available online at http://govinfo.library.unt.edu/ota/Ota_1/DATA/1993/9351.PDF. Last accessed on February 9, 2005.

Vsevolodov, N.N., and V.A. Poltoratskii. 1985. Holograms in biochrome, a biological photochromic material. Soviet Physics Technical Letters 30:1235.

6

Biotechnology Trends Relevant to Warfare Initiatives

INTRODUCTION

Developments in biological and biochemical technologies relevant to modern warfare are advancing rapidly. Technology contributions come from scientists working in academic, military, and industrial environments in many countries. Information from academic laboratories is usually published in open source literature, but advances made both by military research laboratories doing biomedical research and by biotechnology companies are likely to be tightly held secrets or proprietary. Therefore, for the United States to maintain superiority requires being prepared for new developments through constant vigilance, research, and information gathering.

Modern techniques allow easy manipulation of the genetic information carried by viruses, bacteria, parasites, cells, and organisms. One obvious area in which biological research is relevant to the health of warfighters is the development of pathogens that are engineered to be resistant to current antibiotics or vaccines, to be more virulent, or to be more easily transmitted. This area of biological warfare, which has been examined by a number of other committees, is excluded from the tasks of this committee at the request of the Technology Warning Division and is not included in this report.

Beyond biological warfare, however, there are many ways in which biological techniques can be used to alter the mental or physical readiness of troops for battle, to confound current methods for detecting biological or chemical agents in the field, or to divert the energies of troops to tasks that are counterproductive; or, such techniques can be used as means for developing bio-inspired approaches for communication. This chapter highlights examples of some of these technologies and assesses their states of development. The approach taken here involves first postulating new BLUE force capabilities that leverage this burgeoning research field and then evaluating potential RED force applications of related technologies.

Watching People Think

> I have two children and love them very much. But my love to see God was stronger than my love for my children, and I'm sure that God will take care of them if (sic) I become a martyr. . . . I'm proud to be the first (sic) female martyr.
>
> Reem Saleh Riyashi,
> Seventh female Islamic Fundamentalist suicide bomber,
> January 14, 2004

> The fact that a woman took part for the first time *in a Hamas operation* marks a significant evolution . . . women are like the reserve army—when there is a necessity, we use them. Today we needed her because there are a lot of problems for a man to reach out to Israelis in the West Bank and Gaza.
>
> Sheik Ahmed Yassin,
> Founder, Islamic Resistance Movement (Hamas),
> January 14, 2004
>
> *Washington Post* Foreign Service
> M. Moore, Jerusalem

Until now, it has been impossible to understand scientifically how persons can behave in ways that Western political, psychological, and psychiatric criteria define as pathological. This inability to understand motivation has caused U.S. military planning and response strategy to be focused on preemptively, post hoc punishment and on attempts to educate through ineffective traditional propaganda and occasional "active measures."

The reason for the confounding nature of the problem and for the failure of this nation to stem its growth relate directly to the simple fact that traditional Western models of behavior cast such actions as psychopathological. It is likely that these actions, rather than being pathological in the contexts in which they reside, are the actions of rational thought and of educational processes that U.S. leadership has not defined, and that they will escalate until and unless the United States can "watch these people think."

Scientific Methods That May Predict Behaviors

Physicians and psychologists are now using a new set of technologies for analyzing brain function. Initial data have been collected and analyzed in three parallel research streams which support the contention that the U.S. research community is now poised to change the paradigm of dealing with behavioral phenomena in subjective Western practice.

The technologies of structural magnetic resonance imaging (MRI) and functional MRI (fMRI), magnetoencephalography (MEG), and near-infrared spectroscopy (NIRS) are being newly applied to real-time brain imaging. During the brain scans, the subjects of the experiments observe, through virtual-reality technology, images, sounds, and voice commands, and they also see written text. Online proprietary software ensures in real time that the appropriate (hypothesized from past extensive behavioral research) part of the brain cortex (e.g., the occipital sensory visual and auditory centers) is engaging the "message" presented. Pre- and post-identification of activation levels (blood-oxygen-level-dependent, fMRI and MEG) from cognitive processing (e.g., prefrontal cortex), emotional uploading to that process

(e.g., from the limbic system's amygdala and para-hippocampal nuclei), and the effects of rational behavior (pre-instructed commands to the subjects) are collected and analyzed.

Next-generation experiments will extend this work to a clearer understanding of how the following—(1) cultural affects of personality, fashioned especially in fundamentalist ashrams and Islamic fundamentalist schools for preteenagers; (2) ideographic, tonal, and symbolic languages (e.g., Farsi, Hindi, Mandarin, and Thai) versus linear and lexical (e.g., English and German) languages; and (3) constructs of written materials—engage differently the brains of different individuals. The research is objective and repeatable. It is independent of preassigned values of any cultural disposition or orientation. The neurophysiology of thought is being studied now in experiments that demonstrate the active brain centers that subtend language differences, emotional experience (moral repugnance, fear, anger, disgust, sadness, and pleasure), and value-based religious and personal experience.

Brain imaging is an area of active research; while discernible progress has been achieved, its full potential is as yet unknown. Brain-imaging technologies may provide a better understanding of behavior, performance, readiness, and stress that is relevant to troop readiness, understanding of cultural differences in motivation, and prisoner motivation. Additional, related information is provided in Appendix E, which also includes more specific descriptions of how such advances could be used by BLUE forces.

COMMITTEE FOCUS: CHALLENGES TO COMMUNICATIONS SUPERIORITY

Communications superiority plays a dominant role in the effectiveness of BLUE force operations. This capability relies on sophisticated technologies and flexible networking of the knowledge generated through such technologies. Today U.S. forces "own the C4ISR [command, control, communications, computers, intelligence, surveillance, and reconnaissance] information network," although the direct challenges described in Chapter 3 are on the horizon.

The covert transmission of information between forces is essential to effective timing and control of actions (both offensive and defensive). Achieving RED force command, control, and communications (including intelligence gathering, surveillance, and reconnaissance) among its independent, dispersed units could support effective guerilla engagement of traditional forces. Such communications might involve the transmission and receipt of short messages (e.g., commands that trigger prearranged events, coordination for precision fire, or relocation of operations) or more complex messages (e.g., those establishing strategies, complex timing, tiered responses, or detailed changes in operations). A framework to achieve effective, inexpensive, yet reliable communication between RED force units under these conditions must be easily accessible, undetected by BLUE forces, and sufficiently robust to carry all of the required information in a manner that can be validated. Hiding simple to complex packets of information in easily accessible physical form or in widely accessible databases could support the basic requirements. Integrating such seemingly innocuous databases with traditional mail that is physically handed off, or with a global, instantaneous, free-access communications system could generate the capability for RED force C4ISR across dispersed, independent units.

The transmission of encrypted messages across the Internet is commonplace, but it provides no cover of invisibility to its users. Hiding information within seemingly innocuous transmissions (steganography) could further veil the information. A successfully hidden message may be overlooked as a part of something else, whether that is the physical package of the information (such as microdots) or the complexity of the message medium itself (such as hidden information in digital images). For example, steganography can be used for the legitimate validation of image authenticity. The Content ID Forum and the Digital Content Association of Japan have created digital watermarks, equivalent to short

messages, to prevent piracy.[1] The information density of such watermarks allows a single letter of ASCII (American Standard Code for Information Interchanges) text to be fixed across three pixels,[2] generating enough capacity to carry a small message hidden in the noise of the image signal. However, as document size increases, the induced noise will degrade the quality of the image to the point of becoming detectable.

Covert Communications via DNA

One inexpensive and reliable way to transmit more complex information might be to hide data or messages in the sequences of DNA or in the databases describing the sequences of DNA (or in the sequences and structural data of proteins) that are so prevalent in the scientific literature. While digital systems are binary in nature, the information content of a DNA database is coded in a base-four sequence represented by the letters A, T, C, and G. (In a physical sense, the actual structure and sequences of DNA that hold a potential data density are more than 1 million gigabits per square inch, compared with a typical PC hard drive of approximately 7 gigabits per square inch.[3]) Recent publications have projected this approach to the construction of actual DNA containing hidden messages. Typically, data describing functional DNA in the scientific literature contain large stretches of sequences that are not intimately related to the function of the gene. The capacity of the human genome database to hold steganographic data without exceeding the normal noise-to-signal ratio is enormous.

Researchers Clelland and Bancroft developed a simple physical methodology to encode and recover secret DNA messages embedded in the 3 million-fold excess of normal human DNA.[4] However, there is potentially a much more rapid and simpler way of transmitting the hidden information than physically moving constructed DNA as samples or microdots. Simply encrypting a message into the base-four language of DNA (IBM has developed a language for storing information in DNA sequence data[5]) might be sufficient to hide messages between RED force teams. Such coded information might seem perfectly normal in the context of daily scientific discussions on the Internet. (See Chart 6-1.) These messages could be transmitted and received quickly, but they would rely on the appearance of scientific validity to remain undetected.

More secure transmission of information could be achieved by embedding the encrypted message into the redundant or apparently superfluous regions of a database describing an actual genome (the

[1]For more information, see, for example, http://www.cidf.org/japanese/english/docs/gen/cidf-gen-en-38.pdf. Last accessed on February 11, 2005.

[2]For more information, see, for example, http://en.wikipedia.org/wiki/Steganography#Steganographic_techniques. Last accessed on February 11, 2005.

[3]For more information, see, for example, http://www.kuro5hin.org/story/2004/10/26/02313/946. Last accessed on February 11, 2005.

[4]For more information, see, for example, http://inka.mssm.edu/~bancroft/papers/NATURE.pdf. Last accessed on February 11, 2005. Clelland and Bancroft have won a patent for DNA steganographic authentication. Applied DNA Sciences (Los Angeles) is actively pursuing DNA-based authentication of a wide range of materials and has been the subject of recent press coverage. Application of the steganographic potential of DNA (in the form of DNA microdots or packets of DNA transmitted through conventional methods) increases the potential to hide the medium of delivery while further hiding the message or identifier within the DNA itself. Encryption of the base-four lexicon is a logical extension of this approach, but may not be necessary in practical application. Such a physical or database-representation medium for covert message transmission is capable of holding information ranging from single words to very large documents.

[5]For more information, see, for example, http://www.bio-itworld.com/news/090904_report6001.html. Last accessed on February 11, 2005.

CHART 6-1 Technology Assessment: Exploitation of DNA Databases for Covert Communications

Technology		Observables
Exploitation of DNA databases for covert communications		Registration for access to Web site resident DNA or protein structure databases is easy to obtain but can be tracked. Most such databases can be copied but not modified by the user (limiting their usefulness for transmitting messages to the provision of the legitimate database with its well-known signal-to-noise ratio). Comparison of the signal-to-noise ratio of candidate messages to the authentic database might indicate the presence of hidden data. Open literature Web sites that do not require registration and allow some manipulation of the data could be candidate mailboxes. The convergence of (1) Internet discussion of DNA databases that are small enough to afford short upload and download characteristics and (2) unlikely participants might suggest steganography.
Accessibility	**Maturity**	**Consequence**
Level 1	Warning	Threaten BLUE communications superiority.

"noise" regions among the "signal" regions of legitimate scientific interest). Typical noise-to-signal ratios in such data could effectively hide large amounts of information. This approach might be expanded to include the data sets for three-dimensional structures of proteins to hide the coordinates for a literal map of a battle theater. To the extent that Internet access (telephone, digital subscriber line, cable, wireless, satellite) is available and reliable, communication between RED force units might approach real-time capability.

Many approaches to encryption and steganographic hiding could be imagined. The potential of this approach derives from the large "noise" component of current databases and the ease with which such databases are shared in the global community. As molecular biology defines the noise regions, it may become easier to identify false or incorrect databases.

Covert Communications via Bacteriorhodopsin

Biomolecular electronics are being applied to the encryption of messages using protein-based holograms. Much of the work has focused on the use of bacteriorhodopsin, a protein produced by the salt marsh archaebacteria *Halobacterium salinarium* found in high-temperature brine pools. This transmembrane protein is a green, sunlight-driven proton pump that can maintain its structure and function at temperatures as high as 140°C (Shen et al., 1993). The native molecule is composed of three protein chains, each of which has a molecule of retinal bound deep inside. Retinal contains a string of carbons that strongly absorb light. When a photon is absorbed, it causes a change in the conformation of the

molecule from a straight form to a bent form that powers the pumping of protons.[6] The protein has been adapted for device application because it can undergo structural changes induced by light once every few milliseconds for hundreds of millions of times.

As stated in the NRC report *Opportunities in Biotechnology for Future Army Applications*:

> Bacteriorhodopsin has excellent holographic properties because of the large change in refractive index that occurs following light activation. It converts light into a refractive index change with approximately 65% efficiency. Furthermore, the protein is 10 times smaller than the wavelength of light. This means that the resolution of the thin film is determined by the diffraction limit of the optical geometry rather than the graininess of the film. Bacteriorhodopsin can absorb 2 photons simultaneously and therefore can be used to store information in 3 dimensions by using 2-photon architectures (NRC, 2001).

Bacteriorhodopsin can also be genetically engineered to do different tasks and adapted for numerous protein-based devices (Wise et al., 2002; Hillebrecht et al., 2004). Mutations have been introduced that enhance its holographic properties, and one of the most successful device applications has been in the development of holographic and volumetric three-dimensional (3-D) memories. In principle, an optical 3-D memory can store roughly three orders of magnitude more information than that on a 2-D optical disk in the same size enclosure. These protein-based memories have the advantage of the memory medium's being extremely rugged. It can withstand substantial gravitational forces and is unaffected by high-intensity electromagnetic radiation and cosmic rays. These memories are also lightweight and insensitive to moisture. Therefore, protein-based polymer cuvettes would be a suitable memory medium for troops to carry with them into harsh environments.

Bacteriorhodopsin-based films can also be produced for use in developing pattern-recognition devices and large-scale associative memories and associative processors that would allow for the processing of intelligence and sensor data in visual formats from multiple sources in real time (NRC, 2001). One company offering bacteriorhodopsin for sale for use in "optical data processing, optical switches, holography, information processing, nonlinear optics and light sensors" is the Consortium für Elektrochemische Industrie GmbH in Munich. (See Chart 6-2.)

The current problem with the use of this technology is that, to be read, such a protein-based hologram cube (the size of a sugar cube) requires a light source the size of a large suitcase. However, if the light sources and instrumentation are shrunk to the size of a personal digital assistant, the cube becomes practical to be carried and read in the field.

