Critical Technology Accessibility

Committee on Critical Technology Accessibility, National Research Council

ISBN: 0-309-65853-5, 72 pages, 6 x 9, (2006)

This free PDF was downloaded from:
http://www.nap.edu/catalog/11658.html

Visit the National Academies Press online, the authoritative source for all books from the National Academy of Sciences, the National Academy of Engineering, the Institute of Medicine, and the National Research Council:

- Download hundreds of free books in PDF
- Read thousands of books online, free
- Sign up to be notified when new books are published
- Purchase printed books
- Purchase PDFs
- Explore with our innovative research tools

Thank you for downloading this free PDF. If you have comments, questions or just want more information about the books published by the National Academies Press, you may contact our customer service department toll-free at 888-624-8373, visit us online, or send an email to comments@nap.edu.

This free book plus thousands more books are available at http://www.nap.edu.

Copyright © National Academy of Sciences. Permission is granted for this material to be shared for noncommercial, educational purposes, provided that this notice appears on the reproduced materials, the Web address of the online, full authoritative version is retained, and copies are not altered. To disseminate otherwise or to republish requires written permission from the National Academies Press.

THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

CRITICAL TECHNOLOGY ACCESSIBILITY

Committee on Critical Technology Accessibility

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

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

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

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

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

International Standard Book Number 0-309-10146-8

Limited copies are available from:

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

Additional copies are available from:

The National Academies Press
500 Fifth Street, N.W.
Lockbox 285
Washington, DC 20001
(800) 624-6242 or (202) 334-3313
(in the Washington metropolitan area)
http://www.nap.edu

Copyright 2006 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

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

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. 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. Ralph J. Cicerone and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

COMMITTEE ON CRITICAL TECHNOLOGY ACCESSIBILITY

ROBERT J. HERMANN, *Chair*, Global Technology Partners, LLC
PIERRE A. CHAO, Center for Strategic and International Studies
ANTHONY J. DeMARIA, Coherent, Inc.
EDSEL D. DUNFORD, TRW (retired)
CHRISTOPHER C. GREEN, Wayne State University School of Medicine
JOSEPH F. GROSSON, Lockheed Martin Corporation
ALFONSO VELOSA III, Gartner, Inc.

Staff

MICHAEL A. CLARKE, Lead Board Director
DANIEL E.J. TALMAGE, JR., Study Director
CARTER W. FORD, Research Associate
LaSHAWN N. SIDBURY, Senior Program Associate

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Preface

The questions posed in the task for this study are part of a very broad and important set of issues for the Department of Defense. To answer them required the Committee on Critical Technology Accessibility to develop its own perspective about the context within which the questions could be placed. As a result, this report provides judgments and recommendations about both the specific questions and the broader context.

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 Defense Intelligence Agency 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, Carter Ford, and LaShawn Sidbury in the production of this report.

Robert J. Hermann, *Chair*
Committee on Critical Technology Accessibility

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

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:

Charles B. Duke, Xerox Corporation (retired),
Jacques S. Gansler, University of Maryland,
Donald A. Hicks, Hicks & Associates (retired),
Anita K. Jones, University of Virginia,
George Muellner, Boeing Phantom Works,
Alton D. Romig, Jr., Sandia National Laboratories, and
Joel S. Yudkin, 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 William H. Press, Los

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

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

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Contents

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Acronyms

ARCI	Navy's Acoustic Rapid COTS Insertion (program)
AT&L	Acquisition Technology and Logistics
COTS	commercial off-the-shelf
DIA	Defense Intelligence Agency
DIBCS	Defense Industrial Base Capabilities Study
DoD	Department of Defense
DSB	Defense Science Board
DUSD	Deputy Under Secretary of Defense
GDP	gross domestic product
HUMINT	human intelligence
IC	integrated circuit
IT	information technology
JDAM	Joint Direct Attach Munition
NRC	National Research Council
OODA	observe, orient, decide, act
PCB	printed circuit board
TIGER	Standing Committee on Technology Insight—Gauge, Evaluate, and Review
TWD	Technology Warning Division

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Boxes

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Executive Summary

There has been a steady increase in the influence of globalization on private, commercial, and national security activities in the United States. This influence has created new products, driven down the price of products, increased the volume of goods consumed, and broadened the base for economic growth in most parts of the world. Globalization is a fact of world economic activity (DSB, 1999; NRC, 2005a). This trend means that many useful products will be available only from non-U.S. commercial sources. American military systems designers will inevitably be faced with enjoying improved performance, price, and schedule from global products or suffering the penalties of nonoptimal performance by choosing domestic products that are deemed more trusted.

To gain an improved perspective on the issue of dependence on foreign source suppliers, the Technology Warning Division (TWD) of the Defense Intelligence Agency (DIA), with the assistance of the Standing Committee on Technology Insight—Gauge, Evaluate, and Review (TIGER), identified the need for a new study. The National Research Council (NRC), asked to respond to that need, organized the Committee on Critical Technology Accessibility to carry out the study. The statement of task for the committee is as follows:

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

> The NRC will impanel an ad hoc committee of experts to respond to the following questions:
>
> A. What products/components/technologies currently being solely procured from foreign suppliers could significantly disrupt U.S. defense capabilities if access to them were denied (through conflict, embargo, treaty, etc.)? What countries are the principal suppliers of these products/components/technologies? What would be the impact of such denial? What is the risk that such denial may occur? What alternatives should be considered and in what time frame?
> B. What emerging technologies/products that, if the United States chooses not to pursue domestic production, could significantly disrupt U.S. defense war fighting capabilities if access to them were denied? What countries might be the principal suppliers of these products/components/ technologies? What would be the impact of such denial? What alternative procurement methodologies should be considered for future acquisitions and in what time frame?

The committee looked for but did not find an existing, exhaustive database of foreign products/components being procured by the Department of Defense (DoD) and decided to not attempt to develop such a database on current foreign sourcing across the vast numbers of DoD systems. Nor did the committee assess, for each foreign component, the impact of denial on operational capability or try to understand the particular mitigation opportunities and consequences. Finally, it did not develop a collective assessment of the technological and industrial trajectories of emerging technologies that promise to be key to our nation's security. The size and scope of such an effort would have exceeded the time and resources available to the committee, and it became clear from the information provided to it and from its deliberations that this was not the right approach.

However, the committee did listen to government plans and perspectives, discussed the issues with recognized experts,[1] and independently reviewed source material and past literature. In addition, the members of the committee arrived with substantial background, service, and expertise in these matters. As a result, the committee believes it can still make many important judgments with respect to the task, and in this report it has undertaken to do so. As it addresses the relevant issues, it demonstrates some of the logic that would underly a more systematic approach to these

[1]See Appendix B for a complete let of presentations to the committee.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

assessments across the whole of the defense and national security establishment. The elements of that approach are addressed following its response to two overarching questions.

QUESTION A: THE RISK OF DENIAL OF CRITICAL PRODUCTS FROM FOREIGN SOURCES

Based on the information they received and their own knowledge, committee members were unable to identify any product or technology currently being exclusively procured from a foreign supplier that could significantly disrupt U.S. capabilities or operations should it suddenly become unavailable. Some of the reasons for this conclusion include the following:

- Over the last 60 years, the United States has created an industrial base for the domestic supply for every major strategic and critical military capability that requires specialized and expensive facilities. In particular, it has retained the industrial capabilities to produce nuclear weapons; missile defense systems; space systems and space control capabilities; armored vehicles; submarines and ships; aircraft; aircraft stealth and counterstealth; and underwater detection, classification, and targeting as well as underwater stealth and counterstealth. This does not mean that these primary systems do not have foreign content, but that the nation is able to manage the content, advantage, and risk associated with the foreign components in these systems.
- For network creation and management and information management, the critical domestic capability is the ability to integrate systems and match them to the operational needs of the military organization. The individual components of the network are important, but the systems integration ability is critical. The United States has a capable industrial base for integration, and there is little risk that it will be subject to dominance by a foreign supplier.
- The committee believes that most of the scenarios for future conflict involve military action using forces available at the time of the decision to go to war. This come-as-you-are type of operation does not provide an opportunity for a foreign source to deny the component and thereby impact significantly current operations, because the components should already be in the system. Further, there should be a reserve of materials for all components to serve as spares

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

and provide additional capability during operations. If reserves planning is not done well, it will not only be foreign suppliers that are the problem. The often-cited example of the potential vulnerability to denial of foreign components—the case where a Swiss manufacturer stopped the shipment of guidance components for the Joint Direct Attack Munition (JDAM) bomb during Operation Iraqi Freedom—is actually proof of the opposite: namely, robustness of the global supply chain. An alternative supplier was identified and qualified within 48 hours and no deliveries of JDAM bombs were impacted.[2]

- Today's U.S. joint warfighting force is a very diverse set of things and contains few, if any, single-point failure modes. Further, although almost all the elements of a current and future DoD force capability will have foreign content, the suppliers of this content are manifold, diverse, and not amenable to coordinated denial.

For these and other reasons, the committee believes that the risk-versus-reward assessments of foreign dependence are primarily supply management issues and must begin with defining and assessing risk, impact, and mitigation consequences. From a technology warning perspective, identifying and analyzing any changes to these mitigating circumstances should be a priority.

QUESTION B: ASSURING ACCESS TO FUTURE CRITICAL PRODUCTS AND TECHNOLOGIES

If the United States were to become strategically dependent on a foreign industrial base for items that are critical or for which the regeneration of a U.S. industrial base would take a long time, the risk would be unacceptable. The committee does not see any signs of that at this time, but the possibility should be taken into account when determining what the U.S. industrial base needs to be for defense purposes. The committee identified four areas of future technological and industrial advancement that warrant discussion: (1) information technology (IT) components; (2) IT services,

[2]Testimony to the United States-China Economic and Security Review Commission of Gary A. Powell, Acting Deputy Under Secretary of Defense (Industrial Policy). Available online at http://www.acq.osd.mil/ip/docs/china_economic_and_security_review_commission_8-22-05.pdf. Last accessed on February 7, 2006.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

which include many forms of the capability to manipulate, store, and exploit data and information; (3) nanotechnology; and (4) biotechnology. The committee also identified another area of concern, systems integration capabilities.

The committee cannot imagine a healthy U.S. economy without extensive U.S. industrial participation in the IT sector. It does not think the United States must be able to provide every product in this sector, but it does believe it must have within its domain companies that are leading participants in the global marketplace. Without that, both the national economy and DoD's ability to leverage this crucial set of products will be unacceptably limited. For IT components, which include many forms of the ability to manipulate, store, and exploit data and information, the committee sees no prospect that the United States will somehow fail to participate strongly, but it does wish to put on record its judgment that this sector is strategic and critical.

The potential of nanotechnology and biotechnology to both separately and jointly create profoundly new materials and capabilities means it must be assumed that U.S. industry can and will produce strategic and critical capabilities for our nation's security. The advances in both technologies will be largely driven by global commercial markets rather than by the U.S. military and the national security agencies (NRC, 2005b). For DoD to have assured access to these capabilities, it will be necessary for the nation to have healthy commercial industries in both sectors. DoD must therefore monitor progress in these sectors and intervene if necessary to assure a safe outcome for the nation.

Though not a technology or an industry in the same sense, one of the strategic and critical capabilities for a superior military force is the ability to integrate disparate technical and operational elements into a coherent entity that can achieve the mission objectives. This systems integration capability needs to be sustained, and the committee suggests monitoring and assessing U.S. strength and competence in this area.

A GLOBALIZATION MANAGEMENT STRATEGY

Globalization is an irreversible trend. This means that many new products that are and will be useful for DoD's mission are being created by this globalization process (Spencer, 2005). Design choices that favor improved system performance must allow using products from the global commercial marketplace, and many useful products will be available only from these

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

global commercial sources. The use of components and services from foreign sources brings with it risks and uncertainties that DoD needs to address.

From its deliberations the committee concludes that dealing with foreign sourcing is embedded in a larger supply assurance issue. Therefore, it is persuaded that the right management approach is to depend on the knowledge and judgment of the DoD acquisition and logistics officials as the starting point for an assessment of risk versus reward. Each of these officials has a supervisory chain that can provide guidance to couple the program manager's judgment to priorities beyond his purview. This same supervisory chain will also have the opportunity to review the judgments at the program level and will ensure that a DoD-wide perspective is applied.

