Final Report

of the

Defense Science Board

Task Force on

Globalization and Security

December 1999

Office of the
Under Secretary of Defense for
Acquisition and Technology
Washington, DC 20301-3140

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20000105 005

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is UNCLASSIFIED

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
December 1999

3. REPORT TYPE AND DATES COVERED
Final Technical, 1999

4. TITLE AND SUBTITLE
Report of the Defense Science Board Task Force on Globalization and Security

5. FUNDING NUMBERS
N/A

6. AUTHOR(S)
Dr. Donald A. Hicks

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Science Board
Office of the Under Secretary of Defense (AT&L)
3140 Defense Pentagon, Rm. 3D865
Washington, DC 20301-3140

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Science Board
3140 Defense, Rm. 3D865
Washington, DC 20301-3140

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

11. SUPPLEMENTARY NOTES
N/A

12a. DISTRIBUTION AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

15. NUMBER OF PAGES
163

16. PRICE CODE
N/A

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	N/A	N/A

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

17 DEC 1999

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION, TECHNOLOGY, AND LOGISTICS)

SUBJECT: Report of the Defense Science Board (DSB) Task Force on Globalization and Security

I am pleased to forward the final report of the DSB study on Globalization and Security, chaired by Dr. Donald A. Hicks. The purpose of this Task Force was to consider the preservation of U.S. military dominance in a rapidly changing global environment.

The Task Force recommends that the Department of Defense step forward and boldly meet the challenges of capturing globalization's benefits to sustain U.S. interests into the 21st century. It recognizes that change comes slowly due to a range of cultural impediments, legal and regulatory obstacles, and restrictive and unclear policies. Globalization brings with it opportunity and risk. The Task Force report provides methods for the Department of Defense to be more aggressive in capturing the benefits of or mitigating the risks posed by globalization.

The Task Force recommendations highlight some of the needed changes in the way the Department conducts its business in order to maintain military dominance amidst global technological leveling. Specific recommendations include: fully leveraging the commercial sector capabilities to include commercial business practices as well as commercial products; ensuring the integrity of essential software-intensive systems; adopting personnel security policies to the new global information technologies; and clarifying its position on cross-border defense industry mergers and acquisitions. The Task Force also believes it is important for the Department of Defense to take steps to modernize the regulatory regime affecting both the export of defense products and services and transnational defense industrial integration.

I concur with the Task Force's conclusions and recommend you forward the report to the Secretary of Defense.

Craig I. Fields
Chairman

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301-3140

DEFENSE SCIENCE
BOARD

December 1, 1999

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: DSB Task Force on Globalization and Security

Over the past thirty years I have chaired several and participated in a number of Defense Science Board Task Force studies. The DSB Task Force on Globalization and Security has been unusually challenging because of the sheer number of complex and controversial issues falling within our charter. Taken together, the essence of our task has been to consider the preservation of U.S. military dominance in this rapidly changing global environment.

America's open society presents a challenge when considering the desire to protect information and technology. Despite this openness, and the resulting difficulty associated with controlling our most advanced technology, the United States has been able to maintain military dominance for many decades. The United States has invested the resources necessary to develop a superior infrastructure of both creative people and advanced weapon systems. Together with excellent tactics, training, and maintenance, these resulting defense capabilities are the basis for America's military dominance and have thus been important to protect.

That said, the United States has had mixed success in protecting many of its leading-edge defense capabilities. Over the past forty years, U.S. citizens, cleared at the highest levels, have been discovered giving critical information to foreign countries—both adversaries and allies and friends. Others have been apprehended in violation of the International Traffic in Arms Regulations. And from time to time new discoveries of such activities surface. Moreover, the fact that nations pursue information through espionage should not surprise us. Because of our defense capabilities the United States is an important target. If we are not pursuing a similar course, we are not carrying out an important mission.

The incredible explosion in globalization will make protecting technologies even more difficult. Globalization—in all of its manifestations—has led to a tremendous leveling of access to both information and potential capabilities for our allies and friends as well as potential adversaries. This phenomenon has profound consequences for U.S. military superiority, which this study attempts to address. One characterization of the consequences is the "good enough" weapon system capability in the hands of potential adversaries, such as North Korea's progress in ballistic missiles. The leveling effect of globalization is a thread that runs through the Task Force findings.

The impact of technology leveling is exacerbated by another unfortunate trend that attacks the innovation underlying the "Revolution in Military Affairs." The DoD production budget has been reduced by more than 70 percent over the last decade. Commensurate with this decline is a reduction in defense industry independent research and development (IR&D) funding. Traditionally, defense industry IR&D has funded the development of many of America's most advanced military technologies and innovative integrated defense systems. Industry has historically put about three percent of the DoD procurement budget back into IR&D. However, as budgets have declined, contractors not only have less IR&D funds, but they are diverting a significant percentage of these monies to the pursuit of future line-items in the defense budget. The result is severely depressed U.S. military-technological innovation and a defense industry devoted primarily to the development of Service-preferred legacy system replacements—not necessarily what the Services need to meet emerging strategic challenges.

Globalization also offers tremendous benefits that, if embraced by DoD, could counter the risks articulated herein. Of course, these benefits are not risk-free. However, the Department can manage them with thoughtful planning. Striking such a risk-reward balance is a fundamental tenet underlying Task Force findings and recommendations. Managing the risks of globalization calls for changing the way the Department does business in a number of areas. Let me highlight some of the areas to be discussed in detail in the report and where findings and recommendations will also be made:

- *The Department needs a new approach to maintaining military dominance.*
- *DoD needs to take full advantage of the commercial sector—not only commercial products and services but also commercial business practices.*
- *The Department must act aggressively to ensure the integrity of critical software-intensive systems.*
- *The Department needs to reaffirm periodically its willingness to consider cross-border defense industry mergers and acquisition and to take steps to modernize the regulatory regime affecting both the export of defense products and services and transnational defense industrial integration.*
- *DoD should adapt its personnel security program to the emerging global information technology environment.*

Overarching many of these recommendations, the Task Force calls for establishing permanent groups to continually monitor critical areas—determining essential military capabilities and strategies for preservation; managing advocacy for leveraging the commercial sector and understanding its risks; and vulnerability analysis for critical information systems. These teams are designed to assist the Department in managing the risks of globalization.

The Task Force was extremely fortunate in the exceptionally experienced individuals of many backgrounds who agreed to serve in this effort. The DoD personnel, individuals from the CIA and NSA, military and staff professionals, and contractor staff all

performed admirably. We were also fortunate in having key senior managers from the State and Commerce Departments who were with us throughout the study.

Thomas Jefferson said that the boisterous sea of liberty is never without a wave. We must now sail through a major sea-state change requiring very competent hands on the tiller.

Don Hicks

Donald A. Hicks
Chairman

TABLE OF CONTENTS

TERMS OF REFERENCE

TASK FORCE MEMBERS, ADVISORS, AND STAFF

EXECUTIVE SUMMARY i

1. INTRODUCTION 1

2. CHARACTERIZING GLOBALIZATION 5

THE GLOBALIZATION PHENOMENA 5

GLOBALIZATION OF INDUSTRY 5

3. HOW GLOBALIZATION IS AFFECTING DOD 7

GLOBALIZATION'S IMPACT ON DOD'S SUPPORTING INDUSTRIAL BASE 7

Commercialization of the DoD Supplier Base *8*

Globalization of the U.S. Defense Sector Product Market *9*

Globalization of U.S. Defense Sector Ownership *11*

Benefits and Risks of Industrial Base Globalization *13*

GLOBALIZATION'S IMPACT ON THE INTERNATIONAL MILITARY-TECHNOLOGICAL ENVIRONMENT 21

Strategic Implications of Global Technological Leveling *22*

Export Controls: An Imperfect Panacea *26*

4. FINDINGS AND RECOMMENDATIONS 31

MAINTAINING U.S. MILITARY DOMINANCE AMIDST GLOBAL TECHNOLOGICAL LEVELING 31

COMMERCIAL ACQUISITION 38

GLOBALIZATION OF THE U.S. DEFENSE SECTOR 47

PERSONNEL SECURITY 51

ANNEX I **RECOMMENDATION 4.3.3—PROPOSALS FOR MODERNIZING U.S. GOVERNMENT REGULATORY AND ADMINISTRATIVE PROCESSES ASSOCIATED WITH THE EXPORT OF U.S. DEFENSE PRODUCTS AND SERVICES AND WITH THE INTERNATIONAL TRANSFER OF U.S. DEFENSE TECHNOLOGY** 55

ANNEX II **RECOMMENDATION 4.3.4—PROPOSALS FOR MODERNIZING THE ADMINISTRATIVE AND REGULATORY PROCESSES ASSOCIATED WITH FOREIGN DIRECT INVESTMENT (FDI) TO FACILITATE FDI IN THE U.S. DEFENSE SECTOR** 69

ANNEX III **TAKING FULL ADVANTAGE OF THE COMMERCIAL SECTOR TO MEET DOD NEEDS** 75

ANNEX IV	VULNERABILITY OF ESSENTIAL U.S. SYSTEMS INCORPORATING COMMERCIAL SOFTWARE	83
ANNEX V	COMMERCIAL SPACE SERVICES AND THEIR IMPACT ON NATIONAL SECURITY	95
ANNEX VI	MAINTAINING MILITARY DOMINANCE AMIDST GLOBALIZATION THROUGH THE PRESERVATION OF ESSENTIAL MILITARY CAPABILITIES	109
ANNEX VII	GLOBALIZATION AND PERSONNEL SECURITY	119
ANNEX VIII	LIST OF CLEARED U.S. CITIZENS CONVICTED OF ESPIONAGE	125
ANNEX IX	BRIEFINGS RECEIVED BY THE DSB TASK FORCE ON GLOBALIZATION AND SECURITY	127
ANNEX X	LIST OF ACRONYMS	129
ANNEX XI	BIBLIOGRAPHY	133

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-3010

ACQUISITION AND TECHNOLOGY

06 OCT 1998

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference--Defense Science Board Task Force on Globalization and Security

You are requested to form a Defense Science Board (DSB) Task Force Study on Globalization and Security to provide advice to the Deputy Secretary of Defense and the Under Secretary of Defense for Acquisition and Technology regarding the following issues:

The industrial base serving the Department of Defense is undergoing the following transformations:

- supplier companies, particularly for lower tiers, are increasingly located outside the US (includes both US and foreign-owned firms located abroad); and the identification of location is not always easily accomplished, particularly at the component or tool level;

- supplier companies are increasingly owned, in part or in whole, particularly for lower tiers, by foreign entities and individuals (includes firms located both abroad and in the US); and identification of ownership is not always easily accomplished;

- there is increased purchasing, particularly at lower tiers, including components and tools, of commercial-off-the-shelf (COTS) materiel;

- supplier companies increasingly employ and are dependent on open network architectures and the global information infrastructure for the operation of the firm, including design, inventory, shipping, purchasing, and so on;

- technical talent is increasingly trained and employed on a global basis, with a great deal of geographic and job mobility, and with increasing employment of "remote" work from anywhere on earth;

- the subsystems and components that are purchased (e.g., software, microelectronics) have become so complex in the pursuit of higher performance and lower cost that, practically, they cannot be thoroughly tested;

- formerly defense-only technologies (e.g., night vision equipment, communications satellites) are now being developed and sold commercially, and on a global basis, and dual-use technologies/services once dominated by the US (e.g., space launch) are now often cheaper and more widely available outside the US.