COMMITTEE FOCUS: CHALLENGES TO BATTLE READINESS

Troops must be ready to respond to threats on short notice as well as to participate in planned military actions. Disease that incapacitates but does not kill (as opposed to the effects of weapons of mass destruction) can be disabling and the source of the infection difficult to determine. Particular vulnerabilities are the foodborne, vectorborne, and zoonotic diseases that could be introduced locally and for which vaccines, good diagnostics, and treatment are not available. A number of pathogens could be envisioned for such development. Two that are particularly likely are noroviruses and avian influenza virus.

The committee notes that such developments fall outside the realm of acceptable offense from the BLUE perspective. As observed in Chapter 1, however, BLUE forces may well encounter RED forces that are willing to employ capabilities that the United States would not consider.

[6]For more information, see, for example, Protein Data Bank, http://www.rcsb.org/pdb/molecules/pdb27_1.html. Last accessed on February 11, 2005.

CHART 6-2 Technology Assessment: Bacteriorhodopsin for Holographic Messaging and Development of Advanced Holographic Technologies

Technology	Observables
Bacteriorhodopsin for holographic messaging and development of advanced holographic technologies	This technology is likely to come from advances in DVD (digital video disc) technology for movies. The most likely source would be the commercial sector (e.g., technology companies such as Apple Computer and Gentec). Web sites for light shows, rock bands, pseudomilitary companies, and special-effects houses should be monitored.

Accessibility	Maturity	Consequence
Level 2	Watch	Threaten BLUE communications superiority.

Noroviruses

Particularly disabling pathogens are viruses in the *Norovirus* family. Noroviruses (also called Norwalk-like viruses) are spread through contaminated food or water; they cause acute vomiting, diarrhea, and fever. There are many viruses in this group, so multiple episodes of infection are common. Noroviruses are extremely contagious because of their low infectious dose (<100 viral particles), prolonged asymptomatic shedding (up to 2 weeks after recovery), ability to resist chlorination, and stability in the environment. Norovirus outbreaks are common in military deployments and were the most common cause of disability among soldiers in Operations Desert Storm and Desert Shield (McCarthy et al., 2000). A 2002 outbreak among British soldiers and hospital staff in Afghanistan resulted in closure of the field hospital. Eleven people with severe symptoms were evacuated to Germany and England, partly because of the inability to diagnose the disease (MMWR, 2002).

Currently, this group of viruses cannot be cultured, so the ability of individuals to purposefully introduce infection through contamination of the food or water supply is limited (the only source of virus is stool of an infected person). However, this is an area of intense investigation, and the recent report of the culture of a mouse norovirus may lead the way to the culture of human noroviruses (Wobus et al., 2004). If cultured organisms were available, strains for which immunity is uncommon or does not exist could be chosen for introduction at strategic times and places. The DNA copy of the virus could then be used to produce specifically altered forms of the virus that could be designed to evade immunity, to have increased virulence, or to deliver genes encoding toxins or other virulence factors. (See Chart 6-3.)

Avian Influenza

Another pathogen of concern is the family of avian influenza viruses—both H5N1 and H7N2 have caused severe human illness. Influenza virus is spread by the respiratory route, so an introduction of infection into a military population might be more difficult than with a foodborne or waterborne virus. However, it could be introduced through infection of local animals such as pigs or chickens. Lack of immunity in the human population would ensure widespread disease. The major current barrier to the use of this virus to disable military populations is the lack of human-to-human transmission of current strains. (See Chart 6-4.)

CHART 6-3 Technology Assessment: Development and Distribution of Norovirus Organisms

Technology		Observables
Development and distribution of norovirus organisms		An indicator is evidence that a laboratory is conducting research aimed at producing a representative of this group of viruses in culture. This would include development of new lines of cells derived from the gastrointestinal tract. Development of mechanisms of stabilizing the virus and development of vaccines that could be used to protect the adversary would be an indicator of deployment.
Accessibility	**Maturity**	**Consequence**
Level 2/3	Warning	Debilitation of BLUE forces.

CHART 6-4 Technology Assessment: Development and Distribution of Avian Influenza Organisms

Technology		Observables
Development and distribution of avian influenza organisms		Indicators would include construction of high-containment laboratories for work with virulent strains, reports of laboratory-acquired infections, or increased use of primates in containment facilities. Development of vaccines to protect the adversary would be an important component of such a research program.
Accessibility	**Maturity**	**Consequence**
Level 2/3	Watch	Debilitation of BLUE forces.

Research that leads to an understanding of the biologic determinants of transmissibility by respiratory secretions will allow scientists to engineer current virus strains for efficient spread. The technology is already available and in use for genetically engineering influenza virus.

Although many laboratories are working on influenza, relatively few are investigating the determinants of transmissibility. Initial work is likely to be with easily manipulated animal model systems (e.g., mice, ferrets) in which virologic determinants of transmission from one animal to another by the respiratory route can be identified using genetically engineered strains of virus.

Synthesis of Decoys

A release of infectious agents as weapons of mass destruction (WMDs) is a current major military concern. Several organisms have been developed as WMDs by one country or another. Sophisticated sensors based on the known antigenic composition and genetic or protein sequence of these organisms considered to be of highest risk are in current use, and advanced versions are under development. A release of compounds or agents that react with these detectors, but are not the actual agents, would be of

CHART 6-5 Technology Assessment: Development and Distribution of Organisms as Decoys

Technology		Observables
Development and distribution of organisms as decoys		One indicator would be evidence that an adversary had gained knowledge of the specific technology being used (e.g., stolen or missing data, devices, technical reports). Research on genetic manipulation of antigenic determinants or key signature sequences through recombinant technology would be relevant.
Accessibility	**Maturity**	**Consequence**
Level 3 (likely dedicated military laboratories)	Unknown	Spoofing of weapons of mass destruction sensors.

no risk to the adversary, but it would precipitate time-consuming responses in U.S. troops. The responses could include preparing medical units, delaying operations while time- and energy-consuming confirmatory tests are performed, and causing military personnel to put on protective gear that might impair mobility, comfort, and function. Such mimics would create reticence to enter certain areas. Similar approaches are applicable to chemical agents.

For decoys to be developed, the adversary would need to have knowledge of the methods and identifiers used by the sensors. For instance, mass spectrometry methods will identify signature peptides or protein or nucleic acid sequences, and immunologic detectors will identify specific protein antigens in the organism. (See Chart 6-5.)

SUMMARY

Biotechnology capabilities are rapidly expanding and becoming more and more readily available to scientists throughout the world. Emerging biotechnologies in functional brain imaging, communications, the spread of disabling infections, and sensor spoofing are likely to affect the conduct of military operations and the status of national security in the future. These biotechnologies have been highlighted in this chapter.

The neuroimaging techniques of EEG, MEG, fMRI, and NIRS provide direct measurement of brain function. Technology underlying these modalities is advancing rapidly to allow a multitude of measurements. These technologies may provide a better understanding of behavior, performance, readiness, and stress that is relevant to understanding the cultural differences in motivation and prisoner interrogation.

There are many opportunities on the horizon for biology to play a role in communications. These include protein cube holography and bacteriorhodopsin solid-state devices for storing high-density information, and DNA sequences as a medium for hiding covert messages.

DNA is currently available, capable of storing and communicating large amounts of hidden information, in a compact and stable medium as DNA itself or in the signal-to-noise ratio of sequence data. Work on bacteriorhodopsin has been ongoing for a substantial period, and genetic manipulation of this remarkable molecule continues to open new opportunities for its use. One of these uses is holography, but there are also other technologies that are maturing for embedding messages in holograms. The technology for reading holograms is the current limiting factor in exercising this potential.

Infectious diseases are a continuing concern. They offer opportunities for a wide range of genetic modifications and could be deployed in many different ways but were not a primary focus of this report. However, the current emphasis on weapons of mass destruction has led to the development of sophisticated sensors that, when activated, trigger responses that can be costly in time and can limit troop responses. A release of materials that trigger sensors, but are not threats, is one way of decreasing battle readiness in U.S. troops.

The area of application of biotechnology to military purposes is currently wide-ranging. It will expand very rapidly over the next decade.

REFERENCES

Hillebrecht, J.R., K.J. Wise, J.F. Koscielecki, and R.R. Birge. 2004. Directed evolution of bacteriorhodopsin for device applications. Methods in Enzymology 388:333-347.

McCarthy, M., M.K. Estes, and K.C. Hyams. 2000. Norwalk-like virus infection in military forces: Epidemic potential, sporadic disease, and the future direction of prevention and control efforts. Journal of Infectious Diseases 181(SUPP/2): S387-S391.

MMWR (Morbidity and Mortality Weekly Report). 2002. Outbreak of acute gastroenteritis associated with Norwalk-like viruses among British military personnel—Afghanistan, May 2002. June 7, Vol. 51, No. 22: pp. 477-479. Available online at http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5122a1.htm.

NRC (National Research Council). 2001. Opportunities in Biotechnology for Future Army Applications. National Academy Press, Washington, D.C.

Shen, Y., C.R. Safinya, and K.S. Liang. 1993. Stabilization of the membrane protein bacteriorhodopsin to 140 degree C in two-dimensional films. Nature 366(6450):48.

Wise, K.J., N.B. Gillespie, J.A. Stuart, M.P. Krebs, and R.R. Birge. 2002. Optimization of bacteriorhodopsin for bioelectronic devices. Trends in Biotechnology 20(9):387-394.

Wobus, C.E., S.M. Karst, L.B. Thackray, K-O. Chang, S.V. Sosnovtsev, G. Belliot, A. Krug, J.M. Mackenzie, K.Y. Green, and H.W. Virgin IV. 2004. Replication of norovirus in cell culture reveals a tropism for dendritic cells and macrophages. Public Library of Science Biology 2(12):e432.

7

Findings and Recommendations

This report identifies some of the major challenges confronting the intelligence technology warning community but makes no attempt to prioritize specific emerging technologies for more detailed analysis. Instead, the committee describes broad trends, discusses a prototype methodology that may be of value in focusing future collaborations, and "employs" that methodology on a disparate set of evolving technologies that may threaten U.S. military preeminence.

COLLABORATION WITH EXTERNAL SCIENTIFIC AND TECHNICAL COMMUNITIES

The committee postulated in Chapter 1 and illustrated in Chapters 3 through 6 that the information technology, biotechnology, microtechnology, and nanotechnology families will increasingly provide building blocks of a foundational nature for military-relevant capabilities for RED (adversarial) and BLUE (U.S. military) forces alike. The fact that significant advances in these technologies will be driven largely by commercial demand—on a global scale—rather than by military-specific investment suggests the need for the technology warning community to engage the nongovernmental scientific and technical community in order to bolster its understanding and anticipation of technology trends.

Finding 1: There is a multitude of evolving technologies for which advances are being driven by the nongovernmental, global, scientific and technical communities.

While globalization has been underway for several decades, its intensity and pervasiveness have greatly increased in magnitude and pace; the technology playing field is accordingly undergoing massive change. Technology research and development (R&D), historically dominated by the United States, is increasingly distributed. Small, research-seeded start-up companies are of special importance in the generation of high-technology ideas and products. What this means is that the U.S. defense establishment is no longer in the driver's seat with regard to militarily relevant technological innovation.

Recommendation 1: The Defense Intelligence Agency Technology Warning Division, together with the related intelligence community components that focus on technology warning, should establish an ongoing collaborative relationship with the scientific and technical communities in the industrial and academic sectors.

The National Academies, through the National Research Council, provide both a window into these communities and an appropriate institutional mechanism that could assist in this endeavor. This ad hoc committee, which will be disbanded with the publication of the present report, believes that a standing committee could more effectively support the needs of the Defense Intelligence Agency (DIA). The short-term effort of this committee was hampered by the lack of time to build a shared understanding of the Technology Warning Division's operating environment and to establish the collaborations necessary to adequately leverage the additional expertise readily accessible via the National Academies through the National Research Council. The establishment of a standing committee would help overcome these impediments and provide the foundation for an ongoing collaborative relationship.

INDICATORS RELATING TO GLOBALIZATION AND COMMERCIALIZATION

The forces of globalization and commercialization that are altering the world in terms of the potential for "technology surprise" require new approaches to the identification of indicators for providing technology warning. Throughout this report the committee focused largely on observables derived from open sources, but other potentially valuable sources exist (e.g., confidential discussions with industrial and academic researchers that may yield valuable insights for the technology warning community while protecting proprietary information). Although a diverse array of potential sources is identified in the preceding chapters, the individual sources were not vetted and the committee did not conduct a disciplined evaluation of the completeness of the array, nor did it make any effort to deconflict its sources with those already in use by the community.

Finding 2: New intelligence indicators are likely to be needed to provide technology warning for the diverse spectrum of evolving technologies that are being driven by commercial forces in the global marketplace.

Traditionally, the United States has assumed that it leads the world in science and technology. This perspective leads the technology warning community to look for indications that external actors are trying to "catch up," or to exploit known technologies in new ways. Projected future trends suggest that it should no longer be automatically assumed that the United States will lead in all relevant technologies. This revised perspective imposes a new burden on the technology warning community, generating the need for it to search in different places and in different ways to be able to warn against technological surprise.

Recommendation 2: The Defense Intelligence Agency Technology Warning Division, in collaboration with the related intelligence community components that focus on technology warning, should establish, maintain, and systematically analyze a comprehensive array of indicators pertaining to globalization and commercialization of science and technology to complement and focus intelligence collection and analysis.

The committee believes that the observables identified in this report provide a useful baseline. However, it acknowledges that the first step should be to decompose the broad trends into potential observables more systematically and then to evaluate the utility and applicability of techniques already in use in Open Source Intelligence analysis. For example, while patterns and trends in R&D investments provide useful indicators of the distributed research talent, the globalization of manufacturing facilities may indicate an equally important trend in distributing systems integration expertise. The committee acknowledges that not all important technological advances will occur in this arena, so long-standing approaches to detecting covert advances will continue to be important. However, the committee believes that trends in the global technology marketplace warrant focused strategies.

NEED FOR DISCIPLINED METHODOLOGY

As previously observed, the technology warning landscape is both diverse and complex—particularly given the need to consider not only discrete technologies but also innovative integration and application to multidisciplinary system capabilities. The committee believes that a systematic approach is needed to avoid the trap of simply generating more lists of technologies that will have military significance in the coming years. The committee recognizes, however, that too much rigor could effectively create a new set of blinders that could lead to future "failures of imagination."

Finding 3: The landscape of potentially important evolving technologies is both vast and diverse. A disciplined approach is thus needed to facilitate optimal allocation of the limited resources available to the technology warning community.