The committee does not believe that the process should be a significant burden for the program manager and the logistics and procurement levels. Both should as a matter of course know the sources of supply for their function. They should routinely identify risks to their product sourcing and risks to their supply chain management decisions. They regularly analyze the trade-offs between mitigation opportunities and consequences. Foreign components are but one source of a broader assurance concern. Obliging these officials to regularly report on all significant sources of product assurance and supply chain risk, impact assessment, and mitigation consequences could well be considered a reasonable part of their normal duties.

This method of collecting data and judgments about the data runs the risk of being turned into a pro forma exercise that generates paper but does not contribute to an improved perspective. This fear is amplified by the fact that for the process to work this particular set of issues is to be added to the process currently used to work essentially all of the programmatic issues of the DoD and it does indeed produce a lot of paper. However, it is the process by which problems thought to be important—such as performance, cost, and schedule—are dealt with. If foreign dependence is to be an important issue for the DoD, it should be dealt with by the same process used for other problems thought to be important. If foreign dependence is not thought to be important, this suggestion will not help much nor will any other management approach.

There is an important role for the executing industrial contractor in this process. Most of the necessary data will actually be produced by the contractor. Some of the risk versus reward analyses will also be made by the contractor. Some of this process is already taking place, but to bring about a

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

more comprehensive understanding of supply chain risks, more focus will be needed.

To translate these judgments into action, the committee sets forth the following recommendations. Since all of the issues are embedded in the acquisition and logistics processes, the committee gives USD(AT&L) primary responsibility, but envisions a special role for DIA's TWD.

RECOMMENDATIONS

The committee's recommendations reflect several of the themes put forward in the body of the report. The impact of component denial is not a static estimate. The risks entailed in depending on a foreign-produced component are embedded in the strategy of supply management and the diversity of the impacted operational system or force. The size and power of the globalized commercial marketplace are such that we must find a way to exploit the marketplace's value for our security. The risks and benefits of this exploitation are at least as much an issue of acquisition and logistics strategy as they are of estimating foreign intent. The viability of the future assured domestic supply of critical components for the DoD is dependent on the health of the U.S. industrial base in these sectors.

The committee believes that any systemic approach to determining the vulnerabilities and risks of foreign supply for DoD must involve the DoD organizations responsible for acquisition and logistics as well as DIA's responsibility for estimating the capabilities and intentions of foreign countries. Therefore, the committee's recommendations are directed at USD(AT&L) as well as DIA.

These recommendations might be considered as going beyond both the original statement of task and the stated portfolio of responsibilities of the sponsor (DIA TWD). However, the committee believes the subject warrants the integration of the technology warning function into a broader context of supply chain risks and assurance. Without this broader context, warning cannot be properly evaluated.

While this issue of warning is partly an intelligence function, it must also comprehend technical details at the system level and at the level of lower tier suppliers to the systems as well as the operational significance of the risks of supply availability.

Recommendation 1. USD(AT&L), in collaboration with DIA, should develop a system for monitoring the risks of component unavailability within

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

the procurement and operating elements of DoD. The committee does not believe it is practical to create a detailed database for this purpose. Rather, the responsible procurement and operational authorities in the armed services, the defense agencies, and the combatant commands should regularly assess their vulnerabilities and the sources of these vulnerabilities and recommend mitigation action.

- A self-certification approach by USD(AT&L) should direct the services and defense agencies to annually prepare a product and supply chain assurance report that identifies important vulnerabilities, potentially significant operational consequences, and recommended mitigation actions. This will require supporting assessments by subordinate organizations for each service and agency. This body of data, assessments, and recommendations will form the primary source of authoritative information from which DoD-wide judgments can be made regarding supply chain vulnerability and impact. It will also be an important framework for the TWD in executing its technology warning responsibilities. The committee believes that the current set of DoD directives and guidance documents available to the program managers and their respective supervisory chains are an adequate tool for establishing the priorities for each DoD procurement activity. These data and judgments should be shared with the combatant commanders to permit them to assess the operational consequences of these vulnerabilities for their missions.
- USD(AT&L), in cooperation with DIA, should analyze these annual reports to identify DoD-wide vulnerabilities that might not be detected by the individual services and agencies and to warn of worrisome trends in the integrity of the supply chain, ensuring it is not compromised by foreign supply sources. A small staff element at the OSD level would be adequate and appropriate. DIA TWD should be an integral part of this analytic process to enable the integration of information about supply chain vulnerabilities with intelligence relating to foreign sources and foreign intrusion into U.S. sources. The analyses should be made available to the services, agencies, and commands as they are produced. The analysis should be particularly concerned with the following areas:

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

—Where there is a lack of war reserves or stockpiles.
—Where a weapon system is uniquely in the U.S. inventory and therefore cannot tap into worldwide depots.
—Where developing an alternative source of supply requires significant lead times.
—Where the DoD has developed sole-source, single-solution capabilities.
—Where critical technologies have migrated offshore or been developed there in their entirety.

- Annual updates of the guidance documents should be made available to the program managers and their respective supervisory chains based on the analysis of the program reports from the acquisition, logistics, and operational organizations and other relevant factors.

Recommendation 2. USD(AT&L), in collaboration with DIA, should develop a system for monitoring U.S. industrial health in strategically important global commercial market sectors that are critical to the availability of components for DoD. If trends toward unacceptable risk are identified, USD(AT&L) should formulate actions to mitigate the situation. It appears to the committee that this monitoring responsibility is directly within the charter of the Office of Deputy Under Secretary of Defense (Industrial Policy) and it should be the lead office. The Defense Industrial Base Capabilities Study (DIBCS) series undertaken for the Office of Deputy Under Secretary of Defense (Industrial Policy) has several features that appear to be a good basis for monitoring industrial health.[3]

The committee believes that the set of major strategic and critical U.S. industrial capabilities identified earlier justify the investment of large DIA TWD resources to monitor for and analyze major changes in global capabilities. These capabilities include network creation and management and information management; the integration of IT components; and systems integration. Subsequently, these capabilities must be matched to the needs of particular military organizations. There are four areas of future technological and industrial advancement that also warrant close monitoring by

[3]The entire DIBCS series may be viewed online at http://www.acq.osd.mil/ip/ip_products.html. Last accessed on February 13, 2006.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

DIA TWD: IT components, IT services, nanotechnology, and biotechnology. Of particular interest should be any developments at the interfaces of these four technologies. Finally, the DIA TWD should focus its management resources on tracking global capabilities in nuclear weapons; missile defense systems; space systems and space control; submarine construction; aircraft stealth and counterstealth; underwater detection/classification/targeting and underwater stealth and counterstealth; and electronic intelligence acquisition and analysis.

Recommendation 3. USD(AT&L), in collaboration with DIA, should organize a systematic method of assessing the health of military systems integration in and for the DoD as well as that of potential coalition partners and adversaries. The committee believes this task will require broad experience and judgment and should be undertaken with the assistance of expert external advisory bodies.

REFERENCES

DSB (Defense Science Board). 1999. Final Report of the Defense Science Board Task Force on Globalization and Security. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology. Available online at http://www.acq.osd.mil/dsb/reports/globalization.pdf. Last accessed on February 14, 2006.

NRC (National Research Council). 2005a. Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future. Washington, D.C.: The National Academies Press.

NRC. 2005b. Avoiding Surprise in an Era of Global Technology Advances. Washington, D.C.: The National Academies Press.

Spencer, Jack, ed. 2005. The Military Industrial Base in an Age of Globalization: Guiding Principles and Recommendations for Congress. Washington, D.C.: The Heritage Foundation. Available online at http://www.heritage.org/Research/NationalSecurity/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=81559. Last accessed on February 14, 2006.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Critical Technology Accessibility

BACKGROUND

In 2003 the Defense Intelligence Agency (DIA) requested that the National Research Council (NRC) establish the Committee on Defense Intelligence Agency Technology Forecasts and Reviews (the DIA Committee) to conduct meetings with the intelligence community in order to develop study topics relating to technology warning. The committee was formed and met with interested parties to understand the methodologies and strategies for the application of identified technologies of interest to the DIA under development by the United States and by its allies.

The DIA Committee reviewed information from government sources on technologies under development abroad, by other nations, and met with the DIA to discuss the potential for these technologies to become study topics.

The DIA Committee was asked to produce a report based on its discussions with the intelligence community that examines the capabilities on which U.S. warfighters depend and identifies the potential for adversaries to threaten those capabilities by exploiting evolving technologies (NRC, 2005a). The report proposed a methodology for technology warning and tested this methodology against several scenarios in the subsequent chapters.

It was the intent of both the DIA's Technology Warning Division (TWD) as sponsor and the NRC as convener that this first report would

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Box 1-1
Statement of Task

The NRC will impanel an ad hoc committee of experts to respond to the following questions:

A. What products/components/technologies currently being solely procured from foreign suppliers could significantly disrupt U.S. defense capabilities if access to them were denied (through conflict, embargo, treaty, etc.)? What countries are the principal suppliers of these products/components/technologies? What would be the impact of such denial? What is the risk that such denial may occur? What alternatives should be considered and in what time frame?

B. What emerging technologies/products that, if the United States chooses not to pursue domestic production, could significantly disrupt U.S. defense war fighting capabilities if access to them were denied? What countries might be the principal suppliers of these products/components/ technologies? What would be the impact of such denial? What alternative procurement methodologies should be considered for future acquisitions and in what time frame?

establish the foundation for a long-term collaborative relationship to examine technology warning issues, and so a standing committee was created for this purpose. The Standing Committee on Technology Insight—Gauge, Evaluate, and Review (TIGER) proposed five study topics to the TWD, which chose one of them. The Committee for Critical Technology Accessibility was then organized to respond to the two questions posed in the statement of task (Box 1-1).

INTRODUCTION TO THE ISSUE

There has been a steady increase in the influence of globalization as a part of the private, commercial, and national security activities of the United States (DSB, 1999; NRC, 2005a, 2005b). "Globalization" is defined here as a movement toward a marketplace for products that is global in extent and served by an industrial base for producing those products that is global

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

in extent as well. There are many reasons for the acceleration of this phenomenon. The committee will briefly discuss a few to justify its admonition against trying to roll back this inevitable trend.

The conclusion of the cold war erased the great pressure against global trade that had been part of the deadly struggle for survival between the Soviet Union and the West. Without that pressure, there has been diminishing reason to constrain trade, and economic opinion holds that open trade between societies will provide economic advantages to all parties.

In parallel, advances in information technologies (ITs) and the proliferation of IT products have given a large portion of the globe's more than 6 billion people access to information. This phenomenon has stimulated innovation throughout the world by dispersing both the knowledge needed to make the products and an understanding of the rewards available to those who produce.

This situation has led to a monumental increase in economic activity across the developed world. From 1989 to 2005, world gross domestic product (GDP) increased from $17.4 trillion to $40.9 trillion and the U.S. GDP increased from $5 trillion to $11.7 trillion (World Bank, 2005). Although the United States maintained its position in economic activity, more than $23 trillion was added to GDP in the rest of the world. This increase in market potential has given rise to many new markets, particularly for the new IT products and their producers in many countries. It has driven down the price of products, vastly increased the number of consumer products, and broadened the base for economic growth in most parts of the world. Globalization is a fact of world economic activity testified to by statistics from the DoD (Box 1-2).

Box 1-2
Excerpt from *Annual Industrial Capabilities Report to Congress*

Examples include global commercial markets like information technology and integrated circuits where U.S. defense applications represent about 1 percent and 1-2 percent of the global market, respectively; and steel where direct DoD sales represent 0.4 percent of the U.S. market and 6.3 percent of the U.S. market when also including indirect DoD sales (commercial product purchases). (DoD, 2005, p. 7)

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Fields that were just developed by American or allied country firms have evolved into global arenas, where key developmental and manufacturing activity is as likely (or more likely) to happen in Eastern Europe or Asia as in the United States or Western Europe. U.S. firms are investing large sums in China and India, with Intel, as an example, having announced a 5-year, $1 billion investment in India alone.[1] Business models have also evolved significantly, with multi-billion-dollar technology firms such as Dell, Qualcomm, and Altera developing and designing their products, which are then manufactured by U.S. or Asian firms such as Taiwan Semiconductor Manufacturing Company. The intellectual property market has become global, with firms such as ARM in the United Kingdom and IBM licensing key intellectual property items to generate significant revenue.

The open source software movement serves as another development model: It promotes the sharing of intellectual property in order to build the best possible products in the shortest possible time.[2] This philosophy opens up intellectual property to all players, not just paying customers, and leverages the capabilities of talented engineers and scientist on a truly global basis. Key open source products, such as the Linux operating system or the Apache enterprise server, are starting to be adopted by mainstream markets as multinational firms promote them.