Many of these transformations hold the promise of significant benefit for DoD and its suppliers: lower cost; greater performance; shorter system development and fielding cycles; more stable investment; better interaction, both operationally and politically, with our allies; and such. All of these transformations also carry the risk that critical military or dual-use technology and/or knowledge of US military systems will be transferred, or indeed "leaked," to potential adversaries - possibly obviating a degree of our superiority; or even that adversaries may modify our technology (e.g., DoD information systems) through clandestine means to achieve military ends.

We can reduce the risk by resisting globalization and civil-military integration; and energetically applying traditional approaches to security, usually at great cost of both tangible and intangible sorts, thus deflating the benefits. Alternatively, we may adopt a more sensible risk-reward approach in which we seek innovative policies, procedures, and even technologies that will allow us to embrace the industrial globalization, with associated benefits, listed above, while concurrently: increasing the probability that our technology systems will perform as we expect; decreasing the probability that our adversaries will learn about our technology; and increasing our adversaries' uncertainty whether their clandestine activities are successful.

This study will be co-sponsored by the Under Secretary of Defense for Acquisition and Technology and the Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). Dr. Donald A. Hicks will serve as Task Force Chairman; Mr. Andrew P. Gilmour of the Office of the DUSD (International and Commercial Programs) will serve as Executive Secretary; and LTC Donald J. Burnett, USA, will represent the DSB Secretariat.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act", and DoD Directive 5105.4, "The DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will go into any "particular matters" within the meaning of Section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement officer.

Jacques S. Gansler

TASK FORCE MEMBERS, ADVISORS, AND STAFF

CHAIRMAN

The Honorable Dr. Donald A. Hicks, *Chairman, Hicks & Associates, Inc.; former Under Secretary of Defense for Research and Engineering*

MEMBERS

Mr. Denis A. Bovin, *Vice Chairman, Investment Banking and Senior Managing Director, Bear, Stearns & Co., Inc.*

Dr. Joseph V. Braddock, *Founder and Director, The Potomac Foundation; co-founded BDM International, Inc.*

The Honorable Dr. Ashton B. Carter, *Ford Foundation Professor of Science and International Affairs, Harvard; former Assistant Secretary of Defense for International Security Policy*

Professor Charles L. Cooney, *Executive Officer and Professor of Chemical & Biochemical Engineering, Department of Chemical Engineering, MIT*

The Honorable Gilbert Decker, *Executive Vice President, Engineering and Production, Walt Disney Imagineering; former Assistant Secretary of the Army for Research, Development, and Acquisition*

Mr. James H. Dykstra, *President, SISCORP; former Deputy Assistant Secretary of Defense for Legislative Affairs (Senate)*

Mr. Gordon R. England, *Executive Vice President, General Dynamics*

Dr. Vitalij Garber, *Director of Interoperability, OUSD(A&T); former Assistant Secretary General, Defense Support, NATO*

Dr. E.G. (Glenn) Gaustad, *Vice President, Engineering and Technology, Raytheon Systems Company*

Dr. Theodore S. Gold, *Director, Joint Advanced Warfighting Programs, Institute for Defense Analyses; former Deputy Assistant to the Secretary of Defense (Chemical Warfare Deterrence and Biological Warfare Defense Programs)*

Mr. Everett D. Greinke, *Vice President, GMD Solutions; former Deputy Under Secretary of Defense for International Programs and Technology*

Dr. Robert Hermann, *former Senior Vice President, Science & Technology, United Technologies Corporation*

Mr. Frank Kendall, *Consultant; former Director, Tactical Warfare Programs, Office of the Under Secretary of Defense (Acquisition and Technology)*

Dr. Don Lebell, PE, *Engineering and Management Consultant; former Manager of Information Systems (Automation, Water and Energy Resources), General Electric*

The Honorable Ronald F. Lehman, II, *Director, Center for Global Security Research, Lawrence Livermore National Laboratory; former Director of the U.S. Arms Control and Disarmament Agency*

Dr. Robert W. Lucky, *Corporate Vice President, Applied Research, Telcordia Technologies*

Dr. Joseph Markowitz, *Consultant; former Director of Technology, DoD/Intelligence Community Information Operations Technical Center*

Mr. Walter E. Morrow, Jr., *Director Emeritus, Lincoln Laboratory, MIT*

The Honorable Dr. William Schneider, Jr., *President, International Planning Services, Inc.; former Under Secretary of State for Security Assistance, Science and Technology*

GEN Lawrence A. Skantze, USAF (Ret.), *Consultant; former Commander, Air Force Systems Command*

Mr. Francis J. Sullivan, *Principal, Frank Sullivan Associates; former Staff Director, U.S. Senate Committee on Appropriations*

The Honorable William H. Taft, IV, Ambassador, *Partner, Fried, Frank, Harris, Shriver & Jacobson; former Deputy Secretary of Defense and U.S. Permanent Representative to NATO*

MAJ GEN Jasper Welch, USAF (Ret.), *Principal, Jasper Welch Associates; former Defense Policy Coordinator, National Security Council*

The Honorable John J. Welch, Jr., *Burdeshaw Associates, Ltd.; former Assistant Secretary of the Air Force for Acquisition*

Dr. Herbert S. Winokur, *Partner, Capricorn Management, G.P.*

Dr. Michael I. Yarymovych, *Chief Scientific Advisor to ANSER and Chairman, NATO Research and Development Organization; former Vice President and Associate Center Director, Systems Development Center, Rockwell International*

GOVERNMENT ADVISORS

Mr. Joseph T. Cashin, *Senior Staff Officer, Defense Security Service*

Mr. Victor F. Ciardello, *Director, Financial and Economic Analysis, OUSD(A&T)*

Mr. John T. Elliff, *Director, Controlled Access Program, Community Management Staff, CIA*

Dr. Paris Genalis, *Deputy Director, Naval Warfare, OUSD(A&T)*

Mr. Don Henry, *Office of the Assistant Secretary of the Army (Research, Development & Acquisition)*

The Honorable John D. Holum, *Acting Under Secretary of State for Arms Control and International Security Affairs*

Mr. J. William Leonard, *Principal Director (Security and Information Operations), OASD(C3I)*

Mr. Robert W. Maggi, *Director, Plans, Policy and Analysis, Bureau of Political-Military Affairs, Department of State*

CAPT Robert D. Maslowsky, USN, *N62,Director, Command and Control Systems Division*

Mr. Thomas J. Murtagh, *Assistant Deputy Under Secretary of Defense (Export Finance), OUSD(A&T)*

The Honorable Eric D. Newsom, *Assistant Secretary of State for Political-Military Affairs*

Mr. Randall K. Quick, *Chief, C3, NSA*

COL Ronald R. Reichelderfer, USA, *Senior Army Planner*

The Honorable William A. Reinsch, *Under Secretary of Commerce for Export Administration*

Mr. Earl Rubright, *Science Advisor, United States Central Command*

Mr. Alfred G. Volkman, *Acting Deputy Under Secretary of Defense, International Programs, OUSD(A&T)*

EXECUTIVE SECRETARY

Mr. Andrew P. Gilmour, *OUSD(A&T/International Programs)*

DSB REPRESENTATIVE

LTC Don Burnett, USA, *DSB Secretariat*

STAFF

Mr. John R. Backschies, *Hicks & Associates, Inc.*

Ms. Marya Bavis, *Strategic Analysis, Inc.*

Ms. Barbara A. Bicksler, *Strategic Analysis, Inc.*

Mr. Brad Smith, *Strategic Analysis, Inc.*

Executive Summary

WHAT IS GLOBALIZATION?

Globalization—the integration of the political, economic and cultural activities of geographically and/or nationally separated peoples—is not a discernible event or challenge, is not new, but it is accelerating. More importantly, globalization is largely irresistible. Thus, globalization is not a policy option, but a fact to which policymakers must adapt.

Globalization has accelerated as a result of many positive factors, the most notable of which include: the collapse of communism and the end of the Cold War; the spread of capitalism and free trade; more rapid and global capital flows and more liberal financial markets; the liberalization of communications; international academic and scientific collaboration; and faster and more efficient forms of transportation. At the core of accelerated global integration—at once its principal cause *and* consequence—is the information revolution, which is knocking down once-formidable barriers of physical distance, blurring national boundaries and creating cross-border communities of all types.

HOW DOES GLOBALIZATION AFFECT DOD?

Globalization affects DoD in two distinct, if overlapping, ways. First, it is altering fundamentally the composition of DoD's supporting industrial base while, in turn, necessitating a reengineering of DoD acquisition and business practices. Second, and perhaps more significantly, it is reshaping the military-technological environment in which DoD must compete. These twin trends present DoD with both opportunities for and challenges to the maintenance of global military dominance.

Globalization's Impact on DoD's Supporting Industrial Base

DoD once depended upon, and could afford to sustain, a dedicated domestic industrial base for the development, production and provision of its equipment and services. Today, the "U.S. defense industrial base" no longer exists in its Cold War form. Instead, DoD now is supported by a broader, less defense-intensive industrial base that is becoming increasingly *international* in character. This transformation is due largely to the confluence of four factors: (1) deep cuts in U.S. defense investment in the Cold War's wake (procurement and R&D are down 70 percent and 25 percent in real terms, respectively, since the late-1980s), (2) an explosion in commercial sector high-tech R&D investment and technological advancement, (3) a sustained DoD acquisition reform effort; and 4) a shift in procurement emphasis from weapons and platforms, per se, to the sophisticated information technologies so amplifying their capabilities.

Yesterday's U.S. defense industry is, with few exceptions, reconstituting itself into a global, more commercially-oriented industry. The traditional core of the defense industrial sector—those firms still focusing nearly exclusively on the defense market—comprises firms that will focus increasingly on the integration of commercially-

developed advanced technology to produce military capabilities. That which remains of the traditional U.S. defense sector:

- has undergone an intense period of consolidation;
- has already begun—although mainly in the lower industrial tiers—the process of integration across national borders, via mergers, acquisitions, joint ventures and strategic partnerships with European counterparts, who are themselves in a period of rationalization and consolidation; and
- is now supplied to a significant degree by the commercial sector and is increasingly dependent on commercial business and defense product exports for growth and good health.

The commercial sector, which pays scant attention to national boundaries, is now driving the development of much of the advanced technology integrated into modern information-intensive military systems. This is especially true of the software and consumer microelectronics sectors. Accordingly, future U.S. military-technological advantage will derive less from advanced component and subsystem technology developed by the U.S. defense sector than from the military functionality generated by superior, though not necessarily U.S.-based, defense sector systems integration skills.

The economic and technological imperatives for increased DoD reliance on the commercial sector have also necessitated a reengineering of the Department's acquisition and business practices. Acquisition reform initiatives launched in the early 1990s had evolved by late 1997 into a broader, ongoing Defense Reform Initiative. The most striking aspect of DoD's business practice reengineering is the ongoing, Defense-wide transition to an all-electronic business operating environment. Within just a few years, virtually all DoD business operations, and many critical military functions (e.g., logistics), will be conducted over the Internet and World Wide Web.