The committee reviewed a diverse array of lists of technologies—each prioritized from a different perspective. Some lists focus on potential "disruptive" technologies that could have catastrophic consequences in the hands of adversaries, while others focus on technologies with significant commercial potential that may erode the U.S. technological edge. The committee believes that the technology warning community would benefit from a disciplined approach to the identification and prioritization of the evolving technologies that may threaten U.S. military preeminence.

Recommendation 3: The Defense Intelligence Agency Technology Warning Division, in collaboration with the related intelligence community components that focus on technology warning, should adopt a capabilities-based framework within which to identify and assess potential technology-based threats.

The committee believes that a capabilities-based methodology enables a systematic approach to technology warning while reducing the tendency to focus only on advances in discrete technologies. The methodology presented as a prototype in this report was derived from Joint Vision 2020. It is offered as a starting point; the committee acknowledges that additional refinement is needed.

CONCLUSION

The technology warning community, which plays a vital role in advising military leadership, is facing unprecedented challenges. BLUE force strategies are increasingly dependent upon technology-

enabled capabilities assembled from building-block technologies in which U.S. technological leadership is no longer assured. Foreign governments and nonstate actors are gaining access to the same building-block technologies—often via the commercial marketplace. The committee applauds the Defense Intelligence Agency's recognition that unprecedented challenges require new collaborations and new approaches, and commends the efforts already underway.

Appendixes

Appendix A

Biographical Sketches of Committee Members

Ruth A. David, Chair, is the president and chief executive officer of ANSER, an independent, not-for-profit, public-service research institution. In November 1999, Dr. David initiated ANSER's Homeland Defense Strategic Thrust to address the growing national concern of multidimensional, asymmetric threats from rogue nations, substate terrorist groups, and domestic terrorists. In May 2001, the ANSER Institute of Homeland Security was established to enhance public awareness and education and contribute to the dialog on a national, state, and local level. From September 1995 to September 1998, Dr. David was deputy director for science and technology at the Central Intelligence Agency. 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. She represented the CIA on numerous national committees and advisory bodies, including the National Science and Technology Council and the Committee on National Security. Previously, Dr. David served in several leadership positions at the Sandia National Laboratories, where she began her professional career in 1975. Most recently, she was director of advanced information technologies. From 1991 to 1994, Dr. David was director of the development testing center that developed and operated a broad spectrum of full-scale engineering test facilities. Dr. David is a member of the Department of Homeland Security Advisory Council, the National Academy of Engineering (NAE), and the Corporation for the Charles Stark Draper Laboratory, Inc. She is vice chair of the HSAC Senior Advisory Committee of Academia and Policy Research and serves on the National Security Agency Advisory Board, the National Academy of Engineering Committee on Engineering Education, the American Association for the Advancement of Science Committee on Scientific Freedom and Responsibility, the Jet Propulsion Laboratory's Technical Division's Advisory Board, and the External Advisory Committee for Purdue University's Homeland Security Institute. Dr. David is a former adjunct professor at the University of New Mexico and has technical experience in digital and microprocessor-based system design, digital signal analysis, adaptive signal analysis, and system integration. Dr. David received a B.S. degree in electrical engineering from Wichita State University (1975), an M.S. degree in electrical engineering from Stanford University (1976), and a Ph.D. in electrical engineering from Stanford University (1981).

Steven R.J. Brueck is the director of the Center for High Technology Materials (CHTM) and is a professor of electrical and computer engineering and a professor of 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 Association for the Advancement of Science, the American Physical Society, and the Materials Research Society, a fellow of the Institute of Electrical and Electronics Engineers, and a fellow of the Optical Society of America.

Stephen W. Drew holds consultancies with a variety of pharmaceutical and biotechnology organizations. Until 2000, he worked with Merck & Company, Inc., in a series of increasingly responsible positions culminating with distinguished senior scientist. He held vice presidential positions of responsibility in the Merck Manufacturing Division (MMD) as the vice president of Vaccine Science and Technology, vice president of Vaccine Operations, and vice president of Technical Operations and Engineering. Prior to joining MMD 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 a 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 and has launched two companies that service the pharmaceutical and biotechnology industries.

Alan H. Epstein received his B.S., M.S., and Ph.D. degrees from the Massachusetts Institute of Technology in aeronautics and astronautics. He is a member of the National Academy of Engineering (NAE) and is currently the R.C. Maclaurin Professor of Aeronautics and Astronautics and the director of the Gas Turbine Laboratory at the Massachusetts Institute of Technology. His responsibilities include teaching and research in aerospace propulsion, fluid mechanics, power production, and microelectromechanical systems (MEMS). He has been an active consultant to industry and government for more than 25 years—his activities have included gas turbine design and operation, MEMS, system testing and advanced instrumentation, military infrared systems, and vehicle observable technology. Dr. Epstein is a fellow of the American Institute of Aeronautics and Astronautics and a member of the NRC Army Science Board and of the DARPA Defense Science Research Council.

Robert A. Fuhrman is retired vice chairman of the board, president, and chief operating officer of Lockheed Corporation, and past chair of the Air Force Science and Technology Board. He has had a distinguished career, having served as Lockheed's president and chief operating officer and group president for missiles and space, as well as in numerous other positions. Mr. Fuhrman received his B.S. degree in engineering from the University of Michigan and his M.S. in fluid mechanics and dynamics from the University of Maryland. Mr. Fuhrman serves on numerous boards and is a member of many professional societies. He is a member of the National Academy of Engineering, an AIAA honorary fellow, and a former member of the Defense Science Board.

Sharon C. Glotzer is an associate professor of chemical engineering, materials science and engineering, physics, and macromolecular science and engineering at the University of Michigan. She worked previously at NIST, where she was co-founder and director of the Center for Theoretical and Computational Materials Science. She is a recipient of a Presidential Early Career Award and the APS Maria Goeppert-Mayer Award, a Department of Commerce Bronze Medal Award, and an NRC postdoctoral fellowship, and was a Sigma Xi Distinguished Lecturer from 2000 to 2003. She is an active member of the APS, AIChe, MRS, ACS, and AAAS; Dr. Glotzer is first vice chair for the Nanoscale Science and Engineering Forum of the AIChE and vice chair of the Forum on Industrial and Applied Physics of the APS. Dr. Glotzer has presented well over 100 invited presentations and keynote talks at conferences and national professional society meetings and has served as a reviewer of NRC reports. She received her B.S. degree in physics from the University of California, Los Angeles, and her Ph.D. in physics from Boston University.

Christopher C. Green is currently executive director of emergent technologies research at Detroit Medical Center, Wayne State School of Medicine. He is also a fellow in neuroimaging and an assistant professor in the Department of Radiology and the Department of Psychiatry and Behavioral Neurosciences. He is chair of the Joint Independent Science Panel Office/Undersecretary of Operations Research, Department of the Army, and a member of the Medical Subcommittee, Local Emergency Planning Committee, State of Michigan Regional Homeland Defense. He serves on many biotechnology and medical boards of directors. Immediately prior to his current position, he was executive director for both Global Emerging Technology Policy (in GM's Public Policy Center) and also the chief technology officer and executive director of regional science and technology (for GM Asia Pacific Operations). He managed formulation of corporate policy directives in newly emergent issues of health and safety and industrial medicine, and numerous occupational medical research programs. His distinguished career with the CIA extended from 1969 to 1985 as a senior division analyst with the Office of Scientific and Weapons Intelligence. In this role he obtained multidisciplinary research and management experience in medicine, comparative biology, bioengineering, animal and human physiology, endocrinology, and life sciences. Special areas of management experience included the direction of research of doctoral-level and physician scientists in the above areas as well as participation as a senior analyst. He continues as an agency consultant. His medical specialty is forensic medicine and toxicology, and his doctoral research work in neurophysiology concerned human biochemical functioning of the brain, with a focus on functional brain imaging and clinical MRI. Dr. Green was an analyst with the Life Sciences Division, Chief of the Biomedical Sciences Branch/LSD, and deputy division chief. He became a senior division analyst with the newly formed Office of Scientific and Weapons Intelligence in 1978. He received his bachelor's degree from Northwestern University in pre-med, his Ph.D. from the University of Colorado Medical School in neurophysiology, and his M.D. from the Autonomous City University in El Paso, Texas/Monterey, Mexico, with honors. He also holds the National Intelligence Medal.

Diane E. Griffin is professor and chair of the Department of Molecular Microbiology and Immunology and director of the Johns Hopkins Malaria 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 interest includes 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, is the author or co-author of a number of scholarly papers and articles, is the past president of the American Society for Virology, and is the current president of the Association of Medical School Microbiology Chairs.

J. Jerome Holton is the director of Technical Research, Analyses and Communications with Defense Group, Inc. In this position he is responsible for DGI's branding, strategic planning, and positioning in the government support sector, including the policy, technology, and operations issues for weapons of mass destruction (WMD) 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 counter-proliferation of, counterterrorism/domestic preparedness issues 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 with the National Academies as a member of the Committee on Alternatives to Anti-Personnel Landmines and as a reviewer for the NRC report *Army Science and Technology for Homeland Security*. He earned his Ph.D. in experimental physics from Duke University.

Michael R. Ladisch is the director of the Laboratory of Renewable Resources, Engineering Department, and Distinguished Professor of Agricultural and Biological Engineering and Biomedical Engineering at Purdue University. He earned his B.S. degree from Drexel University and M.S. and Ph.D. degrees from Purdue University, all in chemical engineering. His areas of expertise are bio-separations, bio-nanotechnology bioprocess engineering, and bio-energy. His research has resulted in systematic approaches and correlations for scaling up chromatographic purification techniques from the laboratory to process-scale manufacturing systems. He is currently investigating the scale-down of bio-separations and the rapid prototyping of microfluidic biochips for the rapid detection of pathogenic microorganisms. He is familiar with biotechnologies and has a broad background in bioscience and bioengineering. His work has resulted in 150 publications, a textbook on bioseparations, 14 patents (issued and applied for) and over 100 presented papers at national professional society meetings, and he has been the recipient of numerous research and teaching awards. He was elected to the National Academy of Engineering in 1999 for developing and scaling up new approaches and materials for process chromatography, adsorptive bioseparations, and biocatalysis. He has served as a member of U.S. delegations and advisory panels to Russia, Thailand, China, and Japan to review the status of biotechnology programs. He has also chaired several committees within the National Research Council concerning biotechnology.

Darrell D.E. Long is professor of Computer Science at the University of California, Santa Cruz and director of the Storage Systems Research Center in the Jack Baskin School of Engineering. He has broad research interests in the area of computing systems, including operating systems, distributed systems,

high-performance storage systems, fault tolerance, performance evaluation, and mobile computing. He received his B.S. degree in computer science from San Diego State University in 1984 and his M.S. and Ph.D. degrees in computer science and engineering from the University of California, San Diego in 1986 and 1988, respectively. He is a member of the Association for Computing Machinery and of the Usenix Association, where he serves as the chair of the Scholars Committee, and he is a senior member of the IEEE Computer Society, for which he has served as chair of the Technical Committee on Operating Systems, and now serves on the Executive Committee of the Technical Committee on Operating Systems. He also serves on the National Security Panel and Intelligence Subpanel for Los Alamos and Livermore National Laboratories.

Frederick R. Lopez has a 33-year career as an engineer with McDonnell-Douglas Aircraft Company and Raytheon Company. He is also a retired brigadier general, United States Marine Corps Reserves. Currently, he is the director of engineering for Raytheon Electronic Warfare Systems in Goleta, California. General Lopez is 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 and service as an Infantry Officer with Master Parachutist Qualification, 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 27 years in the U.S. Marine Corps Reserve. General Lopez received a B.S. degree in mathematics from California State Polytechnic College and his M.S. in computer science from West Coast University, Orange, California.

Richard M. Osgood, Jr., joined Columbia University in 1981 and became Higgins Professor of Electrical Engineering and Applied Physics in 1988. From 2000 to 2004, he served as associate laboratory director at Brookhaven National Laboratory. Dr. Osgood was, with Professor Yang, a co-founder of the Columbia Microelectronics Sciences Laboratories (MSL) and has served as director or co-director of MSL and the Columbia Radiation Laboratory (CRL). He is a member of the ACS and the MRS and a fellow of the IEEE and OSA. He was co-editor of *Applied Physics* (1983-1995) and associate editor of the *IEEE Journal of Quantum Electronics* (1981-1988). Dr. Osgood serves as a consultant to numerous research institutions and government agencies, including MIT Lincoln Laboratory. He was also on the DARPA Defense Sciences Research Council (Materials Research Council) and the Los Alamos National Laboratory Visiting Advisory Board (Chemical Sciences and Technology Division). Dr. Osgood has served as councilor of the Materials Research Society and as a member of the DOE Basic Energy Sciences Advisory Committee. In 1991, Dr. Osgood received the R.W. Wood Award from the Optical Society of America and was invited to deliver the OIDTA lecture at the Japanese Optical Association. His research interests include integrated optical devices and design, surface physics, and laser sources. He received his B.S. degree from the U.S. Military Academy, his M.S. in physics from Ohio State University, and his Ph.D. in physics from Massachusetts Institute of Technology.

Stewart D. Personick is a member of the Board of Directors of Optical Communications Products, Inc., a member of the U.S. Federal Communications Commission's Technological Advisory Council, and a consultant to industry in the field of telecommunications and networking. From September 1998 to August 2003, he was the E. Warren Colehower Chair and Professor of Telecommunications at Drexel

University and the director of Drexel's Center for Telecommunications and Information Networking. From 1970 to 1985 he worked as an individual contributor, and as a research manager (Bell Laboratories, TRW, Bellcore), in the field of optical communications technology and applications. Since 1985 he has focused his research and management activities on emerging and next-generation telecommunications systems, technologies, and applications. He was a vice president, in charge of a wide variety of research and systems engineering efforts, at Bellcore (now Telcordia Technologies) from September 1985 to July 1998. He also served as the senior management link from Bellcore and its telecommunications industry clients to the emerging Internet community. He served as a member, and as chair, of the U.S. Federal Networking Council Advisory Committee during the critical transition of the NSFnet to the current set of commercial and federally sponsored networks. He holds a B.E.E. (1967) from the City College of New York/CUNY, and an S.M. (1968) and an Sc.D. (1970) from the Massachusetts Institute of Technology. He is a fellow of the IEEE (1983), a fellow of the Optical Society of America (1988), and a member of the U.S. National Academy of Engineering (1992). He received the IEEE/OSA John Tyndall Award in 2000 in recognition of his pioneering contributions to optical fiber communications technologies, systems, and applications.