These global market changes impact decision making on the acquisition of technology. The rapid evolution of products such as cell phones, which have an expected life of 2 years, drives technology cycles with much shorter time frames than military products, which typically operate for a decade or more. Global intellectual property markets enable engineers in other countries to have access to key U.S. dual use technologies and give U.S. engineers access to foreign technologies. Certain regions around the world have industrial policies to develop cutting-edge centers for technology and manufacturing, such as Singapore's investment in biotechnology or China, Korea, and Taiwan's investments in semiconductor manufacturing. As U.S. companies respond to these global market forces, they make business decisions that drive research and manufacturing capabilities offshore, with implications for military preparedness.

---

[1]For additional information, see http://www.rediff.com/money/2005/dec/05intel.htm. Last accessed on February 13, 2006.

[2]For additional information, see http://www.OSS-institute.org. Last accessed on February 9, 2006.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

This trend means that many new products that support DoD's mission are being created by this globalization process (Spencer, 2005). Design choices that favor improved system performance must include the possibility of using products from this global commercial marketplace. The massive global profits from these products provide the basis for investment in further advances in product performance. Because many products with improved function, price, and schedule will be available only from these global commercial sources, military systems designers will inevitably be faced with choosing between them and domestic products with nonoptimal performance. Further, the use of products from the global marketplace, coupled with continuous technology refreshment to keep up with the state of the practice, will continuously reduce ownership cost while increasing reliability and mission performance, making them appealing to defense engineers.

This situation prompted TWD to raise two sets of questions. The objective of this report is to try to answer these questions, to suggest further study that would be useful in pursuit of the answers, and to address some related topics that might help with the dilemmas implicit in the questions. Appendix C is a compendium of related reports that discuss the broader issue of globalization and may provide the reader with additional context for this report.

HOW TO ANSWER THE QUESTIONS

In attempting to answer these questions, one needs to understand a number of things. First, there are current considerations:

- Which items are now being procured exclusively from foreign sources?
- What would constitute substantial disruption of U.S. defense capabilities if access to these items were denied?
- How likely is it that access will be denied?
- How could the impact of denial be mitigated?
- What might be the consequences of mitigating the impact?

And, for the longer term, still other considerations:

- Which emerging technologies and products will be important to DoD capabilities?

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

- What might be the industrial base for these technologies and products?
- Are the risks of denial likely to be unacceptable for DoD?
- How could these risks be mitigated?

The risks and impacts of foreign source denial[3] are embedded in a larger supply management[4] issue and are similar to the risks and impacts of other potential sources of supply disruption—for example, plant destruction by fire or explosion, floods, strikes, or transportation failure. Another cause of component denial is obsolescence. Since the technology for many products changes more frequently than the procurement cycle of the DoD, fielded systems often need replacement parts that are obsolete and no longer available from the open market. The likelihood of each kind of denial—supply disruption and obsolescence—must be assessed. Mitigation actions for both will have cost, schedule, performance, and other consequences. A decision maker must act in the context of his or her whole management responsibility.

THE RISKS AND IMPACTS of foreign source denial are embedded in a larger supply management issue and are similar to the risks and impacts of other potential sources of supply disruption—for example, plant destruction by fire or explosion, floods, strikes, or transportation failure.

[3]By "foreign source denial" is meant the risk that the foreign source of a product will deny the defense establishment access to that product.

[4]By "supply management" is meant the acquisition, transportation, storage, distribution, asset visibility, and depot operations of military operations and supplies.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

A perspective on future access to emerging technologies and their products cannot be established on the basis of data alone. For each technology, there needs to be a collective assessment of the risks, their potential impact, and the consequences of mitigating those risks across the DoD and beyond. The committee does not believe such assessments exist nor does it believe there is a systematic effort to undertake them.

The committee looked for and did not find a database of foreign products/components being procured by the DoD and decided to not attempt to develop such database on current foreign sourcing across the vast numbers of DoD systems. Nor did the committee assess, for each foreign component, the impact of denial on operational capability, mitigation opportunities, and consequences. Finally, it did not develop a collective assessment of the technological and industrial trajectory of emerging technologies that promise to be key to our nation's security. However, it did listen to government plans and perspectives, discussed the issues with recognized experts,[5] reviewed past literature, and obtained and analyzed certain relevant information. In addition, the members of the committee arrived with substantial background, service, and expertise in these matters.

As a result, the committee believes that many important judgments can still be made with respect to the questions raised by the sponsor, and it has undertaken to do so in this report. As it attempts to answer these questions, the committee demonstrates some of the logic of what it believes must be a much more systematic and holistic approach to these assessments across the entirety of the defense and national security area. The elements of that approach are addressed following the members' response to the questions.

QUESTION A: WHAT IS THE RISK OF DENIAL OF CRITICAL PRODUCTS FROM FOREIGN SOURCES?

Based on the information received and its own members' knowledge, the committee was unable to identify any product or technology currently being solely procured from a foreign supplier that could significantly disrupt U.S. capabilities or operations. The committee did not come to this stark judgment without substantial debate and will present the underlying facts and assumptions for the reader's examination.

[5]See Appendix B for a full list of presenters.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

BASED ON THE INFORMATION received and its own members' knowledge, the committee was unable to identify any product or technology currently being solely procured from a foreign supplier that could significantly disrupt U.S. capabilities or operations.

First, the committee does not contend that it has performed a comprehensive and complete survey of all the items procured by DoD exclusively from foreign sources and on which the department depends for specific capabilities. The incomplete state of knowledge at DoD and its primary suppliers does not appear to permit such a survey at this time. However, the committee did consider the foreign content of many of the major DoD systems and how denial of access would impact DoD capability or operations. It also explored some worst-case assumptions to test whether detailed data were a prerequisite for making strategic judgments. While the committee does believe that a more detailed and structured approach to evaluating supply chain risk versus reward for all defense procurements is essential for assuring the nation's defense capabilities, it does not believe that detailed information about foreign-sourced components will, by itself, lead to better judgments.

That is not to say that DoD's systems do not have foreign content. Quite the contrary: Very few DoD systems do not have foreign content that is critical to their function (Gansler, 2006). However, as long as DoD manages its supply chain well, the impact of critical component denial can be mitigated.

To answer the questions proposed by the sponsor, the committee used the knowledge available to its members on current DoD systems, an understanding of the suppliers of these systems, and some understanding of the operational circumstances facing our forces.

The committee concludes that the nature of the scenarios in which the use of force would be considered and the diversity of the content found

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

in the systems of a major combatant command rules out the possibility that foreign denial of access to current products could have a substantial effect on combat capability at this time. There are several reasons for this conclusion:

1. Over the last 60 years, the United States has created an industrial base for the domestic supply of every major strategic and critical military capability that requires specialized and expensive facilities. In particular, it has retained the industrial capabilities to produce nuclear weapons; missile defense systems; space systems and space control capabilities; armored vehicles; submarines and ships; aircraft; aircraft stealth and counterstealth; and underwater detection, classification, and targeting as well as underwater stealth and counterstealth. This does not mean that the primary systems do not have foreign content, but that the nation is able to manage the content, advantage, and risk associated with the foreign components in those systems.
2. There are exceptions in that there are some strategic and critical capabilities for which the material components might well be nondomestic. For example, the capabilities for network creation and management and information management are strategic and critical for U.S. military forces as well as for those of its allies. However, the critical domestic capability for these functions is the ability to integrate systems and match them to the operational needs of the military organization. It is the systems integration ability that is so critical, not the individual components. The United States has a capable industrial base for integration, and there is little risk that it will be subject to dominance by a foreign supplier very soon.
3. "You go to war with the Army you have." The committee considered many of the planning scenarios used to evaluate future military force needs. It believes that most of them involve military action with the forces available at the time of the decision. This come-as-you-are type of operation does not provide an opportunity for a foreign source to deny the component and significantly impact current operations. The components should already be in the system. Further, there should be a reserve of materials for all components to serve as spares and provide additional capability during operations. If reserves planning is not done well, it will not only be foreign suppliers that are the problem. A shortage of material during opera-

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

tions can necessitate starting up the manufacture of a domestic part as well, and the lead time for that manufacture is likely to last much longer than the conflict. There was such a case in Operation Iraqi Freedom with batteries. The rate of usage was misjudged for the purpose of estimating the size of the reserves, and emergency action was required to produce a supply.

4. The supply reserves provide a buffer if a foreign supplier denies access or if any number of other contingencies might interrupt access to a needed component. Many observers have noted that currently there are shortfalls in reserves and that procurement authorities are often reluctant to spend their resources for these reserves. The committee does not know whether this is a result of careful risk calculation or a management failure, but if this supply management function is done properly, it will provide a forward buffer of time between an action of denial and the impact of that denial. Denial action by a foreign source may be a warning of further strategic intent and will stimulate action in the supply management domain. Further, commonality of systems with coalition partners provides worldwide depots for certain parts and components.
5. The globalized marketplace has rules of its own. Being an assured supplier is as important in the commercial sector as it is in the military. The mechanisms available for a determined adversary to selectively deny a U.S. military procurement while continuing to supply its global commercial clients would be complicated. The committee's assessment is that such denial will not likely have substantial impact and that disadvantages to the supplier of becoming known as an untrustworthy supplier should act as a deterrent. The committee does not believe this deterrent can be fully relied upon to assure access to strategic and critical capabilities, because these suppliers, whether foreign or domestic, are still vulnerable to manipulation by a determined adversary. However, this market dynamic should be taken into account in the government's assessment of the risks and rewards of sourcing supplies from the global market. This assessment applies not only to military products but also to the global transportation and distribution systems, which will involve foreign providers. Disruption of the global supply and distribution chain can have ramifications as serious as disruption of component supply.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

6. A military force, especially in today's joint warfighting environment, is a very diverse set of entities and does not contain many strategic, single-point failure modes. For the strategic and critical category of assets, sourcing has been determined under strict control regimes, and these failure modes are carefully monitored. For other capabilities, the failure modes are highly distributed. Although almost all the elements of current and future DoD force capabilities will have foreign content, the suppliers of this content are manifold, diverse, and not amenable to coordinated denial. Finally, not only are the suppliers a diverse group but the processes by which the components are procured are also diverse and not amenable to coherent action. The committee believes this diversity of sources will intensify:

> Many authoritative observers, including leading U.S. aerospace executives, view increased globalization—including foreign outsourcing and other types of international alliances and collaboration—as a key strategy for maintaining a healthy U.S. industrial base following a decade of megamergers. (Lorell et al., 2002, p. 2)

The committee believes this answer and the elements of its rationale point to a more systematic approach to managing supply chain risk by the DoD in the future.

QUESTION B: HOW CAN THE FUTURE U.S. INDUSTRIAL BASE BE MANAGED TO ASSURE ACCESS TO CRITICAL PRODUCTS AND TECHNOLOGIES?

What about more strategic, long-term denial? The trouble with comforting come-as-you-are scenarios and military capabilities is that they do not foresee the possibility of a more strategic denial that could impact U.S. military capability.

If the United States were to become strategically dependent on a single or coherently manipulated foreign industrial base for items that are critical or for which the regeneration of a U.S. industrial base would take a long time, the risk would be unacceptable. The committee does not see any signs of that at this time, but the possibility should be taken into account when determining what the U.S. industrial base needs to be for defense purposes.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

IF THE UNITED STATES were to become strategically dependent on a single or coherently manipulated foreign industrial base for items that are critical or for which the regeneration of a U.S. industrial base would take a long time, the risk would be unacceptable. The committee does not see any signs of that at this time. . . .

Current Capabilities

There are several industrial capabilities in the United States that the nation has chosen to retain to assure access to critical military capabilities. These so-called "national arsenals" are the basis for the strategic systems that are clearly critical to our security. The principle of domestic ownership and U.S. control is so natural that the matter of their retention has not often been questioned. As mentioned in an earlier section, these primary industrial capabilities are nuclear weapons; missile defense systems; space systems and space control capabilities; armored vehicles; submarines and ships; aircraft; aircraft stealth and counterstealth; and underwater detection, classification, and targeting as well as underwater stealth and counterstealth.