Benefits and Risks of Industrial Base Globalization

The potential benefits of globalization are manifold. Increased use of the commercial sector cannot be separated from the effects of globalization. Nor is increased DoD reliance on the commercial sector reversible without sacrificing the huge gains in capability achieved through rapid insertion of leading-edge commercial technology (particularly information-related), and comparable gains in efficiency through use of commercial services. Greater commercial reliance also has the potential to increase the pace of modernization by reducing system acquisition cycle time. The DoD experience of product development cycles for defense systems of 18 years contrasts sharply with much shorter such cycles for most commercial products.

Moreover, commercial acquisition could lower substantially the cost not only of new systems, but also of system upgrades and operational support. Indeed, the impact on DoD capabilities of the post-Cold War decline in defense resources has been manageable only through greater use of commercial products and services. Finally, the Department's adoption of "world-class" commercial business practices—enabled by the full exploitation of Internet-based information technologies—could enhance dramatically

DoD's organizational efficiency and effectiveness. This could allow DoD to cut overhead costs and reinvest the savings in force modernization, and to improve its logistical support to the warfighter.

Cross-border defense industrial integration—and transatlantic links in particular—can help spread the fiscal burden of new system development and production and, from a U.S. perspective, facilitate greater access to our allies' technology and capital. Competition between transatlantic industrial teams—each consisting of both European and U.S. members—could yield innovative, high-quality products, and, for domicile governments, a greater return on defense investments. Such competition would likely stimulate innovation and create the incentive to adopt the industrial and acquisition-related efficiencies that generate downward pressure on system cost and acquisition cycle-time. Transatlantic defense industrial links are a potential source of greater political-military cohesion within NATO and of a stronger alliance industrial underpinning, and thus would help to promote more uniform modernization and thus enhance U.S.-European interoperability.

Such links could also amplify NATO fighting strength by enhancing U.S.-European interoperability and narrowing the U.S.-European technological gap. Perhaps most important, strong transatlantic industrial links could help DoD avert a distinctly negative outcome: the emergence of protectionist "Fortress Europe-Fortress America" defense trade blocs that could serve to widen the U.S.-European military-technological gap and weaken overall NATO integrity.

To be sure, there are risks to DoD in relying more heavily on a fully globalized commercial sector and on a transnational defense industrial base. On balance, however, the Task Force found these risks to be manageable and noted comparable vulnerabilities in DoD's traditional approach to defense procurement—reliance on a captive U.S. defense industry. But while the Task Force deemed the risks manageable, it recommends more aggressive and accountable management of those risks.

The Department's transition to an Internet-based business operating environment—designed in part to enhance civil-military integration—places most of DoD's digital activities and information within the cyber-reach of any and all who want to rapidly gather intelligence on the United States and/or who wish us harm. Such global interconnectivity could provide potential adversaries an open-source intelligence boon. Adversaries scanning DoD websites will likely exploit electronic data mining and aggregation capabilities to piece together rapidly and inexpensively information on U.S. capabilities, operations and personnel that heretofore would have taken much more time, effort and resources to obtain.

Global interconnectivity can also provide adversaries an electronic penetration pathway into U.S. information systems to harm the confidentiality, integrity or availability of essential information and functionality. Such activities are now referred to broadly in national security parlance as information operations. The principal risk associated with commercial acquisition is that DoD's necessary, inevitable and ever-increasing reliance

on commercial software—often developed offshore and/or by software engineers who owe little, if any allegiance to the United States—is likely amplifying DoD vulnerability to information operations against all systems incorporating such software.

Commercial software products—within which malicious code can be hidden—are becoming foundations of DoD's future command and control, weapons, logistics and business operational systems (e.g., contracting and weapon system support). Such malicious code, which would facilitate system intrusion, would be all but impossible to detect through testing, primarily because of software's extreme and ever-increasing complexity. Of equal concern is the ubiquity of exploitable, though inadvertent, vulnerabilities in commercial software. In either case, the trend toward universal networking increases the risk. Inevitably, increased functionality means increased vulnerability.

Compounding matters, the current personnel security system is ill-configured to mitigate the growing information operations risks. The problems lie generally in the over-classification of information (which skews allocation of security resources), and the inherent limitations of the security clearance model (which provides little, if any, monitoring of personnel for five to 10 years after the clearance is granted). The current security model deals principally with the confidentiality of information, neglecting the integrity and availability of information and information systems.

Information technology has also outpaced some of the core concepts upon which the traditional DoD security system is based: the control of physical access, and the distinctions between classified and unclassified information. Security programs have focused on the control of physical access to information and materials, because the spies of the past generally have exploited their physical access to the material they wanted to compromise. However, the practices and tools of physical access control (e.g., access to facilities, controlled areas, or photocopiers) are ineffective against the remote cyber-spy and trusted insider cyber-traitor. The current personnel security system also tends to focus primarily on classified information and activities. It is clear today, however, that the classified world is not the only one with a security requirement. DoD has a number of unclassified systems that are, in every sense, "mission critical" (e.g., wartime blood supply management networks) yet essentially unprotected by the existing security system.

The traditional risk associated with cross-border defense industrial integration is the unauthorized or unintended direct or third-party transfer of "sensitive" U.S. military technology. However, the strong compliance record of foreign-owned, controlled or influenced (FOCI) firms operating in the U.S. under DoD security agreements (e.g., Security Control Agreements, Special Security Agreements, Voting Trusts, or Proxy Board Agreements) indicates that the risks are manageable. Several U.S. government studies, in fact, conclude that our risk mitigation measures have been very successful. Indeed, the evidence shows that regulatory compliance has been of a higher order for domestic subsidiaries of foreign parents than for domestic firms. To be sure, unauthorized technology transfer is a serious problem. Yet, it is a longstanding and, in all

likelihood, enduring one that comes from all azimuths, including U.S. citizens cleared to the highest levels and legitimate exports. So long as the established security mechanisms are in place, the risk of unauthorized disclosure can be mitigated, if imperfectly.

Beyond unauthorized technology transfer, the risks associated with cross-border defense linkages are less clear-cut. To the extent that foreign direct investment in the U.S. defense sector leads to the offshore relocation of domestic development and manufacturing facilities, it could result in the erosion of certain domestic defense industrial skills. There is legitimate concern about potential disruptions in the supply of critical components or subsystems should sole industrial sources for such articles move offshore or come under foreign ownership. And, there is a related concern about potential loss of DoD influence over weapon system design should cross-border consolidation result in a very few large transnational firms selling to dozens of major buying nations (thus reducing DoD's market share). The Task Force examined these potential risks, but found none of them new, nor compelling when cast against the potential benefits of transnational defense industrial integration.

Globalization's Impact on the International Military-Technological Environment

From a long-term strategic standpoint, globalization's most significant manifestation is the irresistible leveling effect it is having on the international military-technological environment in which DoD must compete. Over time, all states—not just the U.S. and its allies—will share access to much of the technology underpinning the modern military.

The international conventional arms market, once driven mainly by political imperatives, is now driven increasingly by economic imperatives. This is perhaps less true of the United States—the Arms Export Control Act requires conventional arms transfers to be consistent with U.S. foreign policy and national security objectives—but the U.S. defense sector is far from immune to the trend. The economic pressure on firms to export, combined with their governments' willingness to let them do so and with the increasing level of cross-border collaboration, will progressively erode the effectiveness of conventional arms and defense technology export controls worldwide. When combined with the black and gray market availability of most types of defense products, and the pressure on already export-minded firms to offer their most sophisticated equipment, these trends suggest that, with few exceptions, advanced conventional weapons will be available to anyone who can afford them.

The technology DoD is most anticipating leveraging to maintain military dominance is that which the United States is *least* capable of denying its potential competitors. Access to commercial technology is virtually universal, and its exploitation for both civil and military ends is largely unconstrained. The most important enabling technologies for information-intensive U.S. concepts of warfare—access to space, surveillance, sensors and signal processing, high fidelity simulation, and telecommunications—are available to the U.S., its allies, and its adversaries alike. Indeed, owing to the proliferation of military technology, the commercialization of former military-specific technology, and the increasing reliance of militaries worldwide on commercially-developed technology, and the general diffusion of technology and know-how, *the majority of militarily useful*

technology is or eventually will be available commercially and/or from non-U.S. defense companies. The so-called "Revolution in Military Affairs" is, at least from a technology availability standpoint, truly a global affair.

Potential competitors are exploiting their newfound access to militarily useful technology in a manner strategically detrimental to DoD. They are not trying to match U.S. strengths or achieve across the board military parity with the United States. Rather, as several recent DSB Summer Studies have pointed out, potential competitors are channeling their more limited defense resources into widely-available capabilities that could allow them to exploit a fundamental weakness of American power projection strategy: the absolute reliance of most U.S. forces on unimpeded, unrestricted access to and use of theater ports, bases, airfields, airspace and coastal waters. By 2010-2020, potential adversaries, exploiting a truly global military-technical revolution, will likely have developed robust capabilities—conventional and unconventional—for disrupting U.S. homeland preparations to deploy to the theater of conflict; denying U.S. forces access to the theater; degrading the capabilities of the forces the U.S. does manage to deploy; and, in the process, raising, perhaps prohibitively, the cost of U.S. intervention. In short, technological leveling—globalization's most strategically unsettling manifestation from a U.S. perspective—is clearly the engine of the emerging "anti-access" threat.

Consequently, there is growing risk inherent in U.S. power projection and force modernization strategy. Left unchecked, this may lead to a decline in the U.S. military's utility for influencing events abroad or protecting U.S. global interests at acceptable cost—a serious erosion of military dominance. At the root of the problem are the inherent limitations—namely, sluggish deployment times and heavy dependence on theater access—of the legacy, primarily short-range, general-purpose force elements to which the vast majority of the Services' modernization funding is currently dedicated. *Viewed in this light, the continued budgetary, strategic and force structuring primacy of legacy systems in DoD budgets has a clear and high opportunity cost: the investment agility necessary to transform U.S. strategy and forces to meet the emerging strategic challenges posed by global military-technological leveling.*

Compounding this problem are the continuing declines in DoD research, development, test and evaluation (RDT&E) and defense industry internal research and development (IR&D) spending, and the related skewing of such R&D investment toward near-term priorities and away from fundamentally new capabilities. The result is severely depressed U.S. military-technological innovation at a time when the premium on innovation has never been higher.

Theoretically, the U.S. could mitigate the undesirable effects of global military-technological leveling by coordinating with its allies the multilateral control of conventional military and dual-use technology exports. This approach worked reasonably well during the Cold War through the Coordinating Committee on Export Controls (CoCom). However, multilateral controls today are no longer a significant factor affecting access to highly sophisticated dual-use technology and they have been only marginally more successful in the conventional weapons arena. CoCom's success

derived from its members facing a common threat—the Warsaw Pact and, to a lesser extent, China—and sharing a common objective: retarding Warsaw Pact and Chinese technological advancement. CoCom also benefited from the disproportionate leverage the United States, its leading advocate, held over the other members as the guarantor of Western security. The Cold War's end undermined this cooperative impetus, and the U.S. can no longer count on its allies, its closest competitors in the high-tech sector, to follow America's lead. The lukewarm success of CoCom's successor, the Wassenaar Arrangement, is a testament to the declining utility of multilateral technology controls in the post-Cold War era.

The strategic significance of global military-technological leveling cannot be overstated. It presents a direct challenge to perhaps *the* fundamental, if subliminal, assumption underlying the modern—and certainly post-Cold War—concept of U.S. military superiority: that the United States enjoys disproportionately greater access to advanced technology than its potential adversaries. This assumption also underpins the logic holding that technology controls are the *sine qua non* of U.S. military dominance.