Alton D. Romig, Jr., is currently vice president, Nonproliferation and Assessments, at Sandia National Laboratories, Albuquerque, New Mexico. His responsibilities include the leadership and management of the development and engineering activities that provide systems, science, technology, and expertise in support of national objectives to reduce the threat to the United States from proliferation and use of weapons of mass destruction. Program areas include remote sensing, proliferation assessment, intelligence activities, international security, physical security, and nuclear/chemical/biological nonproliferation and counterintelligence. Dr. Romig is a member of the National Academy of Engineering and is active on a number of National Academy of Engineering/National Research Council committees and boards. He is a fellow of the American Association for the Advancement of Science (AAAS) and TMS (The Metals, Minerals and Materials Society). Dr. Romig is also a fellow and former president of ASM, International (formerly, American Society for Metals). He also serves on the boards of Atomic Weapons Establishment Management Limited, a Lockheed Martin joint venture company in the United Kingdom, and Technology Ventures Corporation, a Lockheed Martin subsidiary dedicated to technology commercialization. For his pioneering work in analytical electron microscopy and solid-state diffusion, Dr. Romig has received several awards, including the Burton Medal (1988), awarded by the Electron Microscopy Society of America to an Outstanding Young Scientist; the K.F.J. Heinrich Award (1991), given by the Microbeam Analysis Society to an Outstanding Young Scientist; the ASM Silver Medal for Outstanding Materials Research (1992); and the Acta Metallurgica International Lectureship (1993-1994). Dr. Romig has also been named the 2003 ASM-TMS Distinguished Lecturer in Materials and Society. He received his B.S., M.S., and Ph.D. degrees in materials science and engineering from Lehigh University in 1975, 1977, and 1979, respectively. In 1979, he joined Sandia National Laboratories as a member of the technical staff, Physical Metallurgy Division. After a variety of management assignments, he was named director, Materials and Process Sciences, in 1992. From 1995 to 1999, he was director of Microsystems Science, Technology, and Components. In 1999, he was named chief technology officer and vice president for Science, Technology, and Partnerships. In that role, he was chief scientific officer for the Nuclear Weapons program, accountable for Sandia's interactions with industry and the Laboratories' Campus Executive program. In addition, he was responsible for the Laboratory Directed Research and Development program. He served in this capacity until attaining his present position in 2003.

S. Shankar Sastry was chair of the Department of Electrical Engineering and Computer Sciences at the University of California, Berkeley from 2001 to 2004. The previous year, he served as director of the Information Technology Office at DARPA. From 1996 to 1999, he was the director of the Electronics Research Laboratory at Berkeley, an organized research unit on the Berkeley campus conducting research in computer sciences and all aspects of electrical engineering. He is currently the NEC Distinguished Professor of Electrical Engineering and Computer Sciences and a professor of bioengineering. Dr. Sastry received his Ph.D. degree in 1981 from the University of California, Berkeley. He was on the faculty of MIT as an assistant professor from 1980 to 1982 and at Harvard University as a chaired Gordon McKay professor in 1994. He has held visiting appointments at the Australian National University, Canberra, the University of Rome, Scuola Normale, and the University of Pisa, as well as at the CNRS laboratory LAAS in Toulouse (poste rouge), as professor invite at Institut National Polytechnique de Grenoble (CNRS laboratory VERIMAG), and as a Vinton Hayes visiting fellow at the Center for Intelligent Control Systems at MIT. His areas of research are embedded and autonomous software, computer vision, computation in novel substrates such as DNA, nonlinear and adaptive control, robotic telesurgery, control of hybrid systems, embedded systems, sensor networks, and biological motor control. Dr. Sastry has served as associate editor for numerous publications, including *IEEE Transactions on Automatic Control, IEEE Control Magazine; IEEE Transactions on Circuits and Systems*; the *Journal of Mathematical Systems, Estimation and Control*; IMA *Journal of Control and Information*; the *International Journal of Adaptive Control and Signal Processing*; and the *Journal of Biomimetic Systems and Materials*. He has coauthored over 300 technical papers and books. Dr. Sastry was elected to the National Academy of Engineering in 2001 and the American Academy of Arts and Sciences in 2004. He also received the President of India Gold Medal in 1977, the IBM Faculty Development Award for 1983–1985, the NSF Presidential Young Investigator Award in 1985, the Eckman Award of the American Automatic Control Council in 1990, an M.A. (honoris causa) from Harvard University in 1994, election as a fellow of the IEEE in 1994, the distinguished Alumnus Award of the Indian Institute of Technology in 1999, and the David Marr Prize for the best paper at the International Conference in Computer Vision in 1999.

James B. Smith is vice president of Precision Engagement at Raytheon. Precision Engagement is a Raytheon Company strategic business area (SBA) that draws on the capabilities of the entire company. Precision engagement is the ability to locate, discern, and track objectives or targets; to employ the best systems available to achieve the desired effects; to assess results; and to reengage with decisive speed and overwhelming operational tempo as required. Precision engagement is effects-based engagement, relevant to all types of operations. Prior to his current position, he served as director of Navy C2 programs, Lockheed Martin Mission Systems. He retired from the U.S. Air Force as a brigadier general and served as commander, Joint War Fighting 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 and the modeling, simulation, and deploying of solutions that demonstrated a high probability of operational success. A carrier fighter pilot, General Smith logged nearly 4000 flight hours in the F-15 and T-38 and flew combat missions during the Gulf War. He is a graduate of the U.S. Air Force Academy with a bachelor's degree in military history; he holds a master's degree in history from Indiana University.

Camillo J. Taylor is currently an associate professor in the Computer and Information Science Department of the University of Pennsylvania. His research interests include reconstructing and rerendering three-dimensional images from two-dimensional images and vision-guided robotic systems. He has

refereed many journal publications with the most recent being "A Vision-Based Formation Control Framework." His most recent of the many refereed conference proceedings is "Camera Trajectory Estimation using Inertial Sensor Measurements and Structure from Motion Results." Dr. Taylor received his A.B. degree in electrical computer and systems engineering from Harvard College, his M.S. degree in computer engineering from Yale University, and his Ph.D. in electrical engineering from Yale University. He is a member of the Institute of Electrical and Electronics Engineers and the Association for Computing Machinery and has received numerous awards throughout his career.

Dianne S. Wiley is a Boeing Technical Fellow for Space Exploration Systems, NASA Systems, Washington, D.C. 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 the 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 this 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 B

Presentations to the Committee

MEETING 1, WASHINGTON, D.C., AUGUST 3–4, 2004

Technology Warning Division DWO-4
Steve Thompson
Defense Intelligence Agency

Contract Vectors
Deems Emmer
Defense Intelligence Agency

ALO/UAV Futures Technologies Experiment
Ever Morales
Defense Intelligence Agency

Integration of Technologies into Weapons
Glen Simpers
Defense Intelligence Agency

Bridging the Science and Technology and Intelligence Communities: Assessing the National Security Significance of International Science and Technology
Gerald Epstein
The Center for Strategic and International Studies

MEETING 2, WASHINGTON, D.C., OCTOBER 27–28, 2004

What Appears to Be "Happening"?
Dennis Bushnell
NASA Langley Research Center

Biodefense Medical Products
Erik Henchal
U.S. Army Medical Research Institute of Infectious Diseases

NTAs and Chemical Threats
Thomas Cao
U.S. Army Dugway Proving Ground

How Do I Know I Am Sick
Robert Armstrong
National Defense University

MEETING 3, WASHINGTON, D.C., JANUARY 12–13, 2005

Indicators and Warnings
John Gannon
Select Committee on Homeland Security

Thoughts on Information Assurance Threats in a Net-Centric Environment
Neal Smith
National Security Agency

NIC Civil Science and Technology Portfolio
Rich Engle
National Intelligence Council

Science and Technology Intelligence
Charles Clark
Weapon and Space Systems Intelligence Committee

Appendix C

Background Material for Chapter 1

This appendix provides definitions of the 26 key technologies listed in Box 1-1 in Chapter 1 of this report. The definitions, arranged here in alphabetical order, are quoted from a 2001 study sponsored by the Central Intelligence Agency (OTI IA, 2001). In that study, a panel of experts identified three tiers of technologies (see Box 1-1 in Chapter 1) likely to impact national security by the 2015 time frame.

Advanced Materials: Development of materials, generated at the micro level, that are the building blocks for stronger, more efficient physical structures of all sizes. These materials are not inherently mechanical systems (such as MEMS) but are building blocks that can be combined to produce physical systems of greatly increased physical strength or other highly desirable attributes (e.g., electrical conductivity).

Alternative Energy: Development of energy from a source that can be replenished or that replenishes itself, such as solar and wind energy, and is generally environmentally less harmful than 'traditional' energy sources. This excludes fuel cells and nuclear power. Electrical energy—once generated—may be used in a variety of applications including transportation, manufacturing, or energy weapons applications.

Brain-Machine Interfaces: Development of computers with wide-ranging interfaces that will ultimately include pointing, gesturing, and other forms of communication, allowing substantive human-computer interactions without the need for physical contact. This will require complex integration of speech recognition, natural-language processing, speech analysis, knowledge-based reasoning ability, and speech generation.

Cloned or Tailored Organisms: Organisms that are genetically modified to produce repeatable characteristics. These may be animals or plants used as source material for medical purposes or food sources. Productivity associated with plant and livestock production is significantly increased in these products.

Directed Energy (Microwave): Development of high-power directed energy systems (excluding lasers) that allow for the coherent (no diffusion) transmission of energy (at the "megawatt" level) in the radio

frequency (RF) spectrum. These may be used as weapons or as alternate (nonwire-based) methods of energy transmission, including transmission of energy to and from space.

Distributed Energy: Development of small-scale, efficient, stationary, energy-generation technologies that use a variety of fuels and technologies (natural gas, solar energy, and fuel cells). These generation systems are distributed in homes, businesses, and workplaces such that existing large conventional power generation systems are secondary. The resulting energy grid has much higher levels of reliability and efficiencies because of fewer transmission losses.

Distributed-Grid-Based Processing Systems: A type of computing in which different components and objects comprising an application can be located on different computers connected to a network. It requires a set of standards that specify how objects communicate with each other. Distributed computational systems, in combination with multiagent software, can achieve extremely high processing levels.

Efficient Software Development: Development of significant enhancements in algorithm designs and development, testing, and production of software such that the human labor and time required for developing complex code are greatly reduced and a much more efficient use is made of computer processing capability.

Fuel Cells: Development of efficient, safe, cost-effective hydrogen, natural gas, or other, not yet identified, fuel cells. These devices would produce electricity through chemical processes. Fuel cells are in limited use today in a variety of applications, such as automobiles.

Gene Therapy: The treatment of disease by either replacing damaged or abnormal genes with normal ones or providing new genetic instructions to help fight diseases such as cancer.

High-Power Lasers: Development of high-power directed energy lasers that allow for the coherent (no diffusion) transmission of energy (at the "megawatt" level) in the "laser" portions (Infrared [IR], near IR, visual) of the RF spectrum. These may be used as weapons or as alternate (nonwire-based) methods of energy transmission, including transmission of energy to and from space.

Hypersonic/Supersonic Aircraft: Development of propulsion, fuels, and materials to allow for sustained routine military hypersonic and/or commercial supersonic flight. This would allow transcontinental movement of personnel, weapons, and equipment in far less time.

Image Understanding: This consists of automatic target recognition and machine vision. It involves achieving rapid and accurate pattern recognition of shapes using machine-processed sensor data, then using the recognized pattern to identify and track objects. Such systems provide high reliability for machine (weapon) recognition of shapes and objects and enable the military to identify, assess, and track targets.

Microelectromechanical Systems (MEMS): MEMS technology is the integration of mechanical elements, sensors, actuators, and electronics on a silicon substrate. Current applications include ink jet printer heads, sensitive pressure and mass sensors, accelerometers for airbag deployment, and MEMS-based moving mirrors as switches to fiber-optic telecommunications networks. Future devices could be based on polymers, with their raw materials far less expensive and less equipment intensive for manufacturing than current materials. The most promising area for application of polymer MEMS is in biomedicine.

Molecular Electronics (or "moletronics"): Electronic transport through individual molecules. Speculative applications include low-power logic in circuits, simplified high-speed memory, and cellular automata and neuromolecular networks in computers or other information technology devices.

Multilingual Voice Recognition: Development of computer systems that can recognize spoken words in various languages. Such systems can be distributed so that language no longer becomes a barrier in human interactions.

Nanotechnology: The ability to measure, manipulate, and organize matter on a nanoscale—1 billionth to 100 billionths of a meter. This will lead to dramatic changes in the way materials, devices, and systems are understood and create major developments in areas such as computer efficiency, human organ restoration, and "designer" materials.

New-Generation Nuclear Power Plants: Development of safe, environmentally improved, and cost-competitive electrical power generation from nuclear processes (fission and possibly fusion).

Next-Generation Space Shuttle System: Development of propulsion, fuels, and materials for routine sustained military and/or commercial travel into space. This may be a fully reusable two-stage-to-orbit vehicle with Concorde-like flight operations.

Optical Communications: Development and use of optical signal generation, amplification, switching, and transmission of communications data. A complete "optical pipe" enhances the efficiency (speed and volume) of communications streams.

Performance-Enhancing Drugs: Development of mental and physical performance-enhancing drugs such that human physical or cognitive ability is increased in a clearly measurable way (more than 10 percent) across the entire age spectrum.

Regenerative Medicine (including tissue engineering): Development of procedures to grow human and animal organs, skin, and cartilage for health-care purposes and for the production of food, clothing, and many other products. Includes development and manipulation of laboratory-grown molecules, cells, tissues, or organs to replace or support the function of defective or injured body parts.

Sensor Webs: Development of complex arrays and networks of sensors that could be used both in space for strategic needs and at the lowest echelons for urban warfare. One example would be the deployment of a large constellation of synthetic aperture radar imaging satellites to provide nearly real-time world-wide coverage. All information from sensors is relayed to a central uplink, where information is uploaded into a computer and analyzed.

"Smart" Materials (organic and inorganic): Development of materials that have internal sensing and adjustment mechanisms such that they can repair themselves if damaged or if structural integrity is threatened or reduced. Organic materials for control of biological systems (sewage treatment and photo-synthesis) have self-contained feedback mechanisms to respond to changes in the environment so the overall process is sustained or improved.

Ubiquitous Water Generation: Development of economical, clean, safe, potable water. This water has been through the flocculation, filtration, disinfection (via chlorine or ozone), and fluoridation processes. The technology includes developments in desalinization; such techniques may or may not depend on development of new energy sources.