There is a subset of the industrial base, termed the "arsenalized" environment, that covers industries and technologies whose center of gravity is U.S. military consumption, and the large companies involved in the development and manufacture of these products are in effect captive to the military (in other words, they are "arsenalized"). In this environment, there will be explicit government controls over who manufactures the products, who has priority access to the products, and what export controls are required for any international business. Good examples of this environment are the nuclear submarines and submarine-launched ballistic missiles. For these capabilities, the military is the only customer of a captive domestic indus-

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

try, and they are considered strategically critical by the DoD. The committee's review of several strategic and critical industries leads it to conclude that none of these industries should be left for foreign entities to take over nor are they likely to be. Because of the strict controls maintained over these industries, the committee does not see a serious risk of denial for their products. Even for these capabilities, there may be a temptation to enhance performance or cost by introducing foreign content with attendant risks. Given the controlled environment, the government will be able to avoid these risks by denying itself these performance or cost advantages. The particulars will be different for each case, but the choice cannot be avoided. It would be convenient if all-domestic options with full advantages were available to the designers, but the committee does not see that as a credible outcome given the globalization of the manufacturing sector.

Future Industries

For emerging industries, the situation is not quite as clear. The committee identifies four areas of future technological and industrial advancement that warrant discussion: (1) information technology (IT) components; (2) IT services; (3) nanotechnology; and (4) biotechnology.

The committee notes that it is not just the components or functional products in these sectors that count. The United States is currently dependent on foreign sources for much of its machine tool needs, and semiconductor component manufacturers in this country are substantially dependent on some critical foreign-sourced tools for their domestic production.

The committee cannot imagine a healthy U.S. economy without strong U.S. industrial participation in the IT sector. It does not think the United States must host a capability to make every product in this sector, but it does believe we must have within our domain some industries that are leading participants in this broad, global marketplace. In addition, DoD must continue to invest in specialized industrial capabilities for critical functions such as cryptology and radiation-hardened and electromagnetic-pulse-resistant component design and process development.

Without that investment the ability of both the national economy and the DoD to leverage this crucial set of products will be unacceptably compromised. Please note again that the DoD is and will be heavily dependent on the existence of a healthy domestic commercial sector to assure its system needs.

IT services include many forms of the capability to manipulate, store,

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

and exploit data and information. The committee sees no sign that the United States will somehow not participate strongly in this market sector, but it wishes nonetheless to aver that this capability is strategic and critical. Further, the IT sector includes still another issue of concern—namely, the hidden capacity for an unfriendly perpetrator to manipulate performance, a concern that the committee addresses later in the report.

It is difficult to project with precision the specific strategic and critical capabilities that will come from the nano and bio sectors. However, the potential of these technologies to separately and jointly create profoundly new materials and capabilities means that we must assume that they can and will produce strategic and critical capabilities for our security. One key example is DNA-based high-speed/high-capacity computing, where nano-bio synergisms become an enabler for IT. The power of these learning algorithms far exceeds that of today's biosimulated neural net architectures (NRC, 2005a).

The committee believes that in each area the advances in technology will be largely driven by global commercial markets rather than by the U.S. military and national security agencies. The size of these markets and the research and development levels they support will overwhelm any financial participation by the U.S. government. For our nation and others, public and private investment is aimed at assuring that the national economy is positioned to gain value from these technology advances. The central thrust is not defense or national security.

Using Both Global and Captive Domestic Sources

Whether for future products and services or for the more mature products currently used by DoD, the committee can conceive of no sourcing strategy that does not include some use of the globalized marketplace while maintaining some "arsenalized" sources of elements critical to our national security. If necessary, DoD can, as it has in the past, invest in specialized capabilities that will assure its own missions and contribute to the nation's participation in the global commercial marketplace. DoD can also, as it has done before, take advantage of products of the commercial marketplace either as is or with modifications.

For this strategy to be effective and for DoD to have assured access to these capabilities, the committee believes it will be necessary for the United States to have healthy commercial industries in each market sector. While the nation may not need to have within its sovereign domain the facilities

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

and capabilities to manufacture everything that DoD needs, it will be important for DoD to have access to trusted sources of domain expertise, including skilled systems designers and smart buyers of products and services that may have foreign content. This is not be likely to be the case unless we have healthy and competitive industries from which to draw these skills.

The committee's recommended strategy is dependent on the broad-based economic health and competitiveness of the nation in more ways than just those arising from the globalization of the industries upon which DoD depends: namely, in order to afford the level of defense expenditures that characterized the last several decades.

Sustaining a healthy and competitive economy is one of the primary objectives of the nation. It depends on all parts of the government and involves risk and reward assessments well beyond the military dimension. The committee has not attempted to formulate a comprehensive strategy to achieve this grand goal but accepts it is as a manifest objective of the country and assumes that it will be achieved to some degree. While the committee believes that success will require the umbrella of an effective national security capability, it does not believe that the placement of defense expenditures will be a dominant economic factor. Instead, as in the past, we will be forced to deal with the trade-offs between performance, risk, cost, and schedule that accompany sourcing the materials for our security from a mix of global and captive domestic sources.

The Role of Systems Integration

Managers and operators know that they succeed when they are able to harness all the elements of an entity or a system and apply their attributes to the mission of the entity. For military operators, the integration of sensors and detection systems, maneuvering controls, target classification and weapons fire control provides for the fast and effective operation of the whole system. Each element of the system can be properly engineered, but if the elements do not work efficiently together, the system will not perform well.

Box 1-3 gives an example of what a systems integrator does. The integrator looks around the world for the best available technology, products, and software applications. Analyses must be conducted with regard to relative performance, reliability, supportability, produceability, ease of operation, ease of maintenance, technology refreshment cycles, obsolescence con-

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Box 1-3
Example of Systems Integration

To demonstrate the concept of systems integration the following analogy is offered. Imagine that you have just brought home a new flat-screen HDTV, a surround sound system, a VCR, and a DVD player, each of which came from a different manufacturer, to work with your cable box. You now have five remotes sitting on your lap and you are trying to figure out which does what. You can operate the systems together by plugging in the correct leads and individually controlling each of the five remotes. Yes, this is confusing and probably you'll need all five operating manuals near your chair, but it will work. Then you discover that by entering each manufacturer's product codes into your cable remote, you can operate all of your equipment from that one remote control. Congratulations, you are now a systems integrator! Look at what you have accomplished: You have lessened complexity and eliminated steps, and now you can execute commands an order of magnitude faster than you could with the five remotes.

siderations, implications of commercial off-the-shelf (COTS) products and support from the commercial sustainment base, and total ownership cost implications, from design throughout the life and disposal of the system. The analysis of this vast array of information leads to decisions on product selection and overall systems design to produce the most effective system at the least ownership cost. All of this is inherent in the system integrator's trade-space analysis.

Today we rely on systems integration as a mitigating factor in enabling the infusion of foreign technology. In the early days of the cold war our nation had a self-contained force and program management structure for major strategic and critical capabilities. The management construct for these systems provided for a very controlled process with adequate resources and authority to produce effective military systems. Examples include the application of nuclear power to submarines, land- and sea-based ballistic missiles, space surveillance and reconnaissance, and global communications, command, and control.

We now have many examples of major successes in warfighting systems that use COTS processing components and middleware for antisub-

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

marine warfare and surface ship combat systems. Commercial chips sets are used in military aircraft. The rigid enforcement of military-specific instructional set architecture that demanded programming in noncommercial languages has migrated to the use of standard commercial languages, applications, and tools. The result has been an extraordinary reduction in time to design and cost, with attendant increases in availability as well as continuous technology refreshment by leveraging the commercial industrial base. The integration of today's defense electronics systems starts with open architecture principles and proceeds through ever-evolving spirals that lead to mission effectiveness and lower ownership cost.

One of the dramatic examples of successful systems integration with an open architecture is the Navy's Acoustic Rapid COTS Insertion (ARCI) program. Use of an open, capabilities-based (versus requirements-based) business model allowed the Navy to acquire best-of-breed technologies across a broad range of communities. Acoustic superiority was enhanced by rapidly updating the submarine fleet with state-of-the-art functional capabilities, made possible through the integration of skills from the Navy, academia, and small and large businesses. These skills were woven into a "fabric" to capture the best of each organization's strengths, which became known as the Advanced Processing Build.

Under this process, the sonar system was partitioned into processing strings to leverage the strengths of developers and to enable a sequential and incremental capability insertion plan. The ARCI prime contractor, Lockheed Martin, is the system integrator and provides system management; it also developed the active and passive spherical-array and high-frequency passive-array functions. Digital System Resources developed the towed-array functions, and the Applied Research Laboratory, University of Texas, developed the high-frequency active-array functions; Johns Hopkins University served as the test program lead. Raytheon and others continue working as a team under a well-defined plan. This dynamic interweaving of talents has provided dramatically enhanced submarine acoustic performance, with reduced development cost and increased system availability.[6]

[6]For additional information, see http://www.lockheedmartin.com/data/assets/881.pdf; http://www.navalsupport.com/pdfs/USS_Virginia_C3I.pdf; http://www.nationaldefensemagazine.org/issues/2003/Aug/Navy_Courts.htm; and http://www.rti-world.com/list_db_data.php?section=PRESS&pageType=pressitem&contentID=531. Links last accessed on February 9, 2006.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

The above is a dramatic example of why systems integration is one of the strategic and critical capabilities necessary to create superior military forces. It provides the ability to integrate disparate technical and operational elements into a coherent entity that is tailored to the mission objectives of the enterprise. Some of the ingredients of this capability include

- Access to technical and operational understanding of all of the elements of the enterprise (this includes detailed understanding of the threats encountered as well as an understanding of the dynamics of the host platform; interactions for electromagnetic compatibility; requirements for heat, cooling, vibration, inertial loads, fuel, space, weight, moment, and so on).
- The ability to create sophisticated algorithms and integrate them with a myriad of applications into open and scalable architectures.
- Experience in integrating large systems or aggregates of systems and elements in order to apply hard-learned lessons related to configuration management, interface coordination, testing and validation, product data models, data exchange, and a myriad of processes and tools so critical to successful systems integration.
- Confidence that no aspect of a problem is beyond the comprehension of the integrating organization. System integrators know that it is usually easier to search globally, find, and apply a solution than to try invent it from scratch. They have become accustomed to reliably finding, understanding, and applying solutions to obtain desired performance and achieve success. Through the system integration and trade-space analysis process, they can develop total systems that perform better, faster, and cheaper—sort of an industrial equivalent of the military loop of warfighting elements: observe, orient, decide, act (OODA) (Coram, 2002). When the trade space is expanded to include the global technology and industrial base, the ability to achieve better results is obviously magnified.

A Defense Science Board report on globalization and security states that globalization offers tremendous benefits for U.S. security that, if embraced by the DoD can counter the associated risks (DSB, 1999). The Heritage Foundation report *The Military Industrial Base in an Age of Globalization* makes the point that "not participating in the global defense marketplace will increase, not decrease, risk to the U.S." (Spencer, 2005, p. 20). It goes on further to state as follows:

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

> In providing the best systems, U.S. acquirers will look routinely beyond U.S. sources. This practice encourages innovation and provides better products at reduced costs. The question is not whether a given commodity, system, or material is available from a U.S. company on U.S. soil, but whether these products are competitively available through the global marketplace.

Systems integration, as performed by major defense industry prime contractors and by those responsible for integrating disparate systems into coherent forces in the field, is an essential national capability that must be sustained and enhanced through the global trade space (DSB, 1999). U.S. industry does not have a monopoly on the most cutting-edge technology, analytical tools, or precision manufacturing machines. It does, however, have the ability to integrate and deliver to the U.S. military the best and most lethal combat systems, which can observe, orient, decide, and act better than any others in the world.

However, experienced systems engineering professionals have recently expressed concern that U.S. competence in systems integration is not being exploited to its full potential by either the government or its serving industries. The primary reasons for their assertion are the growing bureaucracy and decreasing flexibility of the DoD acquisition process to trade off between total ownership cost, performance, and schedule, as well as DoD's inability to effectively coordinate and integrate requirements across and within the respective services. These weaknesses on the part of the government also extend into the serving industries and weaken the ability of the industrial sector to do the sort of integrating of mission, capability, cost, and schedule trade-offs that it did in the past (NAVSEA, 2002; NDIA, 2002).

Ultimately, if the U.S. economy and broad industrial base are not healthy, the industrial sector could lose its ability to provide integration services to the government, and the broader U.S. technological base from which the DoD draws could weaken as well. This weakness will be reflected in the loss of skilled people and facilities that are necessarily the source of this expertise.