The reality is that the United States' capability to effectively deny its competitors access to militarily useful technology will likely decrease substantially over the long-term. Export controls on U.S. technologies, products and services with defense/dual-use applications will continue to play a role in the pursuit of U.S. foreign policy objectives. However, the utility of export controls as a tool for maintaining the United States' global military advantage is diminishing as the number of U.S.-controllable militarily useful technologies shrinks. A failure by U.S. leadership to recognize this fundamental shift—particularly if masked by unwarranted confidence in broad or even country-specific export controls—could foster a false sense of security as potential adversaries arm themselves with available technology functionally equivalent to or better than our own.

Clinging to a failing policy of export controls has undesirable consequences beyond self-delusion. It can limit the special influence the U.S. might otherwise accrue as a global provider and supporter of military equipment and services. This obviously includes useful knowledge of, and access to, competitor military systems that only the supplier would have, and the ability to withhold training, spares, and support. Equally obvious, shutting U.S. companies out of markets served instead by foreign firms will weaken the U.S. commercial advanced technology and defense sectors upon which U.S. economic security and military-technical advantage depend.

KEY TASK FORCE RECOMMENDATIONS

DoD has not been aggressive in capturing the benefits of or mitigating the risks posed by globalization. Change has come slowly due to a range of factors, including cultural impediments, legal and regulatory obstacles, and restrictive and unclear policies. The Department needs to change the way it does business in a number of areas:

The Department needs a new approach to maintaining military dominance

Globalization is irresistibly eroding the military advantage the U.S. has long sought to derive through technology controls. Accordingly, the more the United States depends on

technology controls for maintaining the capability gap between its military forces and those of its competitors, the greater the likelihood that gap will narrow. To hedge against this risk, DoD's strategy for achieving and maintaining military dominance must be rooted firmly in the awareness that technology controls ultimately will not succeed in denying its competitors access to militarily useful technology.

DoD must shift its overall approach to military dominance from "protecting" militarily-relevant technologies—the building blocks of military capability—to "preserving" in the face of globalization those military capabilities essential to meeting national military objectives. Protection would play a role in an overall strategy for preserving essential capabilities, but its primacy would be supplanted by three other strategy elements: direct capability enhancement, institutionalized vulnerability analysis and assessment, and risk mitigation efforts designed to ensure system integrity.

To shift its approach from *technology protection* to essential *capability preservation*, the Task Force recommends that DoD: 1) establish a permanent process for determining a continuously-evolving "short list" of essential military capabilities, and 2) develop strategies for preserving each essential capability. Both the list of essential military capabilities and the strategies for their preservation are needed to inform the development of: U.S. warfighting strategy and the forces to underpin that strategy (by identifying how and with what the U.S. will need to fight to remain dominant), DoD positions on technology and personnel security (by helping to identify those capabilities and/or constituent technologies which DoD should attempt to protect and how vigorously they should be protected); and DoD acquisition risk mitigation measures (by identifying those systems that should be the focus of intense efforts to ensure system integrity).

DoD needs to change substantially its approach to technology security

The United States has a national approach to technology security, one in which the Departments of State and Defense both play essential roles. The Task Force does not challenge the propriety of the Department of State's statutory obligation to evaluate proposed defense technology transfers against U.S. foreign policy objectives. That said, the leveling of the global military-technological playing field also necessitates a substantial shift in *DoD's* approach to technology security, the principal objective of which is to help maintain the U.S. military-technical advantage.

DoD should attempt to protect for the purposes of maintaining military advantage only those capabilities and technologies of which the U.S. is the sole possessor and whose protection is deemed necessary to preserve an essential military capability. Protection of capabilities and technologies readily available on the world market is, at best, unhelpful to the maintenance of military dominance and, at worst, counterproductive (e.g., by undermining the industry upon which U.S. military-technological supremacy depends). Where there is foreign availability of technologies, a decision to transfer need only be made on foreign policy grounds by the Department of State. DoD should no longer review export license applications as part of its role in the arms transfer process when foreign availability has been established. This will allow the DoD licensing review to

concentrate on cases where the availability of technology is exclusive to the United States.

Moreover, military capability is created when widely available and/or defense-unique technologies are *integrated* into a defense system. Accordingly, DoD should give highest priority in its technology security efforts to technology integration capabilities and the resulting military capabilities themselves, and accordingly lower priority to the individual technologies of which they are comprised.

For those items and/or information that DoD can and should protect, the Task Force believes security measures need improvement. The means for such an improvement might come from a redistribution of the current level of security resources/effort, whereby DoD relaxes security in less important areas and tightens up in those most critical. In short, DoD must put up higher walls around a much smaller group of capabilities and technologies.

DoD must realize fully the potential of the commercial sector to meets its needs

To leverage fully the commercial sector, DoD must do more than simply acquire available commercial products and adopt commercial practices. In some cases, DoD must engage commercial industry in an effort to shape the development of new products and services to better meet its needs. In many cases, DoD must adapt its often-bloated system requirements to, and develop new concepts that fit, operationally acceptable commercial solutions. The Task Force makes two primary recommendations designed to help DoD meet this overarching objective.

First, the Secretary of Defense should give commercial acquisition primacy and broader scope by establishing it as the modernization instrument of first resort. DoD should seek to meet its modernization needs, whenever possible, with commercial solutions (including integrated services, systems, subsystems, components and building-block technologies) acquired using commercial acquisition practices. The Secretary should grant waivers to the acquisition of commercial *products and services* only when program managers can demonstrate that either no commercial options exist or that available commercial options cannot meet all critical performance requirements. DoD should employ commercial acquisition *practices* in all cases. The Task Force recognizes that some integrated, military-specific systems (e.g., precision-guided munitions and combat aircraft) are not and will likely never be provided by the commercial sector. Even here, DoD should meet its needs, whenever possible, with commercial components and subsystems. DoD can and should tap the commercial market to support virtually all of its modernization requirements.

Second, the Under Secretary of Defense for Acquisition and Technology should form and routinely employ "Commercial Acquisition Gold Teams" to provide and manage advocacy for expanded DoD leverage of the commercial sector. The Task Force believes that Gold Teams should be employed during the earliest stages of the acquisition process (the concept definition phase), where they will have the best opportunity to reduce both the time and cost of developing and fielding new systems. Gold Teams should be

focused initially on the commercial industry sectors from which the Task Force believes DoD can derive immediate and profound benefit: air and sea transportation; logistics and sustainment; communications and information systems; space-based surveillance; and high-efficiency ground transportation. The organizational character and composition of the Commercial Acquisition Gold Teams are best determined by the USD(A&T). Teams could be either standing or *ad hoc* in character. Personnel could be either in-house (i.e., DoD), drawn from the contractor/FFRDC community, or a mix of the two.

In addition to these two core recommendations, DoD must also: 1) engage proactively in commercial standards management; 2) conduct a comprehensive review of the Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulations Supplement (DFARS) with the intent of asking Congress to eliminate remaining statutory barriers to DoD procurement of commercial products and services and also commercial sector disincentives for doing business with DoD; and 3) field on the World Wide Web interactive "distance-learning" software that would allow commercial firms to quickly familiarize themselves with the FAR/DFARS; rapidly determine which regulations apply to their specific contracts; and comply fully with those regulations.

DoD should take the lead in establishing and maintaining a real-time, interagency database of globally available, militarily relevant technologies and capabilities

Such a database, which would facilitate rapid and authoritative determination of the foreign availability of a particular technology or military capability, would serve two principal functions. First, it would allow those involved in the export licensing and arms transfer decisionmaking process to determine which technologies and capabilities are available abroad and thus no longer U.S.-controllable. Second, it would facilitate enhanced access by U.S. government and industry weapons developers to the global technological marketplace by illuminating potential foreign sources and/or collaborators.

DoD must ensure the integrity of essential software-intensive systems

With DoD's growing reliance on commercial software increasing its vulnerability to information operations, the Department must redouble its efforts to ensure the integrity of essential software-intensive systems. To this end, the Task Force makes two primary recommendations. First, the Secretary of Defense should affirm the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) as responsible for ensuring the pre-operational integrity of essential software-intensive systems. In turn, the ASD(C3I) should develop and promulgate an Essential System Software Assurance Program which:

- identifies a point organization for software acquisition review to promote the purchase of commercial software while monitoring its vulnerabilities;
- identifies unambiguously the point in the acquisition process where a system's operator should assume responsibility for its integrity throughout its operational life;
- updates guidance concerning program managers' software integrity assurance responsibilities and declare such integrity a Key Performance Parameter (KPP);
- considers the "clean room" acquisition of certain essential systems or subsystems (i.e., one-hundred percent DoD-controlled system development and production);

- introduces "red-teaming" and independent vulnerability analysis procedures into the acquisition process for all essential systems;
- develops specifications and guidelines for the certification of software trustworthiness at a set of pre-defined levels;
- sponsors research at DARPA and NIST on trust certification and management in software, software design methodology, proof of software correctness, taxonomy of vulnerability, and smart (if non-exhaustive) testing; and
- considers using public (hacker) testing to test algorithm, code and system resilience.

Second, the Secretary of Defense should reaffirm the responsibility of essential system operators to ensure the integrity of those systems throughout their operational life, and assign to the OASD(C3I) Defense Information Assurance Program (DIAP) office the tasks of monitoring and establishing incentives to ensure operator compliance, and of overseeing the administration of the resources required for this purpose. The OASD(C3I) DIAP office should be upgraded (in terms of personnel, equipment and funding) and assigned the full responsibility of overseeing program office/operator identification, programming and execution of the required resources, and of submitting a consolidated information assurance budget. In turn, the operators should:

- ensure that intrusion and anomaly detection systems are in place, current, and operating at peak efficiency;
- ensure that sufficient excess capacity is available to counter expected denial-of-service attacks, and/or that other measures are taken to improve recovery and reconstitution of essential systems;
- ensure that systems originally intended as independent backups are still independent given changes in technology and threat by using dedicated vulnerability-analysis "red" teams;
- ensure adequate configuration control of essential systems; and
- deny unauthorized access—using physical, technical and personnel security measures.

The Task Force also recommends that DoD: 1) expand its red-teaming and vulnerability-assessment capabilities; 2) ensure a sufficiently staffed, trained, and motivated workforce to acquire and operate essential systems; and 3) enhance security and counter-intelligence programs to deal with the new challenges presented by relying on commercially purchased systems and subsystems of foreign manufacture.

DoD should facilitate transnational defense industrial collaboration and integration

Greater transnational, and particularly transatlantic, defense-industrial integration could potentially yield tremendous benefit to the United States and its allies. The Task Force, however, identified a range of factors working to inhibit foreign industrial interest in greater integration with their U.S. counterparts. These include insufficient clarity in DoD policy on cross-border defense industrial mergers and acquisitions, and an overly burdensome regulatory environment surrounding both foreign direct investment in the U.S. defense sector and the transfer of U.S. defense technology, products and services.