Wireless Communications: A control system or communications system in which electromagnetic or acoustic waves transmit a flow of data or a signal through air or space instead of through wire or cable. In most cases, RF or IR signals are used. Typical wireless equipment used today are wireless local area networks, global positioning systems, cellular telephones, personal pagers, cordless computer accessories like IR mice and keyboards, home entertainment remote controls, garage door openers, and two-way walkie-talkies. Portions of systems with a large geographic influence may continue to use fiber and cable.

REFERENCE

OTI IA (Office of Transnational Issues, Intelligence Analysis). 2001. Global Technology Scenarios Through 2015: America's Game to Lose. OTI IA 2001-083. CIA Analytic Report. November.

Appendix D

Background Material for Chapter 3

COMMUNICATIONS

Modern communications networks are composed of many links: satellite communication channels provide high-bandwidth pathways within and between continents, cable and fiber channels provide secure high-bandwidth channels over long distances, and radio links of various kinds serve to connect personnel and equipment over short, medium, and long ranges. Each type of link has its own advantages and disadvantages and is vulnerable to different forms of exploitation and attack. A variety of reports published by the National Research Council (NRC) and others discuss these and related topics (NRC, 1991, 1996a,b, 1997, 1998, 1999, 2001, 2002).

Communications networks using the Internet Protocol (IP) stack form the basis of network-centric warfare. While IP networks can operate using a heterogeneous set of techniques for moving the data, the protocols are common to all technologies and present a common set of vulnerabilities that might be exploited by an adversary. Attacks on the protocols themselves, or attacks on the environment based on assumptions made by the protocols, leave them vulnerable to disruption. Attacks on the protocols are well known and have been described in the literature on networking, as have attacks based on the way the protocols operate (e.g., denial-of-service attacks).

The ability to secure communication channels with encryption is clearly a crucial capability. Without this protection RED forces would be able to intercept or exploit information relayed between various divisions of the armed forces, much as the Allied forces were able to intercept Axis radio transmissions during World War II. It is already the case that certain types of encryption technology are subject to stringent export controls under existing laws. However, much of the basic knowledge about cryptographic schemes is commonly available in the public domain. Cryptographic research has been described in the open literature along with the revolution in computing technology that has enabled it.

The newest encryption standard, Rijndael, or the Advanced Encryption Standard (AES; FIPS-197) replaces the Data Encryption Standard (DES) that is now regarded as vulnerable (NIST, 2000). It is important to note that the government did not develop the data encryption algorithm that will be used for most data. The technical skills required to implement secure communication schemes are taught in

undergraduate computer science courses and so are available in many parts of the world. This implies that opposing forces could readily encrypt their own transmissions if they chose to do so. Such encryption can also be expected to be very strong, and difficult or impossible to break using known methods. Programs such as Pretty Good Privacy (PGP) and Gnu Privacy Guard (GnuPG), which can be obtained over the Internet by anyone, provide essentially unbreakable security if used properly.

COMPUTATION

Computational systems are used to process the data gathered by sensor systems and human agents and to produce information that can be used by decision makers in command centers and on the field. As the armed forces become increasingly networked and more data become available online, BLUE forces will rely increasingly on computational systems to sift through the available information to provide situational awareness and to identify patterns. Computational systems are also used to automate difficult or tedious decision processes. Logistic operations, for example, can be optimized through the use of automated planning and scheduling systems.

The economies of scale and competitive pressures in the commercial computer sector have produced a situation where processing power has become a commodity. Powerful 32- and 64-bit microprocessors are produced at low cost both domestically and internationally. One result of this trend is that it has become much simpler for other nations to acquire state-of-the-art computational capabilities. Consider the fact that the majority of the supercomputers in the Top 500 listing are composed of collections of standard microprocessors lashed together with high-performance networks.

It will always be the case that the most demanding computational applications such as image interpretation, automated language translation, data mining, and so on will fuel the drive for ever increasing processing power. However, the skills and components required to construct powerful computational clusters are now widely available internationally.

It is not only access to high-performance computing that is a concern. Increasingly, low-power electronics is an area of active research and development that will be especially important in the area of sensor networks. To provide increased intelligence at the sensor and to reduce the demands on the network, a significant amount of processing will have to occur at the sensor; such processing power is enabled by low-power electronics.

As the price of computing hardware has dropped, the relative importance of software has increased. At this point, some of the most significant technical challenges in implementing the vision of the Future Combat Systems program center on the issue of developing reliable software systems that can coordinate distributed networks of sensors, actuators, and computers into a seamless whole. This task is complicated by the fact that the systems are expected to work in a dynamic environment in which elements may be added or removed unexpectedly and communications are not assured. In this regard, research and development being carried out in distributed systems, grid computing, and sensor networks should be viewed as germane to the military context.

The ability to produce and maintain sophisticated software systems relies on the availability of skilled personnel, programmers, analysts, testers, and others. Here again, it is the case that human resources are available internationally. China, for example, currently graduates five times more engineers than does the United States. The Indian city of Bangalore now has more technology jobs than Silicon Valley. In the face of current worldwide trends, it is unlikely that BLUE forces will have a significant advantage in terms of their ability to design, deploy, and operate the computational infrastructure required to support information collection and exploitation. The number of trained software engineers is declining in the United States but is increasing rapidly in countries in Asia.

SENSING AND SENSORS

Information dominance hinges on the ability to collect tactically relevant information in a timely manner. This information can be derived from a variety of sources. Standoff sensors mounted on satellite platforms or aircraft provide a relatively noninvasive means of assessing the tactical situation in remote locations. A variety of sensors have been successfully deployed on these platforms, ranging from passive imaging sensors that can collect measurements in a range of spectral bands to active sensors that can be used to identify camouflaged vehicles or to produce accurate elevation maps of remote sites. As useful as these standoff sensors are, they can be confounded by bad weather, limited resolution, and camouflage.

Radar systems are also an important component of situational awareness and are commonly used to identify and localize aircraft and to provide a comprehensive understanding of the airspace in the theater of operations. Synthetic aperture radar (SAR), for example, has proved useful in a variety of applications.

On the battlefield, useful information can be derived from a variety of sensors, including chemical sensors, cameras, thermal sensors, and acoustic sensors. It is becoming increasingly attractive to consider deploying collections of small, low-power computational elements equipped with sensors and wireless communication systems that could provide information about a given area of interest. A compelling example is the recent development of acoustic sensor arrays for the detection and localization of sources of gunfire. Also beginning to become available are inexpensive biological sensors. The development of DNA microarray chips, for example, promises to provide inexpensive, rapid identification of biological samples.

A large, redundant multiplicity of sensors is typically deployed to ensure the information dominance on which U.S. forces are now heavily reliant—ranging from space-based sensors to those deployed on unmanned aerial vehicles (UAVs) to smart dust. It is often the case that sensor systems will be deployed in conjunction with communication systems that are used to correlate information obtained in various locations or to transmit sensor information to decision makers in command centers or on the field. Relevant information can also be derived from radio systems that can be used to intercept transmissions or to pinpoint the location of transmission stations, radar installations, or jammers.

Remote Sensing

Remote sensing is watching and listening to the actions of the enemy from a distance. Examples include radar (watching using electromagnetic waves) and sonar (listening using acoustic waves) and can be further divided into active and passive categories as discussed below. The basic functionality is to stand off from the action and monitor the battlespace or the environment for telltale signs of enemy activity. Sensors operate in the range from ultraviolet (UV) to radio frequency (RF) as elucidated below.

- *Active sensing* involves sending out a probe and monitoring a response. The classic example of active sensing is radar—a pulse is transmitted and various modalities of scattered or reflected energy are monitored. The information return can be very rich, as in the case of spectroscopic probing of, for example, molecular species in the infrared (IR) or biological species with a UV excitation. In optimal circumstances, active sensing provides enhanced sensitivity and/or range compared with passive techniques. The disadvantage, of course, is that the enemy can also see the associated emissions and can, in the worst case, direct fire to destroy the sensing capability—and possibly its operators.
- *Passive sensing* relies on detection of natural emissions, such as thermal emissions, muzzle flashes, rocket or airplane exhaust, and so on. Passive sensing is more likely to be covert; there

are weak or no emissions from the detection apparatus in comparison with active sensing. The disadvantage is that the signals are weaker and usually exhibit lower specificity and/or discrimination than that achieved with active sensing. It may be possible to opportunistically take better advantage of ambient signals already available in the environment, such as those from television and radio stations that radiate at high power and at known frequencies. With more sophisticated signal-processing techniques, it may be possible to use these sources in much the same way that active sensing would be used.

Sensor Systems

Synthetic Aperture Radar

Synthetic aperture radar (SAR) is an electronic imaging technology that was introduced in the early 1950s. Its invention is generally credited to Carl Wiley, a U.S. engineer who was then working at the Goodyear facility in Arizona. SAR involves the collection of a set of microwave pulses transmitted and received, from reflection off Earth's surface, from an aircraft or a spacecraft as it moves along a flight path. This collection of received radar echoes forms a phase-history data set, which can be processed by a digital computer into an image of the portion of the ground that is illuminated by the craft's radar antenna beam. SAR filled at least two gaps that were inherent in the capabilities of conventional optical imagers: namely, operation at night and operation in all-weather conditions. With the advent of this type of radar imaging, the various vehicles on a battlefield (at least the stationary ones) could be located by an aircraft carrying a SAR at any time of day or night, and even in the presence of clouds, smoke, or dust.

The most significant limitation of the first SAR imagers was that of relatively poor spatial resolution. Early SARs achieved only several meters of resolution, which could allow an image analyst to delineate large features on Earth's surface but would not, for example, allow one to distinguish a tank from an ambulance on the battlefield. Fifty years later, state-of-the-art SARs typically produce imagery with spatial resolution at a level of several inches, so that vehicle identification is now feasible. Several key developments during the past 20 years have led to this ability of SARs to achieve such a high level of spatial resolution. These include (1) high-accuracy electronic navigation systems, including the advent of the Global Positioning System (GPS), that allow an aircraft's three-dimensional position to be known to a relative accuracy on the order of a wavelength (typically centimeters) across a flight path (synthetic aperture) that may be kilometers long; (2) electronics that allow signals of ultrahigh bandwidth (several gigahertz) to be synthesized and processed; (3) high-speed digital computing electronics that allow large amounts of raw radar pulse data to be formed via signal-processing techniques into digital images in real time or near-real time; and (4) the invention of a robust autofocus algorithm, which is a post-processing methodology that can remove the blurring artifacts in the formed SAR image that result from the small residual position errors left by the electronic navigation system.

Circa 1980, researchers in the SAR arena discovered that another aspect of SAR made it capable of performing certain tasks that were not achievable with optical or IR sensors. This discovery was founded in the fact that SARs are coherent imaging systems, whereas conventional electro-optical and infrared systems are not. As a coherent imager, a SAR transduces not only the amount of microwave energy reflected from Earth's surface, but also the phase of the reflected energy at any given position in the image. The quantity "phase" encodes, among other things, information regarding the precise position of a radar reflector, e.g., a rock, a piece of dirt, or a blade of grass, that lies within one of the resolution cells (pixels) of the formed SAR image. As a result, any change in the position of a reflector

can be measured to within a fraction of a wavelength (e.g., several millimeters) by computing the phase difference as measured by a pair of SAR images taken of the same scene on Earth's surface, but separated in time, typically by hours to days. Known as coherent change detection (CCD), this procedure has been a very effective tool for more than a decade now in detecting subtle surface changes, including vehicle tracks and even human footprints. A second related phase difference technique known as interferometric SAR terrain mapping (IFSAR), can produce digital terrain elevation maps of Earth's surface that are accurate to within inches of elevation when measured on post spacings as small as 1 meter.

Current research in SAR involves attempts to have a computer automatically identify the vehicular targets within a formed SAR image. This set of techniques is commonly known as SAR automatic target recognition (ATR). In addition, serious research and development efforts are aimed at imaging and identifying moving vehicular targets, a capability generally referred to as moving-target indicators (MTIs). Finally, interest continues in SARs that can penetrate foliage (FOPEN SAR) and SARs whose radar transmitter and receiver are not collocated; that is, they are on different platforms (bistatic SAR). SARs will undoubtedly continue to be adapted to meet larger and larger shares of the imaging needs of both military and civilian efforts (Jakowatz et al., 1996).[1]

Orbital Sensors

Orbital sensors are an important part of the U.S. arsenal. Assets range from low-Earth-orbit to geosynchronous sensing systems, with most of the sensing complement in the low-Earth-orbit category. A wide variety of primarily electromagnetic sensors—from the infrared to the ultraviolet—are deployed, and the U.S. military is highly dependent on their capabilities. Increasingly, commercial enterprises are providing similar capabilities, at least in the visible wavelength range, and anyone can now anonymously order a satellite photograph of his or her—or your—neighborhood at very modest cost. Here as elsewhere, it will be important to continuously assess a potential enemy's access and sophistication and not assume that the military capabilities are far superior, as they have been for so long. Because of the commercial uses, access to space resources is no longer a state monopoly.

It is also important to consider what kinds of images an adversary might buy on the commercial market—for a modest price, for example, submeter-resolution images can be purchased over the Internet—and what their value might be for a subpeer state or even a nonstate actor such as a terrorist organization. High-resolution imagery as the domain of only peer adversaries is now a thing of the past, and the impact of this change should be carefully evaluated.

UXV-Mounted Sensors

As unmanned vehicles have become more capable and affordable, reliance on them for sensing has increased. The obvious advantage is that no human is in harm's way and the UAVs, because they are small, fast, maneuverable, and low-observable, provide a major advantage. This capability puts a premium on small, low-power-consumption sensor technologies. Just as in the case of satellite-based sensing systems, these sensors have taken good advantage of the continuing shrinkage of integrated circuit size, power consumption, and weight, as well as advances in micro- and nanotechnologies that are increasingly putting more power into smaller systems. A clear issue for the long term is that the

[1]Personal communication from Charles Jakowatz, Sandia National Laboratories, to the committee, January 26, 2005.

United States is no longer the dominant research community in these areas. Both the Pacific Rim and Europe are devoting significant resources to research in robotics and in micro- and nanotechnologies.[2]

Geolocation Sensor Systems

Global Positioning System. One form of sensing that has become increasingly important is geolocation. The advent of the Global Positioning System (GPS) has made it possible to accurately register the positions of equipment and personnel to tactical imagery or available maps. This capability makes it easier to guide BLUE forces in complex and fluid tactical situations. As reliance on this technology grows, however, the potential for disruption through GPS jamming becomes an increasingly worrisome possibility.