The committee suggests that monitoring and assessing U.S. national strength and competence in systems integration is a vital task. If that strength begins to deteriorate, it could signal the possible degradation of U.S. defense capabilities.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Managing the Exploitation of Globalized Commercial Markets

Many products valuable to the military are dominated by commercial markets and globally distributed suppliers, raising concerns about assured supply. Much of this concern about the reliability of foreign sources has been amplified in recent years by the increasing impact of global markets and globalized industries. Global commercial markets are immense and overwhelm the defense market, substantially diminishing the financial leverage once available to the government to influence the behavior of the commercial market.

However, the size of the marketplace and the promise of large quantities attract the competitive capabilities of a broad range of enterprises from across the globe. One result is the availability of advanced capabilities at greatly reduced prices. This gives a system/product designer unprecedented flexibility with respect to product cost. For example, the Global Positioning System receivers that are essential for our armed forces are more capable and much less costly than if DoD were the sole buyer. There is great leverage in the adaptation of commercially available capabilities for military purposes.

DoD already has some experience in dealing with globalization. In the early 1980s, there was great concern that the Japanese, led by their manufacturing capabilities, would displace United States integrated circuit components producers and leave DoD no alternative but to source from the Japanese. Following a set of recommendations by the Defense Science Board, the DoD intervened with several hundred million dollars and legislated collaboration initiatives between DoD and the component producers (DSB, 1987). Although there is still debate about the leverage provided by the DoD intervention, things did get better and there has been a 20-year period of solid performance by U.S. manufacturers.

In the early 1990s, there was a similar national concern about the trajectory of the flat panel display manufacturing sector. It was evident that the flat panel industry was leaving the United States and that DoD would be left with no alternative but to procure these items from foreign sources (NRC, 1995). In response, DoD organized a several hundred million dollar initiative to create and sustain a domestic supplier by subsidizing one or two companies and providing a limited but guaranteed market (Flamm, 1994). This business proposition was not robust enough to sustain the companies in the face of the overwhelming leverage of the commercial marketplace. In the end, the initiative failed and DoD procures flat-panel dis-

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

plays from foreign sources. Thus far, there have been no supply denial problems and the nature of the commercial marketplace provides substantial protection against an organized denial of these components. The manufacturing market is shared by several Japanese firms, some South Korean providers, and a growing Chinese presence. Although there have been some increases in the time for repair and return of these foreign-provided items that can impact system availability rates, this situation has been mitigated through the lay-in of additional spares. In the committee's judgment, this is a useful example to consider as decision makers address their foreign content issues.

Currently, DoD has an arrangement with IBM to provide application-specific integrated circuits from a trusted foundry (Carlson, 2005; DSB, 2005). This contract provides near-current technology from a domestic supplier within a defined process for assuring the security of the design inputs and the delivered products. This intervention in the global marketplace is possible because there are cutting-edge domestic capabilities operated by IBM. Market forces might, however, make this a less desirable course of action for IBM in the long run. The committee believes this situation will require monitoring in the future.

The printed circuit board (PCB) industry is another good example of a globalized industry. The NRC recently issued a report on the PCB industry highlighting the critical risk to military requirements (NRC, 2005c). Key issues include these:

- Because PCBs are customized to a product, they are unique to the product, whether it is an iteration of a DVD player or an avionics component for an airplane.
- U.S. military acquisition makes up only a small fraction of global requirements.
- U.S. production has decreased significantly, with the industry now centered in Japan, China, and Taiwan.
- While the United States has a strong lead in R&D, other countries are developing their academic and R&D support for the PCB industry.
- Industry technology cycles evolve quickly, with computer and cell phone life cycles driving shorter and shorter industry technology cycles.
- Life-cycle requirements for U.S. military products exceed those for commercial components by a factor of as much as 10. Since updat-

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

ing the technologies in these products calls for a cumbersome testing process for both the product and the system it is in, it is preferable to have access to older manufacturing capabilities.

- The United States has a significant requirement for maintaining products with obsolete technologies.
- Because military volumes are smaller by several orders of magnitude than standard commercial runs, leading vendors prefer their profitable high-volume business or demand a very significant premium for the high-paperwork/low-volume military business.

Currently, the U.S. military has the ability to access PCB products in a variety of ways. It can access products from vendors in multiple locations; it can stockpile some products; it can work with domestic suppliers; and it can reverse engineer and build limited quantities when required. The diversity of global suppliers provides substantial protection against a coherent denial of these products by a single nation.

In addition to the issue of depending on globalized sources of PCB products, the U.S. military needs access to some dedicated domestic manufacturing facilities to deal with the long life-cycle requirements for very small production runs and access to older (including obsolete) manufacturing capabilities that match the systems being used.

Placing Trust in Foreign-Supplied Components, Software, and Services

One of the underlying premises of the argument for having domestic suppliers for military systems is that domestic suppliers can be trusted more than foreign suppliers to supply reliable products. The committee does not believe that is a sound basis for assessing the trustworthiness of suppliers and their components. More factors than nationality should be considered in the process of acquiring assured components.

First, a determined adversary can also gain access to a domestic supplier. As experience in the intelligence community has shown, there is a great threat from the trusted insider. Further, the supply management discipline must account for inadvertent as well as intended component malfunction, whether from foreign or domestic sources. The committee believes that much of the risk of foreign supplier performance can be mitigated by intelligent management of supply sources, component certification, and adequate testing.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

As mentioned earlier, no foreign supplier can afford to be an untrustworthy supplier in the context of its predominant market. Procurement processes that take into account this motive will also mitigate the risk.

The committee believes that acquiring trusted components, software, and services is primarily a matter of sound supply management. It agrees that the nationality of the supplier can be an important factor but is only one of many. A component can be suspect in its availability or in its performance on many counts. In principle, the customer for the component must have procedures for certifying the trustworthiness of the supplier and its components. When the component is unique and specified for DoD, this process may take a very intrusive form. When it is a broadly available commercial component, the process will need to accommodate the motives and dynamics of that commercial sector.

An area of special concern is the hidden capacity for performance manipulation of software and services by an unfriendly perpetrator. As with the risk of faults intentionally embedded in integrated circuits, this potential risk is particularly troublesome because of the difficulties in inspecting and testing the products to detect the implanted flaws.

For this threat as well, the committee believes that a sound supply management process is an essential baseline for mitigation. To increase confidence in acquired software and services for truly critical and strategic functions, it will be necessary to acquire them from sources under a very strict control regime.

In the absence of a comprehensive control regime, it will be difficult to certify suppliers. Intelligence can play a role in assessing the potential for a supplier to manipulate a component. A coherent effort to do strategic damage to the United States is likely to have a detectable footprint. If the government becomes organized in its management of supply assurance and can identify areas of particular concern, intelligence assets can be enlisted to help in the process. The committee also notes that software and service products are often plagued by flaws or poor performance, so design choices for critical functions must use redundancy or other techniques for protecting against flaws of either variety—unintentional or intentional.

These judgments are not peculiar to foreign sources. Domestic sources that are not under a strict control regime are also vulnerable to adverse penetration. Both are liable to generate products with unintentional flaws.

The committee sees no single approach for assuring performance of software and services. Strict control regimes seem essential for truly critical functions. For situations where attractive products are accessed from an

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

uncontrolled global marketplace, mitigation will require accommodating design choices, rigorous inspection, and improved testing procedures.

The committee believes that DIA and the Assistant Secretary of Defense, Acquisition Technology and Logistics, should develop a concept and doctrine for exploiting the critical components available from the global commercial industrial base (Spencer, 2005). The price of avoiding all of these products because they come from foreign sources is too high in terms of system performance, cost, and schedule.

A STRATEGIC APPROACH

The issue of foreign participation in the creation of U.S. military forces has been complicated, troubling, and controversial for a long time. With all of the studies and reports produced on this subject, no set of policies or doctrine has emerged from this very political process that is generally acceptable to the many advocates for different approaches. Some are enthusiastic and cite the inevitability and promise of globalized markets. Others are very concerned by any substantial participation of foreign interests in the development of our military capabilities.

The committee has come to the judgment that progress can best be made by using a management process that accommodates the many advocacies of both the DoD and the Congress, within their current responsibilities and authorities. The risks and impacts of foreign component denial are similar to the risks and impacts of other potential sources of supply disruption. Mitigation actions for each potential source will have cost and other consequences. A decision maker must assess the likelihood of each type of supply disruption and the context of his whole management responsibility. The risks of foreign source denial are embedded in a larger supply management issue. The committee does not wish to imply that merely embedding this issue in the larger supply management issue will sweep the problem away. Supply management for the DoD is a daunting task without the complication of risks associated with foreign sourcing. It does argue, however, that if the government intends to be serious about this subject, it should deal with it in this way.

Key Assessments

1. What are the sources of the critical components? Critical means that the component is essential for the function that is the reason

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

for the procurement. For most systems, components at any tier of the system can be critical.
2. What are the risks identified with access to the foreign components? Whose judgment provided this risk assessment?
3. How do these risks compare with the other potential risks to supply access? Whose judgment provided this assessment?
4. What are the operational capability consequences of the various sources of access denial or uncertainty? Whose judgment provided these assessments?
5. What are the opportunities for mitigating these risks? What are the penalties associated with these mitigation options? Whose judgment provided these assessments?

Addressing Strategic and Critical Capabilities

Strategic and Critical System Capabilities Requiring Specialized and Expensive Industrial Facilities

Consistent with current policies and practices, the nation should retain the domestic industrial capacity to provide selected strategic and critical capabilities. Several industrial capabilities in the United States have been chosen for retention to assure access to their products. These so-called "national arsenals" are for strategic systems obviously critical to our security. The principle of domestic ownership and U.S. control has been so natural that the question of their retention has not often been raised.

In the committee's judgment, the capabilities that should be placed in this category of national arsenals include nuclear weaponry, submarines, space control, access to space, airborne stealth and countermeasures, and underwater stealth and countermeasures. These capabilities may be characterized as follows:

- Each is an absolutely essential element of our nation's security capability, and the committee cannot conceive of our nation being dependent on any other sovereign interest for its access.
- A high degree of secrecy is an explicit element of their leverage for our security.
- The industrial facilities for producing them are not part of the globalized marketplace. Such capabilities are created by nation states for national security purposes and the motivations that underpin their existence are exclusively national.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

The committee's review leads it to conclude that none of these capabilities should be or are likely to be left for foreign industries to fill and that there is therefore no prospect of their denial. It knows that some foreign products are and will be included in the makeup of these systems, but they will have been introduced under the management of a U.S. supplier under close government oversight who will have the opportunity, obligation, and competence to prohibit unacceptable risk for each capability. For this category of capabilities, there are strategic and critical industrial bases that must be sustained.

Strategic and Critical Capabilities Derived from IT

The United States needs the independent ability to create operational capabilities that are derived from the IT sector. Many of these capabilities are strategic and critical but do not rely on unique and heavy industrial facilities. Many of the components are an integral part of the massive, globalized commercial marketplace in this area. Because the technology advances in this domain are driven predominantly by the commercial sector, the committee cannot envision achieving superior capabilities here without some use of commercial products from a globalized industrial sector. The key to creating strategic and critical system capabilities is the ability to integrate these components into coherent networks and information systems that fit operational needs. Strategic and critical capabilities derived from IT include network-enabled operations; knowledge-based information management; and information operations.

It will be necessary to have access to the globalized set of products that can be integrated into the specialized systems needed for our nation's security needs. The committee believes that such access will be routinely possible as it envisions the evolving global marketplace and the military system applications. This access will carry the risks of disruption or denial by foreign adversaries, and these risks must be accounted for as the components are applied.

It will also be important to have the engineering and information management skills to create specialized IT components that will not be available from the global marketplace. This will require the engineering skills and some custom facilities to be able to design and build specialized components. This will often be done in secrecy.

A world-class skill base will be needed to integrate IT components and software into coherent systems tailored to specific needs. In the committee's

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

judgment, that is likely to be true for the United States over the long run if it plays a significant role in the global information systems marketplace.

The committee heard a compelling case for making sure that the nation does not lose all of its domestic capability to produce IC components. Current global trends show that other nations place great value on having a national capability for IC design and manufacture. China in particular is offering massive subsidies to U.S., Taiwanese, Korean, and Japanese producers to create facilities in China. This industrial sector is overwhelmingly dominated by commercial markets, and defense purchases are so small as to be strategically insignificant in financial terms. The committee does not believe the commercial marketplace will permit China to gain a monopoly position in this sector, so the risk of component denial is not large. However, the ubiquity of commercial IC parts throughout DoD systems and their importance to system functionality argue that this situation should be closely watched in case commercial marketplace behavior threatens strategic access.