The Task Force makes three principal recommendations to erode these barriers to effective defense sector globalization. First, DoD should publicly reaffirm, on a recurring basis, its willingness to consider a range of cross-border defense industrial linkages that enhance U.S. security, interoperability with potential coalition partners, and competition in defense markets. Special attention should be paid to illuminating—to the extent practicable—DoD's broad criteria for merger and acquisition approval, and DoD's policy rationale (e.g., the national security benefits of cross-border defense consolidation). Second, the Department of Defense should engage the Department of State to jointly modernize the regulatory regime and associated administrative processes affecting the export of U.S. defense articles. Third, DoD should also modernize the administrative and regulatory processes associated with foreign direct investment (FDI) to facilitate FDI in the U.S. defense sector.

The Task Force also recommends that DoD adapt existing bilateral industrial security arrangements to respond to the emergence of multinational foreign defense industrial organizations. The change in the structure of the defense industry raises a question about whether the existing security practices are appropriate to its inevitable globalization.

DoD needs to reform its personnel security system

Personnel security is the foundation upon which all other safeguards must rest. However, the Task Force is convinced that, with far more information than necessary being classified by the Original Classification Authorities, the DoD personnel security program is forced to sweep too broadly and is consequently spread thin. Over-classification also leads to an over-allocation of security resources to the protection of classified information at a time when greater resources must be devoted to developing new types of security measures tailored to the challenges created by global information technology. DoD should make a serious commitment to developing a coordinated analytic framework to serve as the basis for classifying information, and for implementing that framework rigorously.

DoD personnel security also depends too heavily on the security clearance process. The clearance process does provide a vital initial filter, weeding out individuals with criminal records or other conspicuously irresponsible conduct. Beyond that, however, its utility fades precipitously—a fact with which the Department must come to grips. Unrealistic expectations of the clearance process have inadvertently undermined the very alertness, accountability and situational awareness necessary for security in a networked world.

In the dynamic, networked environment created by global information technology, DoD needs to develop an enhanced situational awareness approach to personnel security that considers new vulnerabilities, threats, and response requirements. Emerging information technologies (e.g., near real-time data mining of financial and foreign travel databases) hold the seeds of effective defensive options. Compartmentation is also a valuable security instrument. DoD should place a premium on protecting information that is properly determined to require control in codeword compartments. Also needed is an appropriate security program for government and defense industry personnel who occupy "sensitive but unclassified" information technology positions (e.g., those critical for

protecting information systems from hostile disruption or manipulation via the global information infrastructure). Here, monitoring on-the-job performance may be more important than full field background investigations.

In the information age, no single set of personnel security countermeasures will suffice; DoD must achieve a complementary mix of technical, procedural, human resources management and traditional personnel security measures. To this end, the Task Force recommends that DoD:

- Adapt its personnel security system to the information age by streamlining the security classification and clearance processes; ensuring that classifications are justified to mitigate the problem of over-classification; and moving away from a rigid clearance structure.
- Compartmentalize its most sensitive information and activities by restoring the "need to know" principle for classified data stored on electronic systems (taking advantage of security, privacy and intellectual property rights management developments in the e-commerce sector.)
- Institute a situational awareness approach to personnel security combining technical monitoring and human resources management tailored to positions presenting the greatest risks and vulnerabilities.
- Develop a new situational awareness program for personnel in sensitive (classified and unclassified) information technology positions.
- Work with the Intelligence Community to develop more effective situational awareness measures to address the insider threat at the classified level, making greater use of outside research and independent threat/vulnerability evaluation.

* * * * * * * * * * *

Globalization brings with it opportunity and risk. Boldness is required to meet this challenge and to capture the benefits of globalization while mitigating its risks. Leadership is the key. Success will hinge on DoD's ability to establish clear policy guidance that is understood within the Department and across U.S. Government agencies, in the Congress, in U.S. industry, and by allies and friends abroad.

1. Introduction

The Defense Science Board (DSB) Task Force on Globalization and Security was chartered by the Under Secretary of Defense for Acquisition and Technology (USD(A&T)) to: (1) examine the impact of globalization on DoD, and (2) advise the Department on innovative policies, procedures and/or technologies that may allow DoD to maximize the benefits of trends associated with globalization while concurrently mitigating their attendant risk. These trends, identified in the Task Force terms of reference, include:

- DoD's growing reliance on commercial technology (particularly information technology);
- the ever-increasing complexity of commercial software and microelectronics, which is rendering impractical thorough DoD component- and system-level testing of such products;
- the commercialization and global availability of formerly military-specific technology (e.g., communications satellites, high-performance computers);
- the declining U.S. dominance in dual-use technologies and services (e.g., space launch, chemical and biotechnology), which are now often cheaper and more widely available outside the United States;
- the migration by DoD and its suppliers to open networks resting on the commercially developed and operated global information infrastructure;
- the growing number of foreign-owned and/or located DoD suppliers;
- cross-border defense industrial integration and collaboration; and
- the international availability and global mobility of the advanced technology human talent pool.

The Task Force began monthly deliberations in early October 1998 with briefings from government, industry, military and academic experts on the range of issues associated with the Task Force charter.

In November 1998, the Task Force formed three working groups. The Working Group on Globalization, chaired by Dr. William Schneider, Jr., examined the characteristics of and regulatory environment surrounding the globalization of the U.S. defense sector. The working group focused on how the U.S. Government could adapt its regulatory apparatus to enhance its ability to benefit from globalization while retaining the desired security and foreign policy controls. The Working Group on Commercialization, chaired by Dr. Joseph Braddock, examined the benefits and risks associated with commercial acquisition, focusing on ways in which DoD can maximize the former and mitigate the latter. Finally, the Working Group on Military Superiority, co-chaired by Maj Gen Jasper Welch, USAF (ret.) and Dr. Ted Gold, examined the impact of globalization on DoD's ability to sustain global military advantage, focusing specifically on the changing calculus between technology "protection" and the direct enhancement of U.S. military capabilities.

In addition, the Task Force formed two subgroups. The Information Security subgroup, co-chaired by Dr. Joseph Markowitz and Mr. Robert Lucky, examined the manner in which DoD's reliance on commercial software may be amplifying its vulnerability to

adversary information operations, and identified steps the Department could take to mitigate this growing risk. The Personnel Security Subgroup, co-chaired by Mr. John Elliff and Mr. William Leonard, examined the challenges globalization brings to DoD's personnel security system and how the Department might adapt in order to meet them.

By December 1998, the Task Force had settled on an overarching objective: *the enhancement of U.S. global military dominance in the face of globalization.* The Task Force believes that DoD can achieve a net capability gain over its potential competitors if it vigorously exploits globalization while concurrently taking prudent steps to mitigate the attendant but manageable risk. Conversely, the Task Force believes that an overly cautious approach to dealing with globalization will result in a net erosion of U.S. military dominance, due primarily to relative or asymmetrical capability gains made by potential adversaries more aggressively and intelligently exploiting the global availability of militarily-useful technology, products and services.

The Task Force's focus on U.S. military dominance, as opposed to U.S. national security in general, reflects a decision to concentrate on the DSB's primary role of advising DoD on how best to meet its core responsibility of fielding a military capable of defending at acceptable cost U.S. interests across the spectrum of conflict. That said, *the Task Force recognizes that ensuring the security of the United States and its international partners requires more than simply fielding a dominant military.* In some instances, steps to maximize U.S. military capability may be in tension with other U.S. foreign policy objectives, particularly those achieved by limiting foreign access to U.S. defense technology, products and services. However, given the DSB's primary role of advising DoD on how to best meet its core responsibilities, members felt priority had to be given to refining DoD's understanding of how best to maintain U.S. military dominance in these rapidly-changing times.

The Task Force also shared the view that DoD should pursue the maintenance of military dominance in a coalition context. While U.S. forces must be prepared to fight and win unilaterally, coalition action is preferred (for myriad reasons) and thus likely in most scenarios. Accordingly, DoD needs to lay the foundation for effective coalition operations, suggesting: (1) the enduring importance of well-equipped allies (particularly our European partners) with whom we are militarily interoperable; and (2) the need to forge a strong and enduring transatlantic defense industrial foundation.

The foci of the Task Force findings and recommendations derived from an assessment of the effect of globalization on DoD. First, globalization is altering fundamentally the composition of DoD's supporting industrial base. This is reflected in the rising prominence of the commercial sector, the increasing importance of exports to the health of the U.S. defense sector, and the growing interest in both the U.S. and European defense sectors in transatlantic integration (via mergers and acquisitions, joint ventures, strategic partnerships, teaming agreements and other collaborative arrangements). Whereas DoD once depended primarily on a domestic "defense industrial base" for the development, production and provision of technology, products and services, the Department is becoming more dependent on a global commercial-defense industrial base of which it is but one of millions of customers.

Second, by leveling international access to militarily-useful technology, globalization is reshaping the military-technological environment in which DoD must compete. Over time, all states—not just the United States and its allies—will share access to much of the technology underpinning the modern military. Accordingly, the United States will derive less military advantage from protecting technology and more from a superior ability to translate globally available technology into dominant military capability. Moreover, as the list of controllable technologies shrinks, DoD will need to protect more fiercely U.S.-unique, cutting-edge, defense-specific technologies whose protection is necessary for maintaining and/or preserving essential military capabilities, even if the technological advantage will be of limited duration. These developments have profound implications for DoD technology security and personnel security policies and practices.

The report is organized to provide the reader with an overview of the issues related to globalization in the body of the report; certain issues are treated more fully in the Annexes and readers are directed there for specific elucidation. Chapter 2 characterizes globalization, its root causes and its impact on industry. Chapter 3 describes how globalization is affecting DoD—both its impact on the defense industrial base and on the military-technological environment. Chapter 4 contains the Task Force findings and recommendations grouped within four main issue areas:

- Maintaining U.S. Military Dominance amidst Global Technological Leveling
- Commercial Acquisition
- Globalization of the U.S. Defense Sector
- Personnel Security

Following these chapters are a series of Annexes providing information integral to the Task Force findings and recommendations.

2. Characterizing Globalization

Globalization—the integration of the political, economic and cultural activities of geographically and/or nationally separated peoples—is not a discernible event or challenge, and it is not new. What *is* new is the dramatic acceleration of global integration and the resulting political, economic, and technological change the world has seen over the last decade. Goods and services, materials, capital, technology (know-how *and* equipment), information, customs, people, and energy all flow across national borders, not always freely but most often successfully. Most important, the phenomenon of accelerated global integration is largely irresistible. Thus, globalization is not a policy option, but a fact to which policymakers must adapt.

Agents of Change: The Globalization Phenomena

Globalization has accelerated as a result of many positive factors, the most notable of which include the collapse of communism and the end of the Cold War; the spread of capitalism and free trade; more rapid and global capital flows and more liberal financial markets; the liberalization of communications; international academic and scientific collaboration; and more rapid and efficient forms of transportation. At the core of accelerated global integration—indeed, its principal cause *and* consequence—is the information revolution. Driven by quantum leaps in telecommunications and computing efficiency and effectiveness, the information revolution is knocking down barriers of physical distance, blurring national boundaries and creating cross-border communities of all types.

Globalization of Industry

Globalization has been an environmental characteristic of virtually every capital-intensive commercial industry for about a decade now, and has more recently spread to the service sector. Product markets, supplier bases, and company ownership have all become increasingly "global" in nature. This change has been largely market-driven—a result of the need to market products widely, meet human resource needs, capture economies of scale, and gain access to both capital and cost-effective suppliers and operational locales. The process of globalization differs across sector lines, contributing to the absence of a clear definition for the term "globalization" or a shared understanding of the how the process unfolds.