In its current incarnation, the GPS signals broadcast from satellites are relatively weak (each satellite radiates 500 watts). This means that it is possible to jam GPS signals with low-power transmitters. The low power of GPS means that it is not available in urban canyons, inside buildings, or under a jungle canopy. With urban warfare becoming increasingly important, alternatives to augment the capability provided by GPS should be developed. Some solutions such as GPS pseudolites are possible and could be deployed on aircraft or aerostats or even on rooftops if controlled by BLUE forces.

Another issue is that this capability is now widely available commercially. How much does this fact detract from the U.S. battlefield advantage? Why have Europe (France in particular) and China partnered to provide an alternative to GPS? If the operators refuse to deny availability of Galileo signals to an adversary, what options does the United States have?

Inertial Navigation. Microelectromechanical systems (MEMS)-based accelerometers make possible short-term inertial navigation that could be used to fill the gaps in information when GPS is not available.

Commercial GPS Navigation. Commercial GPS-like navigation systems, which use television signals and are intended for urban environments, will be available in the near term. Some of these systems will offer a significant increase in bandwidth capability compared with traditional GPS systems, stronger synchronization codes, and much lower operating frequencies that would allow for penetration of urban dwellings.[3]

Ultrawide Band Transduction. Recent work on using ultrawide band (UWB) transducers for precise location has appeared in the open literature. The approach involves emplacement of low-power UWB sources in, say, a building and then using time-of-flight computation to determine precise location.

Tidal Forces. There are currently many solutions to tracking objects that move at high speed, such as fixed-wing aircraft, through the use of GPS and/or inertial measurement units (IMUs). Unfortunately, tracking the movement of slower objects remains a problem in situations where GPS is not available.

Recent work has focused on the use of variations in the local gravitational field. Simulations have been developed using closed-form solutions that analyze these geophysical signals, add appropriate

[2]See, for example, http://www.nano.gov/html/res/IntStratDevRoco.htm. Last accessed on April 8, 2005.

[3]See, for example, http://www.rosum.com/rosum_tv-gps_indoor_location_technology.html. Last accessed on February 11, 2005.

noise levels, and then compute a location based on an iterative technique. These simulations are being used to determine the boundary conditions under which geolocation can be performed and to ascertain the types of sensing and signal-processing technologies required to implement a fieldable microsystem (Novak et al., 2005).

Networked Point Sensors

There is increasing interest in the emergent properties of networked point sensors—extending from large systems (e.g., satellite antenna arrays) to small expendable self-contained microsystems or "smart dust"—as an approach to sensing with improved performance and often with enhanced robustness. Commercial products such as SmartMesh™, a low-power wireless mesh sensor network, are already in use.[4] The vulnerabilities of these systems vary considerably, but clearly the network management aspects are very difficult and are inherently subject to intercept, jamming, and deception strategies.

Since most electronics manufacturing occurs outside the continental United States, it is likely that the United States will face adversaries with significant sensor networking capabilities soon after the technologies are developed. There are no esoteric materials or techniques involved, and, once committed to silicon, the sensors can be replicated inexpensively in the millions. Since software engineering expertise is not confined to the United States, once the algorithms are developed and published in the open literature it can be expected that they will be implemented both in commercial products and by the military establishments of U.S. adversaries.

Sensor Modalities

Terahertz Sensors

The terahertz frequency range (once called the submillimeter spectral region) has seen a recent increase in research activity largely because of the potential ability of terahertz sensors to "see through walls and under clothes." (Such a capability raises many new issues such as those related to privacy in a law enforcement context.) The largest issue is the lack of a suitable set of sources of sufficient power and detectors of sufficient sensitivity. At present much of this work is in the research stage and is available primarily to state actors. Understanding of the interaction of terahertz waves with materials, for example, spectroscopy of complex biomolecules, is at a very primitive stage, with interesting and possibly important suggestions of an enhanced capability for discrimination of signals, but without either a strong theoretical or an extensive experimental foundation.

Infrared Spectrum

The infrared is a very information-rich spectral region. The rotational-vibrational spectra of all molecular species lie in the infrared. Further, the peak of room-temperature blackbody radiation is at about 10 micrometers in the IR so that all of these species radiatively exchange energy with the environment. Monitoring this radiation provides a critical sensing modality. Night-vision imaging sensors are sensitive over a range of near-IR wavelengths and enable troops to operate in nighttime and dark environments. These detectors operate by sensing differences in temperature/emissivity from

[4]See, for example, http://www.dust-inc.com. Last accessed on February 10, 2005.

different surfaces—warm people and machines versus cold plants, and so on. Although the advanced sensors of the U.S. military have led to the concept that "the U.S. owns the night," the danger is that these sensors are entering the commercial sector for a variety of legitimate applications and are thus becoming widely available to friend and foe alike. It will be important to monitor the availability of night-vision equipment to likely adversaries, both state and nonstate, so as to avoid relying on a technological superiority that no longer exists.

Visible Spectrum

The visible spectrum is the range of the greatest atmospheric transmission and is also the region of the spectrum for which sensing equipment is the most advanced and capable. Myriad sensor systems cover this range, and much work has been done in signal processing to extract information from optical images. As sensing equipment is increasingly silicon-dominated and networked processing-intensive, one of the issues to be concerned with is the trustworthiness of the software and hardware, especially as the sources of both move offshore, often to less politically reliable areas.

Acoustic and Seismic Sensors

Acoustic and seismic sensors have proven useful in a variety of military applications. These sensors can serve as simple threshold detectors—that is, to detect signatures that exceed specified limits—or they can be utilized to identify classes of targets. The acoustic signatures of military targets are fairly diverse, and good performance in identifying them is achievable for time-critical targets. Acoustic arrays can provide a bearing to target. Even with a limited number of sensors, properly deployed seismic arrays can provide information on direction of travel. The primary role of these sensors is as a force multiplier. A major challenge is efficiently and effectively analyzing the vast amounts of data generated by even a moderate number of sensors.[5,6]

Imaging/Spectroscopy

Increasing use is being made of spectral imaging of a spatially resolved target. Multispectral imaging and hyperspectral imaging, for example, are unquestionably powerful techniques, but they produce vast quantities of data. One of the major challenges is to synthesize/compile all of the data obtained to provide actionable information. Another is to decide how much of the data to transmit over available communication lines. The increasing emphasis on local data-processing operations to reduce the load on the communications links can be either beneficial or harmful to the ability to maintain information dominance, depending on the situation. The optimal system should be automatically reconfigurable in response to external factors that can change rapidly. This major challenge brings up all of the issues of surety of hardware and software and network reliability discussed above for other sensor modalities.

[5]Frederick T. Mendenhall and Kevin T. Malone, Sandia National Laboratories, personal communication to committee member Al Romig on December 20, 2004.

[6]For more information, see Ackermann, Mark R. 2004. TALON Local Area Network (LAN) Sensor Systems Report. Sandia Report SAND2004-3423. Sandia National Laboratories, Albuquerque, N.Mex.

Chemical Sensors

Chemical sensors can be classified as remote and point sensors. Remote chemical sensors are based largely on spectroscopy, with transitions extending from the near-ultraviolet to the terahertz region. The infrared spectral region is the most information rich for most molecular species. For many detection schemes, false-alarm discrimination is a major issue. The battlefield in particular is a chemical-rich environment, and it is important to be able to distinguish between chemical agents and other species. Nerve agents, for example, are very large molecules with complex rotational-vibrational spectra with many overlapping bonds giving a broad resonance. The phosphorus-oxygen stretch at 10 micrometers is an important signature of many nerve agents. Ammonia, which is commonly found in the battlefield environment, is a small molecule with sharply defined rotation-vibration lines. A high-spectral-resolution, broadly tunable sensor is needed to achieve the necessary discrimination. Many point sensors operate by changing conductivity in the presence of chemical agents. Because many things can cause conductivity to change, adequate discrimination and false alarms are major issues, and it is necessary to have good controls and redundancy to ensure reliable readings.

Ionizing Radiation

Sensing of ionizing radiation is a very mature activity, reaching back more than one-half century. Unstable nuclei go through a process via beta, alpha, positron, and electron capture or fission decay to attain a stable nucleus. The half-lives for these processes differ by many orders of magnitude, as do the levels of radiation emitted during these processes. These energy emissions generally interact with surrounding media and therefore are attenuated as they travel from the emitting source to the detector system. Thus, radiation detection, although possible at large distances in some cases, is normally described as point detection. Often the decay particle can be measured directly, but often it is convenient to detect and quantify the gamma rays emitted during the processes. Most radiation detection systems used for search and other fieldwork rely on the detection of gamma rays and neutrons. Most radionuclides can be identified via detection of their unique gamma-ray signatures (Knoll, 1979).

The ability to identify isotopes based on gamma-ray spectra is greatly facilitated by using detectors with high energy resolution to unambiguously identify the isotope by characteristic emitted energies, which show up as lines at specific energies in an energy spectrum. However, in practice there are trade-offs. Currently, and for the foreseeable future, the gamma-ray detectors with the best resolution are also the most expensive, and they exhibit other characteristics that constrain their use in many field applications. The larger and cheaper detectors exhibit poorer energy resolution. Under some conditions, especially where measurements can be taken for long periods of time (several minutes to hours) and/or in close proximity (approximately a meter or less, depending on source strength and detector size), miniaturized detectors are required or have a niche. This is because source strength and source shielding often dictate that less than 1 million gammas per second in 4-pi geometry are available for measurement, and sometimes one to two orders of magnitude less. For small detectors with a frontal area on the order of 1 to 10 cm^2, this means that at distances greater than 1 meter, 10 or fewer gamma rays may intersect the detector in a second of measurement time.

In many real-world applications, such as at traffic choke points or other points of entry into the United States, measurements must be made in only a few seconds in order not to disrupt commerce unduly. Thus, during such a measurement with small detectors, often the total number of gamma rays striking the detector may be a few hundred, or less. No matter what the detector type (material), for detectors of a reasonable thickness, the probability of interaction will be less than unity. In addition,

many gamma rays will not deposit their full energy within the detector volume, but will scatter and escape the detection volume, so that the photon energies and some other energies will have been detected at less than the full energy peak. Although these scattered gamma rays are useful, they are not specific to the isotope being measured, but present a rather broad, featureless continuum. Thus, in order to determine the presence of a specific isotope using its specific full-energy lines, several hundred, or more, gamma rays must interact with the detector, in addition to those interacting based on radioactive isotopes always present in the environment (background).

The shielding and scattering effects are also energy and material dependent, making the resulting spectrum somewhat complex. Thus, in many applications, larger, rather than smaller, detector volumes are required because of the physics, and there is nothing that can be done to totally overcome this limitation through the use of different detector types or materials. In practice plastic scintillators are the largest and cheapest of the usable gamma spectrometers. However, the energy resolution is so poor in these low-atomic-number organics as to make reasonable isotope identification through normal means almost impossible—i.e., their use as a spectrometer is quite limited.

The next general class of detectors in use is inorganic scintillators, such as NaI and CsI detectors. These detectors are more expensive volume-wise than plastic and are usually smaller. However, their energy resolution and detection sensitivity are significantly better than those of plastic, and they can usually be provided with volume/area such that they are the most typical detector used for fielded systems providing isotope identification.

Another category of detector is based on a room-temperature semiconductor, such as cadmium-zinc-telluride (CZT), and has an energy resolution typically three- to fourfold better than that of an NaI detector. This technology is still under development, and spectral-grade detectors are still difficult to obtain, are quite expensive for the volume obtained, and are variable in detection characteristics from detector to detector (quality control). Their main drawback, however, is the small volumes obtainable—on the order of a few cubic centimeters, at best.

A great deal of effort has been expended in the last decade to grow bigger, better crystals, and to use other techniques, such as combining several detector elements into arrays and providing pulse-shape discrimination, to get better resolution or larger effective sizes. But such technologies are still inadequate for most normal field applications. High-purity germanium semiconductor detectors have the best energy resolution available for fieldable gamma-ray detection. Their energy resolution is better than CZT by a factor of 20 to 30 and better than NaI by a factor of 50 to 100. However, they must be cryogenically cooled to liquid-nitrogen temperatures, thus requiring large dewars or more electrical power for thermo-mechanical cooling than can typically be supplied by a battery-operated system. In addition, the largest sizes are about 1 liter in volume—much larger than CZT, but still much smaller than that available from NaI or plastic. In addition, they are 10 times as expensive as CZT and 20 to 50 times as expensive as NaI. In all cases, costs vary as a function of volume and detector quality.

To overcome the limitations and difficulties associated with spectral unfolding from detectors of poorer energy resolution, software processing techniques have been under development. In most cases, these techniques, which can also be used with high-resolution systems, make it possible to provide at least a primary isotope detection and identification. Using these techniques and detectors it is possible to separate medical from industrial isotopes and special nuclear material and also to make some determination of the amount of shielding—and thus to determine whether a medical isotope of reasonable activity and little shielding, such as an isotope isolated in the human body, is being used in a legitimate application, or if a similar source, but orders of magnitude more intense, is being hidden within heavy shielding (one case of a radiological dispersal device). Such a determination is based on the spectral

shape of the measured spectrum, a result of the energy dependence of absorption/scattering on materials present as described above.

There are circumstances in which the effects of shielding and the requirement to determine specific isotopes of an elemental source would require the use of a high-purity germanium detector. Some low-level emitters, such as enriched uranium, can be detected passively through other, normally associated isotopes, such as U-238 or U-232. The gamma rays emitted specifically from U-235 are low in energy and easily shielded, or are so weak in intensity as to be difficult to detect under most field constraints. Thus, enriched uranium is often detected passively through detection and identification of gamma rays from associated isotopes, if present. Otherwise, active interrogation methods can be employed, typically using neutrons or high-energy gamma rays as the interrogating medium, that cause the U-235 in the sample to fission and thus emit neutrons and other measurable gamma rays. However, such interrogating systems tend to be rather large and expensive and present radiation safety issues. In short, several options are currently available for making radioisotopic measurements. The specific system used must be optimized for the specific situation and associated concept of operations. Ongoing research and development aims to yield new materials and techniques, which will provide some relief in some scenarios. This development should be encouraged and funded. However, there is much that can be done by designing appropriate systems with detectors currently available.[7,8]

REFERENCES

Jakowatz, Jr., Charles V. et al. 1996. Spotlight-Mode Synthetic Aperture Radar: A Signal Processing Approach. Kluwer Academic Publishers, Boston.