Capabilities Not Considered Strategic and Critical

There are many capabilities that are properly considered important to U.S. security but that are not as uniquely essential as those in the first two categories above. For these, assured access to needed components can also be an issue and important to the nation's operational capabilities. However, the breadth of the industries involved and the diversity of consequences makes it impractical to focus on all the industries. Component supply for this category needs to be managed to assure that DoD leadership understands the degree of risk and the degree of advantage that are inherent in having foreign suppliers. This category is typified by the broad set of capabilities normally referred to in DoD budgeting as General Purpose Forces. It includes many pieces of equipment used by the tactical forces that are acquired in large numbers to be applied across most prospective military scenarios. At the individual and unit level, they are vulnerable to many battlefield threats and the investments have not been made to make them invulnerable. DoD recognizes that some individuals and units will necessarily be placed at risk to achieve larger strategic gains and that the investment levels needed to avert this risk would jeopardize these truly strategic capabilities. It is against a broader standard for this class of assets that the committee envisions the risks and rewards of foreign sourcing will be assessed.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Risks and Rewards

There are myriad combinations of products, countries, situations, and scenarios that will give rise to concerns about foreign dependence: Middle Eastern oil, microchips and displays from Japan, PCBs from China, specialty metals from Africa, and many, many more. The concerns exist today and will continue through next week, next month, next year, and the next decade. The impact of any one combination will depend on many parameters, including the geopolitical situation of the moment, the nature of the capabilities at risk, the risks our leaders are prepared to take, and the preparations made in anticipation of denial, to name a few.

Officials at all levels can—and do—make calculated and subjective assessments of these potential events and decisions that cover both short- and long-term issues. The President can decide to reduce dependence on oil from the Middle East, DoD can decide that the risk of depending on foreign sources for flat-panel displays is worth the price and performance, and the Air Force might determine that the risk of foreign dependence in the Joint Strike Fighter Program is worth the advantage of foreign participation, to list a few examples.

The committee recognizes that there are risks at many levels of consequence in depending on foreign sources for components, supplies, and services. Some might pose risk to a platform and others, to a unit or a major force. Some might risk our survival as a country if left unattended. However, the committee cannot make any static assessment for this range of potential variables. China looms in the mind of many to be a possible source of mischief, and perhaps it will be, but our nation's leaders have much time and many options to exercise before that mischief becomes anything more than a possibility.

The committee recognizes that there is no set of procedures that can guarantee that U.S. forces will not suffer from the lack of availability of needed supplies and components either now or in the future. Even the most stringent control regimes with completely domestic suppliers have led to tragic losses of life to enemy forces. There are many supply issues that could permit a coalition of unfriendly nations to cause strategic problems for the United States. Oil is such an issue. It exemplifies the decision issues of cost, mitigation, risk, and the involvement of both domestic and international politics. What can be achieved is a high level of informed judgment about risks and rewards in the full context of the mission of DoD and its subordinate organizations.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

The committee believes that the way to address this broad set of concerns is to ensure that vigilance in the face of the potential risks surrounding foreign dependence is integrated into the regular management processes of the DoD.

A MANAGEMENT STRATEGY

In this section, the committee describes a set of actions for USD(AT&L), DIA, and others in the DoD that it believes will provide a credible basis for managing vulnerability and assessing risks, including the risks of foreign dependence. Some of the issues that guide the management approach include the following:

- The likelihood, impact, and mitigation consequences of supply disruption should be dealt with together at the point in DoD that is responsible for these judgments.
- Detailed data about foreign content are constantly changing.
- The best place to collect real and accurate data on foreign content is at the point of procurement—perhaps the acquisition manager or the logistics manager.
- The most authoritative judgments about the operational impact of vulnerabilities would come from the operational elements of the services, the defense agencies, and the combatant commands.

The committee concludes that the right management approach is to depend on the data and judgment of DoD acquisition and logistics officials as the first point of assessment of risk versus reward. Each of these officials has a supervisory chain that can provide guidance for coupling the program manager's judgment to priorities beyond his purview. This same supervisory chain will have the opportunity to review the judgments at the program level and provide increased assurance that a broader perspective is being applied.

Finally, these data and judgments should be shared with the combatant commanders to permit them to assess the operational consequences of the vulnerabilities identified for their mission responsibilities.

The committee does not believe this process should be a significant new burden for the program manager and logistics/procurement levels. They should, as a matter of course, know the sources of supply for their function and should routinely identify risks to their product sourcing deci-

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

THE COMMITTEE CONcludes that the right management approach is to depend on the data and judgment of DoD acquisition and logistics officials as the first point of assessment of risk versus reward.

sions. They regularly make trade-off analyses of mitigation opportunities and consequences. Foreign components are but one of the sources of assurance concern. It is the committee's judgment that obliging them to provide a regular product and supply chain assurance report that covers all significant sources of risk, impact assessment, and mitigation consequences could well be considered a reasonable part of their normal duties.

Testimony from government witnesses and committee member experience suggest that adequate data on foreign content are not currently available to either the government or its prime contractors. The information is not systematically required in the contractual arrangements. However, with an organized effort, the committee believes that a relatively efficient data collection effort can be added to the existing contractual vehicles. In any case, the committee cannot envision any other means to get the data needed for this or any other management approach. If foreign content is to be an important issue for the country, it must be made important at these points in the DoD process.

This method of collecting data and judgments about the data runs the risk of being turned into a pro forma exercise that generates paper but does not contribute to an improved perspective. This fear is amplified by the fact that the process to work this particular set of issues is to be added to the process currently used to work essentially all of the programmatic issues of DoD, and it does indeed produce a lot of paper. However, it is the process by which problems thought to be important—such as performance, cost, and schedule—are dealt with. If foreign dependence is to be an important issue for DoD, it should be dealt with by the same process used for other problems thought to be important. If foreign dependence is not thought to

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

be important, this suggestion will not help much nor will any other management approach.

There is an important role for the executing industrial contractor in this process. Most of the necessary data will actually be produced by the contractor. Some of the risk versus reward analyses will also be made by the contractor. Some of this process is always taking place now, but to bring about a more comprehensive understanding of supply chain risks, more focus will be needed.

This process for managing vulnerability still does not provide for the creation of an aggregated, DoD-wide perspective. For this purpose, the committee believes the data and judgments developed by the process should be provided to a staff element at DoD for the analysis of aggregated trends and national-level implications. DIA TWD should be an integral part of this analytic process to enable the integration of information about supply chain vulnerabilities with intelligence about foreign sources or foreign intrusion into U.S. sources. The analysis should be concerned with particular areas:

- Where there is a lack of accessible war reserves or stockpiles.
- Where a weapon system is uniquely in the U.S. inventory and therefore cannot tap into worldwide depots.
- Where developing an alternative source of supply requires significant lead times.
- Where the DoD has developed sole-source, single-solution capabilities.
- Where critical technologies have migrated offshore or been developed there in their entirety.

Furthermore, the committee believes that the set of major strategic and critical U.S. industrial capabilities identified earlier justify the investment of large DIA TWD resources to monitor for and analyze major changes in global capabilities. These capabilities include network creation and management and information management; the integration of IT components; and systems integration. Subsequently, these capabilities must be matched to the needs of particular military organizations. There are four areas of future technological and industrial advancement that also warrant close monitoring by DIA TWD: IT components, IT services, nanotechnology, and biotechnology. Of particular interest should be any developments at

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

the interfaces of these four technologies. Finally, the DIA TWD should focus its management resources on tracking global capabilities in nuclear weapons; missile defense systems; space systems and space control; submarine construction; aircraft stealth and counterstealth; underwater detection/classification/targeting and underwater stealth and counterstealth; and electronic intelligence acquisition and analysis.

RECOMMENDATIONS

The committee's recommendations reflect several of the themes put forward in the body of the report. The impact of component denial is not a static estimate. The risks entailed in depending on a foreign-produced component are embedded in the strategy of supply management and the diversity of the impacted operational system or force. The size and power of the globalized commercial marketplace are such that we must find a way to exploit the marketplace's value for our security. The risks and benefits of this exploitation are at least as much an issue of acquisition and logistics strategy as they are of estimating foreign intent. The viability of the future assured domestic supply of critical components for the DoD is dependent on the health of the U.S. industrial base in these sectors.

The committee believes that any systemic approach to determining the vulnerabilities and risks of foreign supply for DoD must involve the DoD organizations responsible for acquisition and logistics as well as DIA's responsibility for estimating the capabilities and intentions of foreign countries. Therefore, the committee's recommendations are directed at USD(AT&L) as well as DIA.

These recommendations might be considered as going beyond both the original statement of task and the stated portfolio of responsibilities of the sponsor (DIA TWD). However, the committee believes the subject warrants the integration of the technology warning function into a broader context of supply chain risks and assurance. Without this broader context, warning cannot be properly evaluated.

While this issue of warning is partly an intelligence function, it must also comprehend technical details at the system level and at the level of lower tier suppliers to the systems as well as the operational significance of the risks of supply availability.

Recommendation 1. USD(AT&L), in collaboration with DIA, should de-

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

velop a system for monitoring the risks of component unavailability within the procurement and operating elements of DoD. The committee does not believe it is practical to create a detailed database for this purpose. Rather, the responsible procurement and operational authorities in the armed services, the defense agencies, and the combatant commands should regularly assess their vulnerabilities and the sources of these vulnerabilities and recommend mitigation action.

- A self-certification approach by USD(AT&L) should direct the services and defense agencies to annually prepare a product and supply chain assurance report that identifies important vulnerabilities, potentially significant operational consequences, and recommended mitigation actions. This will require supporting assessments by subordinate organizations for each service and agency. This body of data, assessments, and recommendations will form the primary source of authoritative information from which DoD-wide judgments can be made regarding supply chain vulnerability and impact. It will also be an important framework for the TWD in executing its technology warning responsibilities. The committee believes that the current set of DoD directives and guidance documents available to the program managers and their respective supervisory chains are an adequate tool for establishing the priorities for each DoD procurement activity. These data and judgments should be shared with the combatant commanders to permit them to assess the operational consequences of these vulnerabilities for their missions.
- USD(AT&L), in cooperation with DIA, should analyze these annual reports to identify DoD-wide vulnerabilities that might not be detected by the individual services and agencies and to warn of worrisome trends in the integrity of the supply chain, ensuring it is not compromised by foreign supply sources. A small staff element at the OSD level would be adequate and appropriate. DIA TWD should be an integral part of this analytic process to enable the integration of information about supply chain vulnerabilities with intelligence relating to foreign sources and foreign intrusion into U.S. sources. The analyses should be made available to the services, agencies, and commands as they are produced. The analysis should be particularly concerned with the following areas:

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

—Where there is a lack of war reserves or stockpiles.
—Where a weapon system is uniquely in the U.S. inventory and therefore cannot tap into worldwide depots.
—Where developing an alternative source of supply requires significant lead times.
—Where the DoD has developed sole-source, single-solution capabilities.
—Where critical technologies have migrated offshore or been developed there in their entirety.

- Annual updates of the guidance documents should be made available to the program managers and their respective supervisory chains based on the analysis of the program reports from the acquisition, logistics, and operational organizations and other relevant factors.

Recommendation 2. USD(AT&L), in collaboration with DIA, should develop a system for monitoring U.S. industrial health in strategically important global commercial market sectors that are critical to the availability of components for DoD. If trends toward unacceptable risk are identified, USD(AT&L) should formulate actions to mitigate the situation. It appears to the committee that this monitoring responsibility is directly within the charter of the Office of Deputy Under Secretary of Defense (Industrial Policy) and it should be the lead office. The Defense Industrial Base Capabilities Study (DIBCS) series undertaken for the Office of Deputy Under Secretary of Defense (Industrial Policy) has several features that appear to be a good basis for monitoring industrial health.[7]

The committee believes that the set of major strategic and critical U.S. industrial capabilities identified earlier justify the investment of large DIA TWD resources to monitor for and analyze major changes in global capabilities. These capabilities include network creation and management and information management; the integration of IT components; and systems integration. Subsequently, these capabilities must be matched to the needs of particular military organizations. There are four areas of future technological and industrial advancement that also warrant close monitoring by DIA TWD: IT components, IT services, nanotechnology, and biotechnol-

[7]The entire DIBCS series may be viewed online at http://www.acq.osd.mil/ip/ip_products.html. Last accessed on February 13, 2006.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

ogy. Of particular interest should be any developments at the interfaces of these four technologies. Finally, the DIA TWD should focus its management resources on tracking global capabilities in nuclear weapons; missile defense systems; space systems and space control; submarine construction; aircraft stealth and counterstealth; underwater detection/classification/targeting and underwater stealth and counterstealth; and electronic intelligence acquisition and analysis.