Often, the process begins in the product market, as industry sectors begin to sell their products globally rather than only or primarily domestically. In other sectors, the process begins when the supplier base, once predominantly domestic, takes on an international composition. In still other sectors, foreign ownership serves to stimulate the globalization of both the consumer and supplier bases by generating the capital necessary for those sectors to develop globally competitive products and services. Apart from a few sensitive sectors where regulation remains an important barrier (e.g., aerospace/defense), the globalization of ownership has followed the shift to more international supplier and consumer markets. Indeed, firms with international supplier, product, and investment bases are responsible for more than half the world's industrial output.

The commercial advanced technology sector in the United States has moved rapidly over the past decade into all three dimensions of globalization (i.e., product market, supplier base and ownership). Products now move relatively freely across national borders. Companies are often multinational in both operation and ownership. Perhaps most significantly, they depend on a worldwide supplier network and labor pool. Consequently, the nationalities of a company's owners and managers, the dominion of its incorporation, the resting-place for its capital, and the location of its development and manufacturing facilities may bear little relationship to one another. This is causing some to revisit the once self-evident definitions of "U.S. company". The traditional definition, structured around the geographical location of a firm's corporate headquarters and the nationality of its board of directors, no longer reflects the processes that actually result in the development and manufacture of U.S. products. Today, a U.S. company may have foreign ownership, foreign management, and foreign manufacturing locations. About all one can be sure of is that it seeks to do business in the U.S. market and to selectively enjoy the protection of the U.S. Government.

3. How Globalization is Affecting DoD

Globalization affects DoD in two distinct, albeit overlapping ways. First, it is altering the composition of DoD's supporting industrial base. In just a few short years, DoD has gone from relying almost exclusively on a captive U.S. defense industry to depending more on the commercial market, both domestic and international. Second, and perhaps more significantly, globalization is reshaping the environment in which DoD must compete. The international military-technological playing field is being leveled by a range of trends, including: an increasingly permissive and sophisticated conventional arms market, the diffusion of advanced dual-use technology, the commercialization of formerly military technology, the increasing reliance of militaries worldwide on commercially-developed technology, and the declining effectiveness of export controls. Thus, all states—not just the United States and its allies—will eventually share access to a majority of the technology underpinning the modern military.

This chapter examines the broader impact of these twin developments, focusing on the extent to which they are presenting DoD with both opportunities for, and challenges to, maintaining military dominance.

GLOBALIZATION'S IMPACT ON DOD'S SUPPORTING INDUSTRIAL BASE

Globalization in the U.S. aerospace/defense sector has been slowed—but by no means blocked—by traditional regulatory barriers:

- a product market where exports are regulated by statute (e.g., the Arms Export Control Act, the Foreign Assistance Act, and the Export Administration Act);
- a supplier base limited—by policy, law and regulation—primarily to domestic firms for technology security and defense industrial mobilization purposes; and
- military specifications to which DoD suppliers have, until recently, had to build their products, thus posing a barrier to entry to the commercial sector doing business with DoD.

These barriers have eroded in recent years in the face of changes in the policy environment, resulting in more rapid globalization than anticipated as recently as five years ago. Indeed, whereas DoD once depended upon, and could afford to sustain, a dedicated domestic industrial base for the development, production and provision of its equipment and services, the "U.S. defense industrial base" no longer exists in its Cold War form. Today, DoD is supported by a broader industrial base that includes both defense-intensive and commercial sectors and which is increasingly *international* in character.

This transformation is due largely to the confluence of four factors: (1) deep cuts in U.S. defense investment since the end of the Cold War (procurement and R&D are down 70 percent and 25 percent in real terms, respectively, since the late-1980s), (2) an explosion in commercial sector high-tech R&D investment and technological advancement, (3) a sustained DoD acquisition reform effort, and (4) a shift in procurement emphasis away

from weapons and platforms to the sophisticated information technologies that are so amplifying their capabilities.

Yesterday's U.S. defense industry is, with few exceptions, reconstituting itself into a global, more commercially-oriented industry. The traditional core of the defense industrial sector—those firms still focusing nearly exclusively on the defense market—comprises firms that will focus increasingly on the integration of commercially-developed advanced technology. That which remains of the traditional U.S. defense sector:

- has undergone an intense period of consolidation;
- has already begun—albeit mainly in the lower tiers—the process of integration across national borders, via mergers, acquisitions, joint ventures and strategic partnerships with European counterparts, who are themselves in a period of rationalization and consolidation; and
- is now supplied to a significant degree by the commercial sector and is increasingly dependent on commercial business and defense product exports for growth and good health.

The commercial sector, which pays scant attention to national boundaries, is now driving the development of much of the advanced technology integrated into modern information-intensive military systems. This is especially true of the software and consumer microelectronics sectors. Accordingly, U.S. military-technological advantage will derive less from advanced component and subsystem technology developed by the U.S. defense sector than from the military functionality generated by superior, though not necessarily U.S.-based, defense sector systems integration skills.

The following sections examine the globalization of the DoD's supporting industrial base from the supplier base, product market and ownership perspectives.

Commercialization of the DoD Supplier Base

The decision to broaden commercially—and thus internationally—DoD's supporting industrial base, made in earnest during the 1990s, was both conscious and necessary. First, information dominance was emerging as the centerpiece of DoD warfighting strategy and modernization planning, and the commercial sector was the source of state-of-the-art information technology. Second, DoD could not afford to continue its dependence upon a defense-unique industrial base that developed systems essentially from scratch. It needed to shed some of the developmental burden and leverage the massive commercial R&D investment in advanced technology. Buying commercial also meant that, because the commercial sector can spread its development costs among huge numbers of units, DoD could also save precious procurement dollars. The net result of DoD's response to these twin imperatives is a dramatic increase in the Department's use of commercial, specifically commercial-off-the-shelf (COTS), components, subsystems, and services.

Software is the commercial sector upon which DoD is currently most dependent. Commercial software is pervasive, whether embedded within integrated weapons systems

as components or subsystems, or purchased directly by the Department as full-up information systems. Several factors contribute to DoD's growing dependence on commercially developed software. Affordability is one. With special-purpose software systems, DoD must pay for R&D and, being the only customer, must accept unit costs inflated by low-volume production. With commercial software, industry pays for R&D, and unit prices are lower as the result of the high-volume production necessary to meet commercial demand. Second, special-purpose systems tend to become "frozen" and maintained at a particular state, whereas commercial market forces and free-market competition often stimulate the upgrade of commercial systems; by using commercial systems, DoD can "ride the wave" of product improvement. Third, commercial systems tend to come with extensive documentation for training and troubleshooting. Training courses also are commonly available to fill a perceived need.

Many of DoD's most critical future systems are based at least partly on commercial software. Next-generation command and control systems, for example, will depend heavily on a "common operating environment" based on commercial operating systems, web browsers, office automation software, and database management systems. Defense communications rely heavily on NIPRNet (**U**nclassified-but-sensitive **I**nternet **P**rotocol **R**outing **NET**work) and SIPRNet (**S**ecret **I**nternet **P**rotocol **R**outing **NET**work), which use Internet protocols and depend on routers and switches whose software is commercially provided. And most telephone switches comprising the public switched network (which carries approximately 95 percent of all DoD communications) are run primarily by commercial software.

At the policy level, DoD has recognized the need to enhance its ability to leverage commercial technology, products and services. Yet, change along these lines has been neither systematic nor revolutionary; the process has affected some facets of U.S. military capabilities while wholly bypassing others.

Globalization of the U.S. Defense Sector Product Market

The U.S. comparative advantage in the global defense export market has grown significantly in the wake of the Cold War. The collapse of the Soviet Union produced a meltdown in both the Russian defense industrial base and its pool of sustaining investment resources. Moreover, the Russian economic decline has precluded continuation of the Soviet practice of extensive product and financial subsidies for its defense exports. Western European nations generally reduced their defense investment significantly after 1991. While U.S. defense investments also declined during the past decade, its defense-related R&D and procurement investments still exceed those of its alliance partners.

Accordingly, while total U.S. defense exports have not increased materially, the U.S. percentage of the international defense market has grown substantially. During the Cold War, the U.S. share of the international defense market was approximately one-third of the total. Although the aggregate defense export market has shrunk by fifty percent in recent years, the U.S. share of the global market has grown to 55-60 percent. This has occurred despite the fact that U.S. defense prime contractors typically export only one-quarter of their annual production (compared to 50-80 percent by many major European

producers). Because of decreased procurement budgets, U.S. prime contractors and many of their suppliers have become increasingly export-minded, with several seeking to achieve 50 percent of their sales through exports over the near term. While this export-centric approach clearly has economic advantages for both DoD and industry, it generates potential conflict with other important foreign policy goals, such as conventional weapons non-proliferation and regional stability. Nevertheless, U.S. Government policy (e.g., President Clinton's *Conventional Arms Transfer Policy*, February 1995) has formally recognized the benefits to U.S. foreign policy objectives from such exports. Additionally, in 1996 the Congress created a $15 billion Defense Export Loan Guarantee Program in DoD to facilitate defense export financing.

Export of U.S. defense articles and services is accomplished through one of two vehicles. One vehicle is the U.S Foreign Military Sales (FMS) system through which the U.S. Government contracts for the purchase of U.S. defense products and services on behalf of allied and friendly governments. The second vehicle is the direct commercial sales process wherein allied and friendly governments contract directly with U.S. companies. The two systems coexist uneasily.

The FMS system has many attributes that are valuable to the customer, to the U.S. vendor, and to the U.S. Government. However, the rigidity of the FMS system procedures makes it very difficult for the U.S. Government to become the conduit of choice when allied and friendly governments seek U.S. defense equipment—particularly when foreign governments elect to make their defense equipment selections by means of an international competition. Unfortunately, this leads to lost opportunities when larger-scale U.S. interests would be best served by direct U.S. Government participation in private sector defense industrial collaborative arrangements. The reality is that the global marketplace is shaped by worldwide defense industry over-capacity. Moreover, the global arms market offers a variety of alternatives to paying customers. Allied and friendly governments may seek non-U.S. sources should they perceive that neither FMS nor direct commercial contract vehicles meet their needs. The ongoing DoD FMS Reinvention initiative—the central thrusts of which include increased responsiveness, flexibility, and U.S. Government-Industry teaming—has the potential to greatly improve the FMS system.

The direct commercial sales approach also has many valuable attributes, one of which is that it links the customer with a U.S. supplier that is generally both flexible and eager to accommodate customer needs. However, the U.S. supplier's actual responsiveness will be driven in part by the U.S. Government export license process. The State Department's Office of Defense Trade Controls (DTC), in accordance with sections 38-40 of the Arms Export Control Act (AECA) (22 U.S.C. 2778-80), and the International Traffic in Arms Regulations (ITAR) (22 C.F.R. Parts 120-130), regulates the direct commercial export of defense articles, data and services on the U.S. Munitions List by taking final action on license applications and other requests for approval for defense trade exports and retransfers. Of the 45,000 Munitions List export license applications submitted in 1998, approximately 70 percent were approved within 30 days by the State Department without DoD review, based on established policy and preference. The roughly 30 percent forwarded by DTC to DoD, however, averaged 81 days total (i.e., State and DoD) review time; currently, reviews involving both DoD and State average roughly 98 days. While

less than two percent of all 1998 export license applications were denied, the majority were approved subject to conditions—which often require extensive research and discussion between DoD, industry and other U.S. government elements to negotiate—that reflect U.S. Government foreign policy and national security concerns.