Knoll, Glenn F. 1979. Radiation Detection and Measurement. Wiley, New York.

NIST (National Institute of Standards and Technology). 2000. Report on the Development of the Advanced Encryption Standard (AES), U.S. Department of Commerce. Available online at http://www.linuxsecurity.com/resource_files/cryptography/r2report.pdf. Last accessed on February 11, 2005.

Novak, Jim L., Michael R. Daily, and Steven B. Rohde. 2005. Geophysical Geolocation System. Sandia National Laboratories, Albuquerque, N.Mex.

NRC (National Research Council). 1991. Computers at Risk: Safe Computing in the Information Age. National Academy Press, Washington, D.C.

NRC. 1996a. Cryptography's Role in Securing the Information Society. National Academy Press, Washington, D.C.

NRC. 1996b. Continued Review of the Tax Systems Modernization of the Internal Revenue Service: Final Report. National Academy Press, Washington, D.C.

NRC. 1997. For the Record: Protecting Electronic Health Information. National Academy Press, Washington, D.C.

NRC. 1998. Trust in Cyberspace. National Academy Press, Washington, D.C.

NRC. 1999. Realizing the Potential of C4I: Fundamental Challenges. National Academy Press, Washington, D.C.

NRC. 2001. Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers. National Academy Press, Washington, D.C.

NRC. 2002. Cybersecurity Today and Tomorrow: Pay Now or Pay Later. The National Academies Press, Washington, D.C.

[7]David Waymire, Sandia National Lahoratories, personal communication to the committee on January 14, 2005.

[8]For more information, see Shefelbine, H.C. and D.J. Mitchell. 2002. (U) Detection and Identification of Radioactive Sources. Sandia National Laboratories, Albuquerque, N.Mex.

Appendix E

Background Material for Chapter 6

POTENTIAL IMPLICATIONS OF BRAIN IMAGING RESEARCH

Behaviors requiring complex integration of several cognitive and motor tasks are core in today's technological world. As our vision and scientific endeavors grow toward Bunyanesque undertakings, we push the envelope of the cumulative stress normal humans can be expected to absorb. Current soldier-system monitoring includes occasional measuring of physiological parameters as well as recording of performance observables following training and familiarization exercises. These techniques are little advanced from clipboard, stopwatch, and fill-in-the-blank subjective rating scales. Although effective at diagnosing general health and skills in combat maneuvering, hand-to-hand combat, and precision fire, these modalities are incapable of providing useful information to prevent the onset of neuropsychiatric conditions before they result in degradation of performance and thus increase the risk of human error.

Recent evidence from operations Desert Shield and Desert Storm and current Iraq operations indicates unequivocally that such concerns are more important now than in past conflicts. Their being accorded greater importance may be due to greater vigilance being paid to field performance under close quarters with better real-time observation, or to a new awareness of the importance of the antecedents to post-traumatic neurosis as a real psychodynamic to an accurate diagnosis, or both. It may also be a condition of the changes in the way we now ask individuals to perform under stress, with increased individualization in both decision making and performance while directly in harm's way. The current enemy and that of the next three decades have an advantage in serving under a sociopolitical-religious mandate unacceptable and unfamiliar in the West.

Finding new ways to elicit, observe, and record behaviors to ensure the continuity of health over long periods of confinement and isolation is a key research area. In addition, decision-under-stress reactions are native to each individual, adding complexity to human factors analysis during traditional training schemes as well as to monitoring of mental acuity. Extra design considerations are also required to fold in the cumulative effects of very long (1 to 2 years) mission durations in harsh climates where stress takes a continuous toll, and of less-than-war situations, in which death nonetheless awaits literally

at every corner, every day. Finally, careful and appropriate attention is needed to psychiatric liability, informed by past experiences, which can at best confound and at worst imperil such missions (Genik et al., 2005, in press).

Current and future tools and techniques in brain imaging promise to provide essential additional information to monitor the effectiveness of training as well as mental status. The recent advent of functional neuroimaging, discussed below, has sparked world interest in the four major noninvasive brain-monitoring modalities: electroencephalography (EEG), magnetoencephalography (MEG), functional magnetic resonance imaging (fMRI), and near-infrared spectroscopy (NIRS). In this appendix the committee explores the current technologies and how in the future they may be engineered and employed for use for monitoring in simulated (training) and actual pre-mission qualification, especially of the young officer cadre entering battle under nontraditional and high-threat conditions. The methodologies are amenable to application in the assessment of mental status and training efficiency, under flexible conditions and in virtual-reality testing and training scenarios.

ENABLING TECHNOLOGIES FOR A NEW BLUE FORCE CAPABILITY

Here the committee postulates a new BLUE force capability that enables training and networked communication, as well as interview/interrogation. It envisions a portable modular sensor suite that is:

- Noninvasive,
- Expandable and flexible, and
- Compatible with current systems.

Current methods for human-human tactical communication must be informed by new cognitive research. In the next decade, it may be possible (with minimal military-specific operational integration of the following technologies) to determine with specificity nonverbal communications between and among soldier systems. The same research will inform a variation of this capability to replace entirely the current hostile, putatively unethical, and near-valueless physical coercion techniques used to determine truth and deception in captured RED forces, both enemy soldiers and nonmilitary combatants.

Enabling technologies include emergent functional brain neuroimaging methodologies together with data fusion software applied to multisensor, multispectral neurophysiological signals.

Potential applications include expanded interpersonal communications via BLUE soldier-system wearable body and helmet mounts; multi-lead covert and overt polygraphy applications and psychological interview techniques; and detection of intentions, deception, and truth in captured RED combatants.

Subsequent sections describe in greater detail the emerging technologies that may enable such capabilities.

Functional Neuroimaging Technologies and Soldier Systems

Human brains are constantly occupied with tasks that include unconscious activities such as regulation of breathing and circulation, and highly cognitive functions such as reading and interpreting technical reports. The human brain does not take well to a complete reboot to a known state, and therefore the measured state of any individual brain is a function of its initial state (genetic makeup) and the entirety of internal chemical and external biosensory stimulation integrated from birth to the present. To overcome the extensiveness of variation, one can take a picture of the brain in a baseline state and immediately afterward apply some external stimulus or have the subject perform a simple task and take

a second picture in the activated state. The difference image will reveal what parts of the brain were activated to confront the stimulus or perform the task. This is the principle behind functional neuroimaging. In practice, baseline and activation states are repeated and recorded several times to average over inherent noise and prove repeatability. Details about how many repetitions are required depend on the imaging method, or modality used.

Electroencephalography is a compendium of measured voltage differences at the scalp obtained from between 10 and 300 probe electrodes. Neuronal activity in gray matter or white matter axonal transmission of signals, the *primary current*, induces cascading *volume currents* in surrounding tissue and ultimately surface currents on the skin. The electrical diffusion is very fast, and for all practical purposes the signals that appear at the scalp are simultaneous with the brain activity. The best spatial resolution is obtained for cortical primary currents. Deeper subcortical primaries are detectable as well with a corresponding decrease in spatial resolution. When used in a functional experiment, the measured voltage temporal changes related to a task or stimulus are called event-related potentials (ERPs).

Involved in construction of an EEG is the electrode pack, which can be a personalized flexible cap, a set of signal amplifiers, a multichannel few-hundred-hertz digital sampler, and an interface multiplexer, such as the next-generation serial bus, for presentation to a standard interpretation display, recording device, or general-purpose onboard computer. When designed to be lightweight and compact using even current technology, a 64-channel EEG can be easily incorporated into a tanker-training module, or into the actual tank, APC, Bradley Fighting Vehicle, BCW enclosed FUCH's scout vehicle, helicopter trainer or actual cabin, and more. Indeed, an EEG system can be incorporated into advanced extravehicular mobility units (EMUs) and integrated with the standard physiological telemetry for nominal additional weight in the new soldier-system dismounted uniform.

Magnetoencephalography measures near-scalp sub-picotesla magnetic field variations due to the time-dependent primary and volume currents using a cryogenic helmet-mounted array of hundreds of superconducting quantum interference devices (SQUIDs). MEG is similar in temporal resolution to EEG. The sensor array is designed to detect currents parallel to the scalp, and MEG excels in distinguishing these from currents perpendicular to the scalp (predominantly cortical surface currents in gray matter convex folds, or *gyral currents*).

The additional weight of precision electronics and control systems necessary for MEG is hard to justify if the only benefit is real-time separation of gyral and cortical surface currents, since individual astronaut EEG meshes can be calibrated with a preflight MEG such that the EEG can determine the area of activation with acceptable accuracy. However, the higher accuracy is justifiable if some of the SQUID measurement, control, and analysis systems can serve as dual-purpose apparatus for other experiments.

The brain activity measured by EEG and MEG is the result of ionic motion within the central nervous system. Ionic production, release, and movement consume energy. This energy is supplied by the conversion of blood-borne oxyhemoglobin to deoxyhemoglobin. Through a complicated chain reaction called the blood-oxygen-level-dependent (BOLD) effect, brain activity results in a net increase in the relative concentration of oxyhemoglobin in the local venous structure of the circulatory system. Oxy- and deoxyhemoglobin have different magnetic susceptibilities and different colors, giving rise to two methods to measure the local hemodynamic response to brain activity.

Magnetic resonance imaging (MRI) works by a simple excitation and relaxation of spin states. When molecules containing hydrogen are placed in a strong static magnetic field, a small but detectable number of hydrogen protons align their spins along the direction of the external field. An applied radio-frequency (RF) pulse near the proton resonant frequency knocks the spins perpendicular to the field, and the relaxation back to ground state releases RF energy in a pattern that can be reconstructed to show both

the composition and the distribution of blood, soft tissue, or any other hydrogen-rich material. A series of fast scans calibrated to optimize detection of the BOLD signal will show the dynamics of brain function under the specific internal or applied conditions; this is known as fMRI, and the major advantages of this modality are three-dimensional spatial resolution and complete skull penetration, making it the only modality to unambiguously detect limbic activations important for determining certain neuropsychological states. In addition to measuring the BOLD signal at higher precision, future hardware advances will allow fine temporal monitoring of neurochemical movement and reactions using ultrafast spectroscopic analysis techniques in fMRI.

Complete commercial clinical MRI scanners weigh as much as an entire communications satellite and are inappropriate to bolt to a military vehicle or helicopter bulkhead. What is promising, though, is that many of the bulky or heavy components of commercial scanners are not necessary in the embodiments that will be deployed: lightweight skullcap monitors with neural-network software based on the ground-heavy MRI scanning systems, and the MEG near-field applied to near-infrared spectroscopy and ported into existing low-power supplies, will be data-, not weight-, dependent. Additionally, whole-body toroid and multiscan high-resolution options are not required, but rather just a system big enough to fit a head with a single detection coil of moderate size because high-resolution scans can be collected pre-mission and digitally carried along. Functional MRI scans are themselves moderate-resolution, and any clinical diagnosis for traumatic injury to a scannable body part can be accomplished with a combination of high- and moderate-resolution images. Finally, the cryogenic components and superconducting magnet energizer or DC electromagnet power supply can be parasitized off other necessary onboard systems, vacuum pumps can be replaced with a good valve, and several ancillary failsafes that make the scanner clinician-proof can be eliminated. All told, an appropriate MRI scanner could be put together in a couple of hundred additional pounds.

Near-infrared spectroscopy, the technology behind the nascent real-time finger-clamp pulse oximeter, has developed into a commercially available 48-channel BOLD-signal-monitoring head array mounted in a flexible cap. The system currently has moderate spatial resolution for cortical activations. Future systems promise better resolution and deeper activation detection. Figure E-1 shows the neuroimaging modalities explained above.

The NIRS modality can be built using available technology and dual-task post-processing equipment. The sensory array is simply pairs of light-emitting diodes (LEDs) and photodiodes either directly mounted in a cap or remotely working through optical fibers. Indeed, the bulk and weight of the detection array make NIRS, like EEG, an appropriate consideration for integration into advanced EMUs as well as vehicle-mounted systems.

Further details of technical methodologies are available in an extended treatise (Genik et al., in press[1]) or complete reviews (Hamalainen et al., 1993; Jezzard et al., 2003). In summary, the above modalities are best when used in combination, and not necessarily simultaneously, as their neuroimaging strengths complement rather than duplicate one another. EEG excels at monitoring gross mental load in steady-state conditions, though it is also adequate for determining activity in pre-mapped cortical structures. MEG can discriminate between gyral and surface currents with moderate spatial resolution, and this can be vital information if a specific brain network structure is located in either of these places. MRI is the only noninvasive modality that can specifically localize deep-brain neural systems responsible for emotional processing, essential information for determining neuropsychiatric health. Finally,

[1]Genik II, Richard J., Li Hsieh, Francis X. Graydon, and Christopher C. Green. Emergent functional brain imaging and rehabilitation opportunities. In J.M. Pellerito (ed.), Driver Rehabilitation: Principles and Practice. Elsevier, in press.

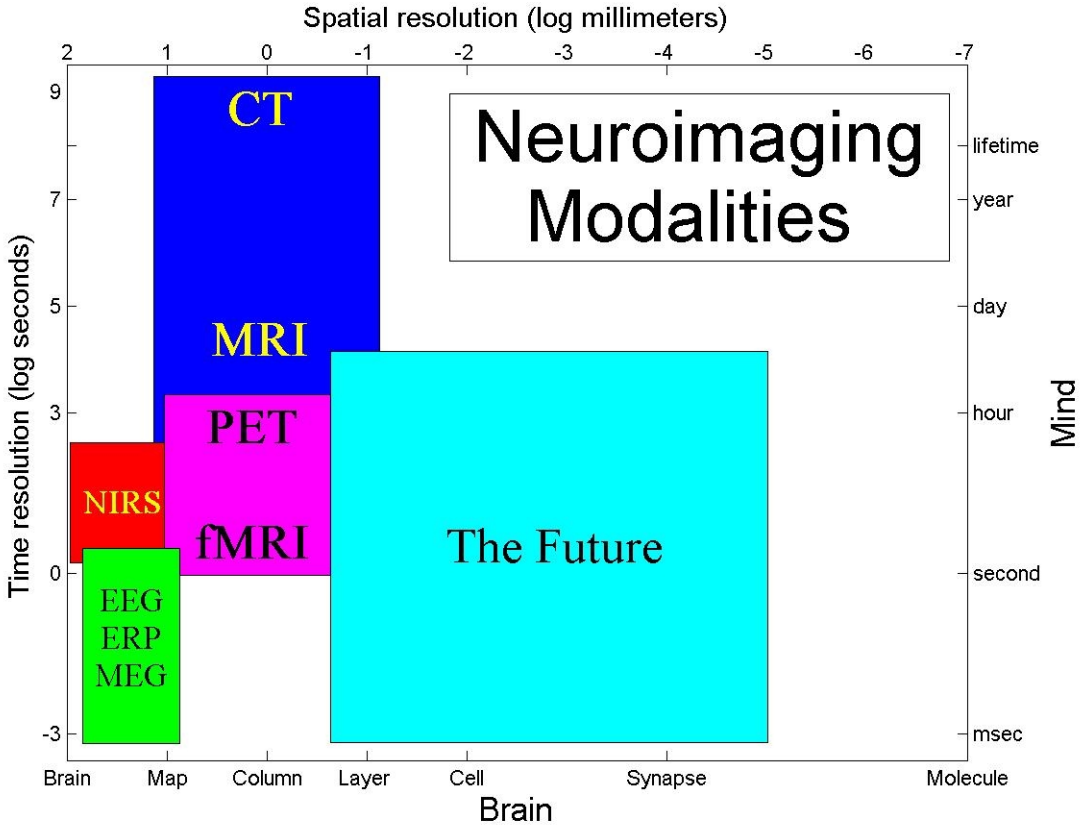

FIGURE E-1 Spatial and temporal resolution capabilities of different neuroimaging modalities. Spatial extent is correlated with basic brain anatomy and the temporal changes in these images with observation of the working mind. SOURCE: Genik et al. (2005, in press).