Recommendation 3. USD(AT&L), in collaboration with DIA, should organize a systematic method of assessing the health of military systems integration in and for the DoD as well as that of potential coalition partners and adversaries. The committee believes this task will require broad experience and judgment and should be undertaken with the assistance of expert, external advisory bodies.

REFERENCES

Published

Carlson, Gary. 2005. Trusted Foundry: The Path to Advanced SiGe Technology. Compound Semiconductor Integrated Circuit Symposium. Institute of Electrical and Electronics Engineers.

Coram, R. 2002. Boyd: The Fighter Pilot Who Changed the Art of War. Boston, Mass.: Little, Brown, and Company.

DoD (Department of Defense). 2005. Annual Industrial Capabilities Report to Congress. Washington, D.C.: Office of the Secretary of Defense. February. Available online at http://www.acq.osd.mil/ip/docs/annual_ind_cap_rpt_to_congress-2005.pdf. Last accessed on February 14, 2006.

DSB (Defense Science Board). 1987. Defense Semiconductor Dependency. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology.

DSB. 1999. Final Report of the Defense Science Board Task Force on Globalization and Security. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology. Available online at http://www.acq.osd.mil/dsb/reports/globalization.pdf. Last accessed on February 14, 2006.

DSB. 2005. High Performance Microchip Supply. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology. Available online at http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf. Last accessed on February 14, 2006.

Flamm, K.S. 1994. Flat-panel displays: Catalyzing a U.S. industry. Issues in Science and Technology 11(1): 27-32. Available online at http://www.ksg.harvard.edu/sed/docs/k4dev/flamm_ist_1994.pdf. Last accessed on February 14, 2006.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

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

Lorell, Mark A., Julie Lowell, Richard M. Moore, Victoria Greenfield, and Katia Vlachos. 2002. Going Global? U.S. Government Policy and the Defense Aerospace Industry. Santa Monica, Calif.: RAND Project Air Force. Available online at http://www.rand.org/pubs/monograph_reports/2005/MR1537.pdf. Last accessed on February 14, 2006.

NAVSEA (Naval Sea Systems Command). 2002. Full Service Contracting Business Strategy Wargame. June 21.

NDIA (National Defense Industrial Association). 2002. Full Service Contracting: An Industry View. January 15. Available online at http://www.ndia.org/Content/ContentGroups/Divisions1/Logistics/PDFs%/Full_Service_Contracting_Industry_View.pdf.

NRC (National Research Council). 1993. Strategic Technologies for the Army of the Twenty-First Century (STAR 21): Health and Medical Systems. Washington, D.C.: National Academy Press.

NRC. 1995. Maximizing U.S. Interests in Science and Technology Relations with Japan: Report of the Defense Task Force. Washington, D.C.: National Academy Press. Available online at http://www.nap.edu/catalog/9294.html. Last accessed on February 14, 2006.

NRC. 2001. Opportunities in Biotechnology for Future Army Applications. Washington, D.C.: National Academy Press. Available online at http://www.nap.edu/catalog/10142.html. Last accessed on February 14, 2006.

NRC. 2005a. Avoiding Surprise in an Era of Global Technology Advances. Washington, D.C.: The National Academies Press. Available online at http://www.nap.edu/catalog/11286.html. Last accessed on February 14, 2006.

NRC. 2005b. Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future. Washington, D.C.: The National Academies Press. Available online at http://www.nap.edu/catalog/11463.html. Last accessed on February 14, 2006.

NRC. 2005c. Linkages: Manufacturing Trends in Electronics Interconnection Technology. Washington, D.C.: The National Academies Press. Available online at http://www.nap.edu/catalog/11515.html. Last accessed on February 14, 2006.

Spencer, Jack, ed. 2005. The Military Industrial Base in an Age of Globalization: Guiding Principles and Recommendations for Congress. Washington, D.C.: The Heritage Foundation. Available online at http://www.heritage.org/Research/NationalSecurity/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=81559. Last accessed on February 14, 2006.

World Bank. 2005. World Development Indicators. Washington, D.C.: International Bank for Reconstruction and Development/The World Bank. March. Available online at http://devdata.worldbank.org/wdi2005/index2.htm. Last accessed on February 14, 2006.

Unpublished

Jacques S. Gansler, "Critical Technology Accessibility," Presentation to the committee on January 10, 2006.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Appendixes

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Appendix A

Biographical Sketches of Committee Members

Robert J. Hermann, *Chair*, is a senior partner, Global Technology Partners, LLC. He is a former director of the Department of Defense's National Reconnaissance Office and a former senior official at the National Security Agency. Dr. Hermann served as a member of the President's Foreign Intelligence Advisory Board during the Clinton administration (1993-1995).

In 1998, Dr. Hermann retired from United Technologies Corporation (UTC), where he held the position of senior vice president, science and technology. In that role, he was responsible for assuring development of the company's technical resources and the full exploitation of science and technology by the corporation. He was also responsible for the United Technologies Research Center. Dr. Hermann joined the company in 1982 as vice president, systems technology, in the electronics sector and later served in a series of assignments in the defense and space systems groups.

Dr. Hermann concluded his tenure as immediate past chairman of the American National Standards Institute (ANSI) board of directors at the end of 2002 following a 3-year term; he had served as chairman of the ANSI board of directors during 1998 and 2000 and was a member of the ANSI board since 1993. Dr. Hermann continues to serve as a senior partner of Global Technology Partners, LLC, which specializes in investments in technology, defense, aerospace, and related businesses worldwide.

Before joining UTC, he served 20 years with the National Security Agency with assignments in research and development, operations, and NATO. In 1977, he was appointed principal deputy assistant secretary of

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

defense for communications, command, control, and intelligence. In 1979, he was named assistant secretary of the Air Force for research, development, and logistics and in parallel was director of the National Reconnaissance Office. He received B.S., M.S., and Ph.D. degrees in electrical engineering from Iowa State University and has expertise in defense acquisition/source selection and export control and commerce for the intelligence community.

Pierre A. Chao is a senior fellow at the Center for Strategic and International Studies (CSIS). Before joining CSIS, Mr. Chao was a managing director and senior aerospace/defense analyst at Credit Suisse First Boston (CSFB) from 1999 to 2003, where he was responsible for following the U.S. and global aerospace/defense industry. He remains a CSFB senior adviser. Prior to joining CFSB, Mr. Chao was the senior aerospace/defense analyst at Morgan Stanley Dean Witter from 1995 to 1999. He served as the senior industry analyst at Smith Barney during 1994 and as a director at JSA International, a Boston- and Paris-based management consulting firm that focused on the aerospace/defense industry (1986-1988, 1990-1993). Mr. Chao was also a cofounder of JSA Research, an equity research boutique specializing in the aerospace/defense industry. Before signing on with JSA, he worked in the New York and London offices of Prudential-Bache Capital Funding as a mergers and acquisitions banker focusing on aerospace/defense (1988-1990). Mr. Chao garnered numerous awards while working on Wall Street. *Institutional Investor* ranked his team the number one global aerospace/defense group in 2000-2002, and he was on the Institutional Investor All-America Research Team every year eligible from 1996 to 2002. He was ranked the number one aerospace/defense analyst by corporations in the 1998-2000 Reuters polls, the number one aerospace/defense analyst in the 1995-1999 Greenwich Associates polls, and appeared on the Wall Street Journal All-Star list in 4 of 7 eligible years. In 2000, Mr. Chao was appointed to the Presidential Commission on Offsets in International Trade. He is also a guest lecturer at the National Defense University and the Defense Acquisition University. Mr. Chao has been sought out as an expert analyst of the defense and aerospace industry by the Senate Armed Services Committee, the House Science Committee, the Office of the Secretary of Defense, DoD's Defense Science Board, the Army Science Board, NASA, DGA (France), NATO, and the Aerospace Industries Association board of governors. Mr. Chao earned dual bachelor of science degrees in political science and management science from MIT. His expertise is in

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

defense acquisition/source selection, defense economics, export control/commerce, global supply, defense industrial issues, global defense industry, and finance/economics.

Anthony J. DeMaria is chief scientist at Coherent-DEOS LLC and professor in residence at the University of Connecticut School of Engineering. He was chairman/CEO and founder of DeMaria ElectroOptics Systems, Inc. (1994-2001). He held several positions at the United Technology Research Center before he retired as assistant director of research for electronics and photonics technology. Dr. DeMaria's research expertise is in the area of utilization of laser devices; the interaction of elastic waves with coherent light radiation; the generation, measurement, and application of picosecond light pulses; gas laser research and applications; acoustic-optics; laser physics and devices; and optics. Dr. DeMaria has been an adjunct professor at Rensselaer Polytechnic Institute, a consultant to government and industry, editor of the *Journal of Quantum Electronics*, and a member of government and industry advisory boards. He was the Distinguished Fairchild Scholar at the California Institute of Technology. Dr. DeMaria is a member of both the National Academy of Sciences and the National Academy of Engineering and was president of the Connecticut Academy of Science and Engineering (1997-2003). He was a research professor in the Electrical Engineering Department of the University of Connecticut (1994-1998). Dr. DeMaria's expertise is in export controls and commerce, industrial engineering, and lasers/optics/photonics.

Edsel D. Dunford had a 35-year career in the aerospace industry at Boeing, Ford Aerospace, and TRW. He retired as president of TRW Inc. with responsibility for its aerospace, automotive, and credit reporting businesses. He participated in the design and development of space systems, from early planetary explorers to the sophisticated communication, surveillance, and intelligence systems of the cold war. Mr. Dunford served on several corporate boards including those of TRW Inc., Cordant Technologies, Howmet International, National Steel Corporation, and Cooper Tire and Rubber. Professional societies include the American Institute of Aeronautics and Astronautics and the National Academy of Engineering. He chaired the NRC Committee on the National Aerospace Initiative in 2003. Mr. Dunford holds a B.S. in electrical engineering from the University of Washington, an M.S. in engineering from UCLA, and attended the Executive Program at Stanford University. He served in the U.S. Army from 1954 to

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

1956. Mr. Dunford has expertise in the intelligence community and in military satellites for intelligence, surveillance, and communications.

Christopher C. Green is currently executive director of the Emergent Technologies Research Division at Detroit Medical Center (DMC), 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 chairman of the Independent Science Panel Office and undersecretary of operations research and is a member of the Medical Subcommittee, Local Emergency Planning Committee, State of Michigan/Detroit Regional Homeland Defense; the board of the Spinal Injury Recovery Center at DMC/RIM; and the SOM MRI planning and review board.

Before his current position, he was at the same time executive director for global emerging technology policy in General Motors' (GM's) Public Policy Center and chief technology officer and executive director of Regional Science and Technology for GM's Asia-Pacific operations. He managed formulation of corporate policy directives in newly emergent issues of driver distraction and global privacy. He championed Asia-Pacific regional operations for health and safety and industrial medicine and numerous occupational medical research programs.

He began a distinguished career with the CIA in 1978 as a senior division analyst in the Office of Scientific and Weapons Intelligence. In this role he had multidisciplinary research and management experience in medicine, comparative biology, bioengineering, animal and human physiology, endocrinology, and the 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 senior analyst. His specialty is forensic medicine and toxicology, and his doctoral research work in neurophysiology concerned the biochemical functioning of the human brain.

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 a bachelor's degree from Northwestern University, a Ph.D. in neurophysiology from the University of Colorado Medical School, and an M.D. from the Autonomous City University in El Paso, Texas/Monterey, Mexico. Dr. Green's relevant expertise is in global supply, the intelligence community, and biotechnology.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Joseph Grosson is executive director for Lockheed Martin Focused Logistics and corporate director of logistics at the Lockheed Martin Corporation. Prior to joining Lockheed Martin, Mr. Grosson served as vice president of the Engineering Systems Group for DynCorp, providing engineering and logistics support services for all DoD components, including supply chain management advanced solutions. In addition, he was the past president of PRC Engineering Systems, vice president for program development for Advanced Technology, Inc., and vice president for program management and business development at VSE Corporation. He was a naval reserve officer for 13 years, which included being involved in the following programs: Military Sea Transportation Service, Office of Naval Material, and Weapons Training Units. Mr. Grosson served in many capacities in the government sector, including as a civilian employee of the Department of the Navy and a member of the Senior Executive Service. Additionally, he was a recipient of the Navy Superior Civilian Service Award. He has administered the research and development program for the nuclear power element of the Navy's Exploratory Development Program, as well as other technology related to conventional shipboard power plant design. Mr. Grosson received his bachelor's degree in marine engineering from the State University of New York Maritime College and a master's degree in mechanical engineering from Catholic University of America. His relevant expertise is in defense acquisition/source selection, global supply, logistics, total sustainment solutions (design to disposal), autonomic logistics systems (onboard diagnostics, prognostics, IT infrastructure, supply chain management, and sense and respond technologies), semantic web and logistic ontologies, design for sustainment, and critical service/infrastructure.