Globalization of U.S. Defense Sector Ownership

The concept of foreign direct investment in the U.S. defense sector is antithetical to traditional defense industrial base concepts. However, there are powerful economic and financial incentives at work encouraging transatlantic consolidation in a manner parallel to other capital-intensive industrial activities. The slow growth in the European defense market compared to that of the United States, and rigidities in the European labor market and official procurement practices, have made the U.S. defense market an attractive one for foreign investors. United States regulatory practices, ironically designed to assure a secure national defense industrial base, have actually become an impetus for foreign direct investment in the U.S defense sector. The need to produce for the U.S. market *in the United States*, a *de facto* U.S. requirement for a 100 percent direct offset for significant purchases of foreign technology or equipment, has made it necessary for offshore firms to become direct investors. The scale of the U.S. defense market, its need for advanced technology solutions, and the attractive competitive aspects of the U.S. market have also increased the demand for U.S. defense properties by foreign investors.

Foreign investment in the U.S. defense sector as a foreign owned, controlled or influenced (FOCI) firm is possible through one of the U.S. Government-sanctioned forms of regulation. The DoD through the Defense Security Service (DSS) has the primary responsibility for negotiating security arrangements—Security Control Agreements, Special Security Agreements (SSAs), Voting Trusts, or Proxy Board Agreements—with FOCI firms to regulate their access to programs in the defense sector where classified information is involved. By obtaining such a "FOCI agreement," U.S. subsidiaries of foreign parent firms are the legal equivalents of domestically owned firms, and are able, legally if not always practically, to compete on an equal basis with their U.S. counterparts. FOCI agreements are designed to ensure that the foreign parent company cannot access either classified or export-controlled unclassified information, and that the responsibility for implementing enhanced security measures is placed with U.S. citizens responsible for managing the foreign owned subsidiary.

The DSS role in the foreign direct investment approval process is limited to its advisory role in support of the deliberations of the Committee on Foreign Investment in the United States (CFIUS), and its direct role in the award of facility security clearances for foreign-owned companies (including firms with significant foreign investment). The CFIUS conducts assessments for the President as to the degree to which a proposed foreign investment would adversely affect U.S. national security interests. Decisions authorizing foreign participation have largely focused on the compliance record and the compatibility of the laws, regulations, and political relationship with the nation in which the foreign parent company is domiciled, or incorporated.

Where regulation is permissive (e.g., UK private sector direct investment in the U.S. defense electronics sector), substantial investment has already taken place. The

mezzanine, or subcontractor, levels tend to receive scant mention in discussions of defense industry globalization. Nonetheless, the construction of a transatlantic "industrial bridge" is underway and accelerating at this level. According to DoD figures, cross-border (U.S.-Europe and intra-European) merger activity has increased each year since 1992, and the trend is expected to continue. Cross-border transactions have increased in number, in value and as a percentage of all industry mergers and acquisitions each year since 1996. Moreover, European companies are increasingly using mergers and acquisitions to enter the U.S. market.

Country	SSAs
Canada	CAE Electronics
Canada	Cincinnati Electronics
Canada	Denro, Inc.
Canada	Short Brothers, Inc
Canada	Versatron Corporation
Denmark	Maersk Line Limited
France	Zodiac of North America, Inc
Germany	CMS, Inc
Israel	EFW, Inc
Israel	Kollsman, Inc
Multiple	AGG Holding Corporation
Multiple	MLRS International Corporation
Netherlands	Eagle-Picher Technologies, LLC
Netherlands	Lips Propeller, Inc
Spain	Tacisa, Inc
Sweden	Wilson, UTC
Switzerland	Fracht FWO, Inc
Switzerland	Hexcel Pottsville Corporation

Country	Proxies
Austria	Vexcel Corporation
Denmark	ETI Engineering, Inc
Germany	J.A. Jones Services, Inc.
Germany	Lockwood Greene Tech., Inc
Germany	Orlando Technology, Inc
Germany	Sierracin Research Corporation
Israel	Comverse Govt Systems Corp.
Japan	PSG Services, Inc
Sweden	Bird-Johnson Company
Switzerland	Panalpina FMS, Inc

Country	Voting Trusts
Japan	Amdahl Federal Services Corp.
Switzerland	Timeplex Federal Systems, Inc

Note: More than one U.S. company may be owned under a FOCI agreement.

UK SSAs
Allison Engine Company, Inc.
Alloy Surfaces Company, Inc.
Carleton Technologies
Chelton Communications Systems, Inc.
Designers & Planners, Inc.
Endevco Corporation
GEC-Marconi Dynamics, Inc.
General Offshore Specialized Svcs, Inc.
Irvin Aerospace, Inc.
Kidde Technologies, Inc.
Laser-Scan, Inc.
Lear Astronics Corporation
Lucas Western, Inc.
Marconi North America
Maritime Dynamics, Inc.
New Boston Select Group, Inc.
Pilkington Aerospace, Inc.
Reflectone, Inc.
SAGE Laboratories, Inc.
SERCO, Inc.
Smiths Industries Aerospace and Defense Systems, Inc.
Ultra Electronics Defense, Inc.
Western Design Corp.

UK Proxies
Allison Advanced Development Co., Inc.
Canteen Corporation
Courtaulds Defense Products, Inc.
James Martin Government Int'l, Inc.
Racal Communications, Inc.
Solitron Vector Microwave Products, Inc.
Telos Corporation of Maryland
Texstars, Inc.

UK Voting Trusts
GCCUS

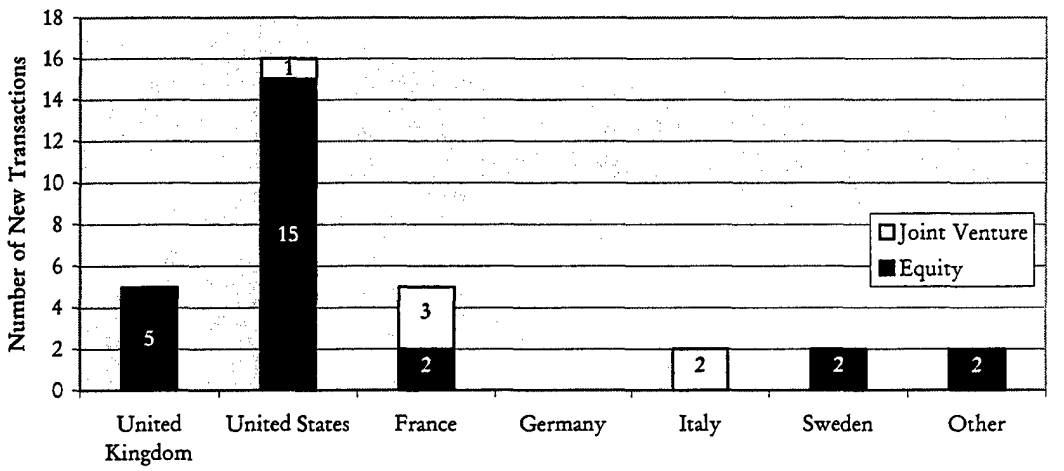
Figure 1:
Foreign Defense/Aerospace Firms under FOCI Agreements with DoD as of July 1999
(Source: DoD)

UK firms are the most active European acquirers, particularly with regard to U.S. firms. This is reflected in the disproportionate amount of U.S. FOCI agreements held by UK firms (32) relative to all other foreign firms combined (31), illustrated in Figure 1 above. Since January 1997, UK defense and aerospace firms have been involved in more than 50

transactions with U.S. firms (23 UK purchases of U.S. firms; 27 U.S. purchases of UK firms) valued at over $13 billion. From January 1998 through March 1999 alone, UK defense/aerospace firms announced or completed 32 cross-border transactions (equity purchases or joint ventures), including 16 with U.S. firms.

The data, captured in Figure 2 below, suggest that UK-Continental European integration may be limited over the near-term to joint ventures, and that UK firms prefer to exchange ownership with U.S. or other UK firms (state-owned firms appear less attractive to UK firms considering equity transactions). The data also suggest that, because of DoD's considerable (and, to date, positive) experience with mezzanine-level U.S.-UK defense industry linkages, the Department might be more willing to approve such a transatlantic arrangement at the "prime" contractor level.

Figure 2:
Transactions by British Defense/Aerospace Firms, January 1998 - March 1999
(Source: DoD)



Benefits and Risks of Industrial Base Globalization

The globalization and commercialization of DoD's supporting industrial base simultaneously pose the prospect of benefits and risks for the Department. On the one hand, a failure by DoD to effectively exploit globalization's benefits could lead to increasing costs, diminished performance, and declining interoperability within the NATO alliance. On the other hand, a failure to engage in effective risk mitigation could also expose DoD to serious risk, particularly with regard to the acquisition of commercially developed information technology.

However, the Task Force believes that the benefits of industrial globalization far outweigh the risks, which, in its view, are decidedly manageable. Thus, a balanced process through which DoD can exploit the benefits of globalization, implemented in parallel with well-designed risk mitigation measures, is indispensable to a successful national security posture in the 21st century.

Benefits of Industrial Base Globalization and the Barriers to their Exploitation

Commercialization of the DoD Supplier Base

Benefits. The commercialization of DoD's supporting industrial base has myriad potential benefits. Increased DoD reliance on the commercial sector can facilitate major capability gains through both the rapid insertion of leading-edge commercial technology (particularly information-related), and the exploitation of and adaptation to robust and advanced commercial services. Greater commercial reliance also has the potential to increase the pace of modernization by reducing system acquisition cycle time. The DoD experience of product development cycles for defense systems of eighteen years contrasts sharply with much shorter development cycles for many commercial products.

Moreover, commercial acquisition could lower substantially the cost not only of new systems, but also of system upgrades and operational support. Indeed, the impact of the post-Cold War decline in defense resources has been manageable only through greater use of commercial products and services. Finally, DoD's adoption of "world-class" commercial business practices—enabled by the full exploitation of Internet-based information technologies—could enhance dramatically organizational efficiency and effectiveness. This could allow DoD to cut overhead costs and reinvest the savings in force modernization, and to improve its logistical support to the warfighter.

Though the Department has tapped the commercial sector to meet many of its software requirements, many other commercial sectors—in which consumer demand has sparked rapid technology and capability advancement—offer untapped potential to meet or even exceed core DoD requirements. The Task Force identified five present-day examples to illustrate this point: air and sea lift, logistics and sustainment, communications and information systems, space-based surveillance, and high-efficiency ground transport. **Annex III, *Taking Full Advantage of the Commercial Sector to Meet DoD's Needs,*** contains a discussion of each.

Barriers. The gradual pace of DoD's shift to commercial acquisition is due largely to cultural barriers. Resistance from the acquisition community to fully engaging the commercial sector, for example, stems from the absence of any conventional wisdom about the degree to which military-unique technologies, capabilities and services can be replaced by commercial solutions. Moreover, while senior DoD leaders have extolled the virtues of commercial acquisition, they have yet to engage fully in the kind of advocacy that may be required to sufficiently push a risk-averse acquisition community.