NIRS provides a relatively inexpensive and robust monitor for cortical activation, a metric important for determining cognitive response efficiency at any instantaneous gross mental activity level.

Neuroimaging and Applications to Crewmember Health and Training

Beyond a discussion of biomedical engineering considerations of brain-imaging modalities, it is vital to determine whether information gathered offers important insight into the health continuum of crewmembers in military vehicles or of the dismounted, but in the future highly instrumented, soldier. The bandwidth will exist, the channels will exist, and the readouts will be distributed to the company level. The first comprehension of the potential for neuroimaging technologies in the context of long-duration spaceflight, as one example, was discussed in a 2001 NASA Jet Propulsion Laboratory workshop.[2] The findings are identical to those expected for the current soldier in isolation, perceived isola-

[2]Workshop on Revolutionary Aerospace Concepts for Human/Robotic Exploration of the Solar System. N.I. Marzwell and H.M. Harris, Jet Propulsion Laboratory, November 6-7, 2001.

tion, and/or continual stress. Moreover, the Bioastronautics Critical Path Roadmap identifies three mission confounders of particular relevance to the current Iraq operational scenario, for example: psychological disruption (e.g., circadian and sleep disorders), neuropsychiatric dysfunction (affective disorders), and nonspecific stress. All are amenable to current emergent neuroimaging modalities and can be studied in real time under fairly realistic conditions. Monitoring behavioral health of the crew can provide important input regarding mission decisions. Furthermore, pre-mission training programs will benefit from the additional insights into crew performance provided by neuroimaging.

Previous soldier long-duration mission training and EEG experiments have concentrated on narrow hypotheses, and the modality has not been adopted as standard procedure. Normal sleep is easily monitored with EEG, and deviations can raise alerts to possible developing situations. Waking EEG measurements show level of alertness and thus can help to determine risk levels for starting or continuing a mission-critical activity. Additionally, sleeping EEG traces have been associated with predictive outcomes for treatment of depression (Hatzinger et al., 2004), waking EEG traces have been associated with post-traumatic stress disorder (Chae et al., 2004), and functional EEG and changes in ERP have been used to monitor attention level in complex cognitive tasks (Ramos-Loyo et al., 2004). The next generation of studies will likely yield insight into many underlying affective disease mechanisms and metrics of behavior such as vigilance. Generation-after-next work will yield predictive algorithms from EEG sleep traces to head off circadian- and sleep-related disorders before they affect waking behavior (failure of human performance because of poor psychosocial adaptation or neurobehavioral dysfunction).

MEG has advantages over EEG for specific monitoring tasks (Barkley, 2004). Work completed in collaboration with Young et al. (2005)[3] concentrates on the basics of piloting motorized vehicles while facing cognitive challenges, where MEG was used to locate functional activity related to event detection. Current work focuses on increasing the cognitive load and seeks to determine thresholds for overload, the point at which event detection breaks down and a driver or pilot can make a fatal error (failure of human performance because of system interface problems and ineffective workload). The next 5 years promise advances in MEG methodology as a complement to both EEG and fMRI, although it will likely be useful only for ground-based preflight training and screening of crewmembers. Generation-after-next technology will be required to start in-flight monitoring using this modality in a regular behavioral health regimen.

Advances in understanding of brain networks involved in piloting motor vehicles and high-performance aircraft based on use of the maturing technology of BOLD fMRI will drive functional neuroimaging understanding of these activities in the next 5 years. Previous studies have focused on narrow aspects of navigation (Uchiyama et al., 2003), attempts to localize impairment of navigational abilities (Calhoun et al., 2004), and the beginnings of next-generation understanding of event detection in simulated driving tasks (Graydon et al., 2004; Young et al., 2005). Current work is focusing on increasing the level of distraction and monitoring the effect on detection of the primary event. It is well known that even heavily sedated primates show activation in the visual cortex as a result of optical stimulation; it is also well known that humans can be looking directly at events and not react to them, a behavior known as cognitive blindness, or colloquially as the "look-but-do-not-see" phenomenon. What is not known at all is what disruption in which brain network causes cognitive blindness, as well as whether the risk of this phenomenon can be consistently modulated (Reilly, 2003). Of special relevance

[3]Young, Richard A., Li Hsieh, Francis X. Graydon, Richard J. Genik II, Mark D. Benton, Christopher C. Green, Susan M. Bowyer, John E. Moran, and Norman Tepley. 2005. Mind-on-the-drive: Real-time functional neuroimaging of cognitive brain mechanisms underlying driver performance and distraction. Presented at SAE 2005 World Congress and Exhibition, April, Detroit, Mich.

here is the identification friend-or-foe problem set: friendly-fire deaths occur regularly in unmanned combat air vehicle (UCAV) and umanned aerial vehicle (UAV) maneuvers, helicopter tactical operations, sniper operations, and mounted Bradley and Abrams operations. Technology to understand and mitigate the "brain internal" disconnect in looking but not seeing, or comprehending, or processing may be more important statistically than a next-generation set of sensors that must be highly networked and computer-centric on the distributed battlefield.

The next generation of fMRI multimodal studies will determine the extent to which emotional responses and psychopharmaceutical impairment affect navigational task learning and performance. It is expected that some optimal level of emotional involvement in navigational decisions, especially those made under stress from high cognitive workload, sleep deprivation, or some induced affective disorder, can be determined; for example, it is likely that optimal decision making occurs somewhere between cold-as-ice detachment and "We're all going to die!" paranoid neuroses. Such tools will be useful in training all categories of operators, whether tankers or snipers, or to provide feedback to helicopter or UCAV pilots, especially those who increasingly may view simulator training as a video game. Moreover, monitoring the efficiency of training and the effectiveness of alert systems can directly impact the risk of performance failure owing to interface problems and ineffective workload, as it has already been shown that pilots show different activation levels once they become fully trained in a maneuver (Peres et al., 2000), when they have reached their fastest reaction times (Mohamed et al., 2004), and when an alert interface is optimized to emphasize vigilance (Reilly, 2003). Thus, the basic groundwork is already in place to "watch soldier-operators think" during and after training that emphasizes attention to psychological states.

Generation-after-next fMRI imaging tools promise to deliver a capability for monitoring deep-brain emotional states in-flight. Research late in the next decade should also lead to simple paradigms and algorithms capable of benchmarking behavioral fitness in a matter of minutes as part of a weekly health regimen including examination of any neurochemistry changes in emotional reception and processing centers.

Once BOLD fMRI benchmarks are established, NIRS technology can be used to monitor cortical signals deemed important during actual task performance instead of a simulated paradigm. NIRS technology can also be used to monitor BOLD signals from increasing cerebral recruitment during extended dismounted activities or other long-duration mission-critical assignments (Drummond et al., 2004).

THE CURRENT OPERATIONAL STATE OF THE ART

Noncontact Multispectral Neurophysiological Sensors

Blood Pressure, Heart Rate, Interbeat Interval, Body Tremor (0.2 to 1.0 Hz), and Ballistocardiogram

Signal-processing algorithms (originally developed for underwater and spaceflight applications) have recently proved applicable to low-frequency improvement in conditions with a very high signal-to-noise ratio, such as for enabling real-time monitoring of numerous human neurological signals in both aware and unaware subjects. The signals illustrate embedded cardiovascular information. Such signal processing has been applied to the known technique of ballistocardiogram.

The validation of the subsystem, sensors embedded in a chair back, legs, and seat with RF signals "ported" to a remote station, was accomplished in a medical school: the subjects had arterial (radial) cannulation, and the software was subsequently "trained" by the ground-truth data. (This was, of course,

a straightforward series of statistical comparisons of signals of varying bandwidths, with the algorithm sequencing for "best fit.") Electron paramagnetic resonance oxygen mappings (EPROMs) were constructed and devices "measured" (approximated by estimation) systolic and diastolic blood pressure with good accuracy (plus/minus 5.0 mm Hg) compared with that of mercury sphygmomanometers.

An interesting "fall-out" of the human subject validation experiments was that the heart rate and interbeat interval were accurate enough to calculate, from tables (programmed in the EPROM), near-real-time caloric expenditure.

Detection of Carotid Artery Blood Flow, Differential Stenosis, and Heart Rate

During the test and evaluation of a small, man-portable infrared (mercury-cadmium-telluride) detector it was observed that thermographic profiles of humans in the near field (>2 and <25 ft) could be obtained, overtly and covertly. The system was tested in a series of subjects and calibrated. The specificity and sensitivity to facial temperature bilaterally over the cheeks and forehead were seen to be operationally useful, and data were collected in less than 1 second (from a seated subject in a reasonably quiet pose) that were accurate to within 0.5 degrees C.

The data were compared and contrasted with breast-tumor and facial thermographic units being used clinically. The pre-stroke detection data were incorporated successfully into an adult male pre-stroke health-monitoring program and deployed for further operational testing and evaluation in a scenario identical to that in an interview/interrogation facility (e.g., used in operational settings). The systems were installed behind infrared-transparent, visually opaque mirrors. The rooms were constructed with low ambient temperatures (<65 degrees F) and fans to enhance the utility of clinical data collection.

Subjects were unaware of the data collection. Scans were read and interpreted by qualified radiologists for clinical use.

Covert Communication System, One-Way to Simulated Polygrapher

A system was developed and fabricated that used a very-low-power, highly collimated and directionally deployed CO_2 laser to transmit voice data (1,000 to 10,000 Hz) to an operator's external auditory meatus, with real-time questions asked for the purpose of interrogating an individual, outside, seated on an instrumented bench (as described above), but inaudibly to the subject. The system was tested and found to work exceptionally well, under reasonable ambient outdoor conditions.

REFERENCES

Barkley, G.L. 2004. Controversies in neurophysiology. MEG is superior to EEG in localization of interictal epileptiform activity. Clinical Neurophysiology 115 (5): 1001-1009.

Calhoun, V.D., J.J. Pekar, and G.D. Pearlson. 2004. Alcohol intoxication effects on simulated driving: Exploring alcohol-dose effects on brain activation using functional MRI. Neuropsychopharmacology 29 (11): 2097-2117.

Chae, J.H., J. Jeong, B.S. Peterson, D.J. Kim, W.M. Bahk, T.Y. Jun, K.S. Kim, and K.Y. Kim. 2004. Dimensional complexity of the EEG in patients with posttraumatic stress disorder. Psychiatry Research 131 (1): 79-89.

Drummond, S.P., G.G. Brown, J.S. Salamat, and J.C. Gillin. 2004. Increasing task difficulty facilitates the cerebral compensatory response to total sleep deprivation. Sleep 27 (3): 445-451.

Genik II, Richard J., Christopher C. Green, Francis X. Graydon, and Robert E. Armstrong. 2005. Cognitive avionics and watching spaceflight crews think: Generation-after-next research tools in functional neuroimaging. Aviation, Space & Environmental Medicine, May, in press.

Graydon, Francis X., Richard Young, Mark D. Benton, Richard J. Genik II, Stefan Posse, Li Hsieh, and Christopher C. Green. 2004. Visual event detection during simulated driving: Identifying the neural correlates with functional neuroimaging. Transportation Research Part F: Traffic Psychology and Behavior 7 (4-5): 307-322.

Hamalainen, Matti, Riitta Hari, Risto J. Ilmoniemi, Jukka Knuutila, and Olli V. Lounasmaa. 1993. Magnetoencephalography—theory, instrumentation and applications to non-invasive studies of the working human brain. Review of Modern Physics 65 (2): 413-505.

Hatzinger, Martin, Ulrich M. Hemmeter, Serge Brand, Marcus Ising, and Edith Holsboer-Trachsler. 2004. Electroencephalographic sleep profiles in treatment course and long-term outcome of major depression: Association with DEX/CRH-test response. Journal of Psychiatric Research 38 (5): 453-465.

Jezzard, Peter, Paul M. Matthews, and Stephen M. Smith (eds.). 2003. Functional MRI: An Introduction to Methods. New York, NY: Oxford University Press.

Mohamed, Mona A., David M. Yousem, Aylin Tekes, Nina Browner, and Vince D. Calhoun. 2004. Correlation between the amplitude of cortical activation and reaction time: A functional MRI study. American Journal of Roentgenology 183 (3): 759-765.

Peres M., P.F. Van De Moortele, C. Pierard, S. Lehericy, P. Satabin, D. Le Bihan, and C.Y. Guezennec. 2000. Functional magnetic resonance imaging of mental strategy in a simulated aviation performance task. Aviation Space Environmental Medicine 71 (12): 1218-1231.

Ramos-Loyo, Julieta Andrés, Antonio Gonzalez-Garrido, Claudia Amezcua, and Miguel A. Guevara. 2004. Relationship between resting alpha activity and the ERPs obtained during a highly demanding selective attention task. International Journal of Psychophysiology 54 (3): 251-262.

Reilly, Clay E. 2003. Motor co-ordination in humans is guided by optimal feedback control. Journal of Neurology 250 (2): 257-258.

Uchiyama Y., K. Ebe, A. Kozato, T. Okada, and N. Sadato. 2003. The neural substrates of driving at a safe distance: A functional MRI study. Neuroscience Letters 352 (3): 199-202.