Alfonso Velosa III is research director for semiconductors at Gartner, Inc. In this position, he manages research on semiconductor unit forecasts and trends, with a particular focus on global manufacturing and semiconductor consumption trends. Previously at Gartner, he was a management consultant leading a variety of custom market strategy projects in the semiconductor, manufacturing, and software arenas. His experience covers a broad range of topics in the technology marketplace, including strategic planning, project and program management, supply chain management, contract negotiations, financial analysis, and product management support. Prior to joining Gartner, Mr. Velosa managed Intel's motherboard and server supply chain for application-specific integrated circuits, from con-

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

cept through production. In addition, he managed the supply chain and negotiated overall relationships and terms with suppliers. He also provided project and program management services to NASA in Washington, D.C., and in Cleveland, culminating in the management of a semiconductor diffusion project that flew on the space shuttle in 1997. He holds a B.S. in materials science engineering from Columbia University, an M.S. in materials science engineering from Rensselaer Polytechnic Institute, and a master's degree in international management from Thunderbird. He is a member of the NRC Board on Manufacturing and Engineering Design. Mr. Velosa's expertise is in critical technology infrastructure, global supply, logistics, the semiconductor industry and the semiconductor value chain, electronic manufacturing services, and supply chain management.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Appendix B

Presentations to the Committee

MEETING 1, WASHINGTON, D.C., DECEMBER 5-6, 2005

Critical Technology Accessibility: A Sponsor's Perspective
Steve Thompson, Chief, Technology Warning Division
Defense Intelligence Agency

Defense Critical Technologies and Foreign Dependence
Paul Halpern, Coordinator, Committee on Foreign Investment in the United States
Office of the Deputy Under Secretary of Defense (Industrial Policy)

Identifying Critical Technologies
Gordie Boezer, Deputy Director, Military Critical Technologies List
Institute for Defense Analyses

China's Process of Reverse Engineering Technologies
Michael R. Danis, Senior Intelligence Officer
Defense Intelligence Agency

Technology Protection: Theory and Application
Chris Carlson, Research Technology Protection Coordinator
Defense Intelligence Agency

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

DoD Vacuum Electronics Technology
Charles Byvik, Associate Director for Electronics, Space, and Sensor Technologies
Office of the Deputy Under Secretary for Defense (Science and Technology)

Extent and Implications of U.S. Dependency on Foreign Manufacturing of Semiconductors/IT Systems
Mark Thompson

MEETING 2, WASHINGTON, D.C., DECEMBER 19-20, 2005

Globalization, Technology Diffusion, and U.S. National Security
Pierre Chao, Senior Fellow
Center for Strategic and International Studies

Foreign Ownership, Control Mitigation
Christopher Griner, Partner
Kaye Scholer, LLP

Semiconductors: Why the Industry Matters and What Others Are Doing to Acquire It
Chuck Wessner, Associate Director
Board on Science, Technology, and Economic Policy
National Research Council

Thomas Howell, Partner
Dewey Ballantine LLP

Globalization, Risk, and Technological Leadership
James A. Lewis, Senior Fellow and Director, Technology and Public Policy
Center for Strategic and International Studies

Discussion with EIA
Dave McCurdy, President
Electronics Industry Association

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Manufacturing Trends in Printed Circuit Technology
David Berteau, Chair
Committee on Manufacturing Trends in Printed Circuit Technology
National Research Council

MEETING 3, WASHINGTON, D.C., JANUARY 9-10, 2006

EADS North America Presentation
Lt Gen Charles Coolidge, U.S. Air Force (retired), Vice President, Air Force Programs
European Aeronautic Defence and Space Company North America

Joint Strike Fighter Program Brief
Jon Schreiber, Director
Joint Strike Fighter International Directorate

BIOSHIELD Case Study
Michael G. Kurilla, Director, Office of BioDefense Research Affairs
Associate Director for BioDefense Product Development
National Institute of Allergy and Infectious Diseases
National Institutes of Health

Foreign Supplier Assessment Center Discussion
Thomas G. Xenakis, Program Manager
Foreign Supplier Assessment Center

Discussion with Jacques Gansler
Jacques Gansler, Vice President for Research, Roger C. Lipitz Chair
University of Maryland

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Appendix C

Previous Reports on Globalization and the U.S. Military Industrial Base

Allen, Gail C. 2001. Defense Industrial Base at a Crossroads. Alabama: Maxwell Air Force Base. April. Available online at http://research.airuniv.edu/papers/ay2001/affellows/allen.pdf. Last accessed on February 14, 2006.

Borich, Robert Allan, Jr. 2001. Globalization of the U.S. Defense Industrial Base: Developing Procurement Sources Abroad Through Exporting Advanced Military Technology. Washington, D.C.: The George Washington University Law School.

Chao, Pierre A. 2005. The Future of the U.S. Defense Industrial Base: National Security Implications of a Globalized World. Paper presented at the Eisenhower National Security Series and National Defense University Foundation symposium hosted by the Industrial College of the Armed Forces. June 2. Available online at http://www.diig-csis.org/file.asp?F=1F149BF5DA56403E80AD9CB9B475B55F%2Edoc&N=EisenICAF%2Edoc&C=resources. Last accessed on February 14, 2006.

Defense Science Board. 2000. Task Force on DoD Supercomputing Needs. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology. October 11. Available online at http://www.acq.osd.mil/dsb/reports/dodsupercomp.pdf. Last accessed on February 14, 2006.

Defense Science Board. 2000. Defense Software. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology. November. Available online at http://www.acq.osd.mil/dsb/reports/defensesoftware.pdf. Last accessed on February 14, 2006.

Defense Science Board. 2006. Defense Critical Technologies. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology. March. Available online at http://www.acq.osd.mil/dsb/reports/2006-03-Defense_Critical_Technologies.pdf. Last accessed on March 20, 2006.

Defense Security Service. 2006. Technology Collection Trends in the U.S. Defense Industry-2005. Washington, D.C.: Defense Security Service.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Defense Technology Information Center. 2006. Militarily Critical Technologies List. Washington, D.C. Available online at http://www.dtic.mil/mctl/MCTL.html. Last accessed on March 20, 2006.

Department of Defense. 2003. JSF International Industrial Participation: A Study of Country Approaches and Financial Impacts on Foreign Suppliers. Washington, D.C.: Office of the Deputy Under Secretary of Defense (Industrial Policy). June. Available online at http://www.acq.osd.mil/ip/docs/jsf_international_industrial_participation_study.pdf. Last accessed on March 21, 2006.

Department of Defense. 2004. Study on Impact of Foreign Sourcing of Systems. Washington, D.C.: Office of the Deputy Under Secretary of Defense for Industrial Policy. January. Available online at http://www.acq.osd.mil/ip/docs/study_impact_foreign_sourcing_of_systems.pdf. Last accessed on February 14, 2006.

Department of Defense. 2004. Foreign Sources of Supply: Assessment of the United States Defense Industrial Base: Report Required by Section 812 of the National Defense Authorization Act for Fiscal Year 2004 (Public Law 108-136). Washington, D.C.: Office of the Secretary of Defense. November. Available online at http://www.acq.osd.mil/ip/docs/812_report.pdf. Last accessed on February 14, 2006.

Department of Defense. 2005. Foreign Sources of Supply: Assessment of the United States Defense Industrial Base (Addendum: Incorporating Fiscal Year 2004 Contract Information). Washington, D.C.: Office of the Secretary of Defense. March. Available online at http://www.acq.osd.mil/ip/docs/812%20_report_fy04_addendum.pdf. Last accessed on February 14, 2006.

Department of Defense. 2005. Response to Questions of the U.S.-China Economic and Security Review Commission. Washington, D.C.: Office of the Deputy Under Secretary of Defense for Industrial Policy. August 22. Available online at http://www.acq.osd.mil/ip/docs/china_economic_and_security_review_commission_8-22-05.pdf. Last accessed on February 14, 2006.

Dombrowski, Peter J., Eugene Gholz, and Andrew L. Ross. 2002. Military Transformation and the Defense Industry After Next: The Defense Industrial Implications of Network-Centric Warfare. Newport, R.I.: Naval War College. Available online at http://www.nwc.navy.mil/press/npapers/np18/np18.pdf. Last accessed on February 14, 2006.

Hamm, Robert E., Jr. 2001. U.S. Defense Industrial Readiness: Getting It Right in the 21st Century. Carlisle Barracks, Pa.: U.S. Army War College.

Healy, Thomas J., and Jane C. Linder. 2003. Outsourcing in Government: Pathways to Value. New York: Accenture. Available online at http://www.accenture.com/Global/Research_and_Insights/By_Industry/Government/OutsourcingValue.htm. Last accessed on March 21, 2006.

Kugler, Richard L., and Ellen L. Frost, eds. 2001. The Global Century: Globalization and National Security. Washington, D.C.: National Defense University Press. Available online at http://www.ndu.edu/inss/books/Books_2001/Global%20Century%20-%20June%202001/globcencont.html. Last accessed on February 14, 2006.

Lewis, James A. 2005. Effect of U.S.-China Trade on the Defense Industrial Base. Testimony Before the U.S.-China Commission. Washington, D.C.: Center for Strategic and International Studies. June 23. Available online at http://www.csis.org/media/csis/pubs/050623_uschina.pdf. Last accessed on February 14, 2006.

Copyright © National Academy of Sciences. All rights reserved.

Critical Technology Accessibility
http://www.nap.edu/catalog/11658.html

Lieberman, Joseph I. 2003. White Paper: National Security Aspects of the Global Migration of the U.S. Semiconductor Industry. Washington, D.C.: United States Senate. June. Available online at http://lieberman.senate.gov/documents/whitepapers/semiconductor.pdf. Last accessed on February 14, 2006.

Lieberman, Joseph I. 2004. Offshore Outsourcing and America's Competitive Edge: Losing Out in the High Technology R&D and Services Sectors. Washington, D.C.: United States Senate. May 11. Available online at http://lieberman.senate.gov/documents/whitepapers/Offshoring.pdf. Last accessed on February 14, 2006.

McLean, Mark A. 2005. Defense Procurement Strategy for a Globalized Industry. Carlisle Barracks, Pa.: U.S. Army War College. Available online at http://www.strategicstudiesinstitute.army.mil/pdffiles/ksil87.pdf. Last accessed on February 14, 2006.

National Research Council. 2003. Securing the Future: Regional and National Programs to Support the Semiconductor Industry. Washington, D.C.: The National Academies Press. Available online at http://www.nap.edu/catalog/10677.html. Last accessed on February 14, 2006.

National Research Council. 2004. Productivity and Cyclicality in Semiconductors: Trends, Implications, and Questions—Report of a Symposium. Washington, D.C.: The National Academies Press. Available online at http://fermat.nap.edu/catalog/11134.html. Last accessed on February 14, 2006.

National Research Council. 2005. Globalization of Materials R&D: Time for a National Strategy. Washington, D.C.: The National Academies Press. Available online at http://www.nap.edu/catalog/11395.html. Last accessed on February 14, 2006.

Ralph, James R., III. 2004. An Examination of the Defense Industrial Base's Ability to Support the Defense Department at War While Transforming. Carlisle Barracks, Pa.: U.S. Army War College. Available online at http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=A424081&Location=U2&doc=GetTRDoc.pdf. Last accessed on February 14, 2006.

Solis, William M. 2005. DOD's High-Risk Areas: High-Level Commitment and Oversight Needed for DOD Supply Chain Plan to Succeed. Testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate. October 6. Available online at http://www.gao.gov/new.items/d06113t.pdf. Last accessed on February 14, 2006.

U.S. Department of Commerce. 1986-2005. Defense Industrial Capability and Technology Assessments. Multiple documents on this topic are available online at http://www.bis.doc.gov/DefenseIndustrialBasePrograms/OSIES/DefMarketResearchRpts/Default.htm. Last accessed on February 14, 2006.

Copyright © National Academy of Sciences. All rights reserved.