There are also lingering regulatory obstacles, found most notably within the Federal Acquisition Regulations (FAR) and Defense FAR Supplement (DFARS), which govern the purchase of goods and services by the Department of Defense. The complex and often politically motivated statutes underlying the FAR and DFARS often restrict DoD's ability to purchase some foreign products or products containing certain foreign material. Many of these statutes were be designed to protect the U.S. defense industrial base and U.S. suppliers of certain commodities from foreign competition.

Historically, attempts to remove these restrictions, in part or in total, have been met with limited success. Attempts to increase DoD's waiver authority have received limited political support because of the powerful constituencies represented in the governing statutes. On the positive side, however, most defense trading partners, including most NATO countries and selected others, have reciprocal procurement agreements with the U.S. Government that result in a waiver of the Buy American Act of 1933. The United States has such agreements with 21 countries and is in various stages of negotiations with several others, including some of the new NATO partners. These agreements, however, do not result in waiving product-specific "buy American" statutory provisions because such provisions have exceptionally limited waiver authority.

The Federal Acquisition Streamlining Act of 1994 (Pub. L. 103-355) helped facilitate increased DoD purchases of commercial items by exempting such purchases from numerous laws. Nevertheless, there are still a number of legal impediments to U.S. and non-U.S. commercial firms participating on DoD procurements. Some of the laws implemented in the FAR and DFARS, for example, are extraordinarily complicated. It is thus a tall order for the uninitiated to determine which provisions govern their specific case. Further complicating the procurement system are frequent (almost weekly) changes to the FAR and DFARS. Such changes are typically the result of statutory modifications or the new interpretations of the existing statutes. The sheer volume, complexity and fluidity of the regulations embedded within the FAR and DFARS serve to discourage commercial firms, U.S. and foreign alike, from doing business with DoD.

Product Market Globalization

Benefits. A global product market provides a number of potential benefits to U.S. national security policy. Placing U.S. defense products in the hands of friends and allies enhances opportunities for doctrinal and force interoperability and, in turn, more successful coalition operations. Economies of scale, adversely affected by the post-Cold War contraction in defense procurement, can be improved through the U.S. defense production base's participation in international procurements.

Barriers. The statutory requirements surrounding the export of defense equipment and services are based on effective U.S. Governmental control of the dissemination of U.S. Munitions List equipment and services. The aim of this statutory grant of authority to the President—the achievement of foreign policy objectives—is embedded in such policy documents as the President's *Conventional Arms Transfer Policy*. The International Traffic in Arms Regulations (ITAR) and the State Department's Office of Defense Trade Controls (DTC) constitute the core of the regulatory apparatus derived from statute.

While the statutory basis for the ITAR is relatively flexible, implementation is based largely on the 1970s model of the defense market. The "buyer-seller" structure of the ITAR reflects a bygone era in which the United States dominated the development and production of advanced technology. This has made it difficult for the regulatory process to recognize and take into account the foreign availability of functional equivalents to U.S. Munitions List items, the impact of unclassified/uncontrolled technology on the

performance of military systems, and the potential for cross-border industrial collaboration.

As a result, the regulatory process, as currently configured, hinders the potentially beneficial cross-border flow of U.S. defense sector products, and frustrates collaboration between U.S. defense companies and their counterparts in allied countries. Specifically, there are too many decision points for export license approvals. Export licenses need to be submitted and evaluated in the context of the entirety of the proposed export (considering at one time all the various subsystems and components involved). Moreover, a separate license is required for each different re-sale (third-party sale) destination. Unfortunately, most applications are submitted in a piecemeal fashion, not taking into account likely third-party exports. This results in multiple reviews to refine and define the limitations of the eventual program. These myriad steps limit the extent to which transatlantic technology flows (e.g., via collaborative projects or indeed integration between U.S. defense contractors and their European counterparts) would otherwise advance the military capabilities of the United States' allies and would, in turn, amplify the effectiveness of future military coalitions in which U.S. forces participate.

Transnational Defense Industrial Integration and Collaboration

Benefits. Cross-border defense industrial links can help spread the fiscal burden of new system development and production and, from a U.S. perspective, facilitate greater access to our allies' technology and capital. Competition between transatlantic industrial teams—each comprised of both European and U.S. members—could yield innovative, high-quality products, and, for domicile governments, a greater return on defense investments. Such competition will stimulate innovation and create the incentive to adopt the industrial and acquisition-related efficiencies that generate downward pressure on cost and cycle-time.

Overall, transatlantic industrial links are a potential source of greater political-military cohesion within NATO and a stronger alliance industrial underpinning. Industrial cooperation and integration will expand common interests in modernization goals, practices, and collaboration. Moreover, such links could amplify NATO fighting strength by enhancing U.S.-European interoperability and narrowing the U.S.-European technological gap. Perhaps most important, strong transatlantic industrial links could help avert a distinctly negative outcome: the emergence of protectionist "Fortress Europe-Fortress America" defense trade blocs that could serve to widen the U.S.-European military-technological gap and weaken overall NATO integrity.

Barriers. There exist formidable barriers to transatlantic defense industrial integration. First, and most simply, DoD's policy on major cross-border defense industry mergers and acquisitions is not sufficiently clear. A consistent complaint among both U.S. and European defense industry executives is that they lack a clear sense of what DoD's criteria are for approving a major transatlantic combination, particularly those involving a "prime" U.S. contractor. This undermines industry executives' confidence that a proposed arrangement will ultimately win DoD approval and, in turn, decreases their incentive to invest the time, energy and resources required for two companies to bring a proposed arrangement forward for government review. Wary of the potentially

disastrous fallout of proposing a major cross-border combination only to see it blocked months later, it appears many firms are taking a more cautious wait-and-see approach.

Second, U.S. Government classification, technology transfer, and export control policies are often perceived abroad as too restrictive for effective cross-border operations. Strong incentive for acquiring a U.S. company can be undermined by the limitations on access to a company's most advanced technology (if it is classified), and by limitations on the sale outside of the United States of products containing export-controlled technology. Similarly, restrictions on non-U.S. employee access to classified information are perceived by some European industry executives as a serious impediment to optimal workforce utilization and day-to-day business operations. Many foreign-owned subsidiaries find certain restrictions on FOCI entities a limitation on the ability of their U.S. managers to participate fully in the U.S. defense market. Even routine interaction between foreign and U.S. employees of FOCI firms are subject to onerous visit and contact approval and reporting requirements. These come on top of the normal requirements prescribed for non-FOCI firms. For example, the firm's security officer must grant approvals for foreign visitors from the parent firm, even though an approved visit request or other authorization may already be in place. The additional procedures offer little security value since other DoD and Department of State compliance requirements dealing with classified and unclassified export-controlled data and technology provide such information.

FOCI firms are put at a competitive disadvantage relative to domestic firms by the National Interest Determination (NID) system. FOCI firms must submit a NID to participate in DoD procurements if the participating firms require access to "proscribed information" (i.e., Top Secret, COMSEC, Special Compartmented Information [SCI], and Restricted Data). Currently, FOCI firms require NIDs for each specific project in which they seek to participate. The NID includes a determination by a senior DoD official, normally at the assistant secretary level, that the national interest requires utilization of the FOCI firm and that no domestic firm can be found to perform the work. Program managers who must formulate the recommendation generally do not have the breadth of responsibility or information to permit them to make such a determination. Thus, program managers can be reluctant to approve a NID submission, potentially resulting in the exclusion—to DoD's detriment—of the FOCI firm from the bidding. Moreover, the NID provision concerning domestic availability runs contrary to DoD's interest in broadening its supplier base. The NID procedure, more than any other, sets FOCI firms apart from their domestic counterparts.

Finally, the time limits within the CFIUS review process, a critical link in the U.S. Government's FDI approval chain, could also serve as a barrier to a potential foreign investor. A CFIUS decision on whether or not to conduct an investigation that would ultimately require a decision by the President is made during an initial 30-day review. In some cases, when one or more agencies participating in the CFIUS review are unable to complete their portions, an investigation is undertaken by default, extending the process by up to 90 days. Moreover, questions raised during the initial 30-day review can cause a case to be withdrawn from consideration, requiring the "clock" to be restarted after questions are resolved. Thus, the 30-day constraint can have the unintended consequence of extending—rather than expediting—the CFIUS review. As timing on FDI is often

critical to the financial viability of the transaction, the risk of such delays may be viewed by potential investors as unacceptable.

Risks of Industrial Base Globalization

Commercialization of the DoD Supplier Base

DoD's growing dependence on fast-moving commercial technologies challenges traditional mobilization assumptions. The rapid cycle time of commercial products and technologies creates new problems of "backward compatibility" for subsystems and components. In protracted conflicts, dependence on an inherently global "commercial industrial base" could potentially increase the likelihood of supply disruptions, and the difficulty of sustaining war reserve stocks.

Dependence on the commercial sector may also lead to inconsistencies in product standards as suppliers oriented toward the commercial market seek to achieve product differentiation for competitive purposes. This could lead to a variation in system specifications from supplier to supplier, potentially diminishing DoD's ability to substitute one product for another.

The Department's ongoing, comprehensive transition to an Internet-based business operating environment—designed in part to enhance civil-military integration—places most of DoD's digital activities and information within the cyber-reach of any and all who want to rapidly gather intelligence on the U.S. and/or who wish the United States harm. Such global interconnectivity could provide adversaries an open-source intelligence boon. Adversaries scanning DoD websites will likely exploit electronic data mining and aggregation capabilities to piece together rapidly and inexpensively information on U.S. capabilities, operations and personnel that heretofore would have taken much more time, effort and resources to obtain.

Global interconnectivity can also provide adversaries an electronic penetration pathway into U.S. information systems to harm the confidentiality, integrity or availability of essential information and functionality. Such activities are now referred to broadly in national security parlance as information operations. The principal risk associated with commercial acquisition is that DoD's growing reliance on commercial software—often developed offshore and/or by software engineers who owe little, if any allegiance to the United States—is likely amplifying DoD vulnerability to information operations against all systems incorporating commercial software.

Commercial software products—within which malicious code can be hidden—are becoming foundations of DoD's future command and control, weapons, logistics and business operational systems (e.g., contracting and weapon system support). Such malicious code, which would facilitate system intrusion, would be all but impossible to detect, primarily because of software's extreme and ever-increasing complexity. Moreover, adversaries need not be capable of or resort to implanting malicious code to penetrate commercial software-based DoD systems. They can readily exploit inadvertent vulnerabilities (bugs, flaws) in DoD systems based on commercial software developed by others.

Unfortunately, DoD has little if any market or legal leverage to compel greater security in today's commercial software market. DoD can, however, influence the issue indirectly by sponsoring research into such areas as trust certification and management; software design methodology; proof of correctness; taxonomy of vulnerability; and smart, if non-exhaustive testing. (**Annex IV, *Vulnerability of Critical U.S. Systems Incorporating Commercial Software*,** offers a more detailed discussion of the risks associated with commercial software acquisition and recommendations for risk mitigation.)

Compounding matters, the current personnel security system is ill-configured to mitigate the growing information operations risks. The problems lie generally in the over-classification of information (which skews allocation of security resources), and the inherent limitations of the security clearance model (which provides little, if any, monitoring of personnel for five to 10 years after the clearance is granted). In addition, information technologies have outpaced some of the core concepts upon which the traditional DoD security system is based: the control of physical access, and the distinctions between classified and unclassified information.

Despite all the policies and regulations in place to deny sensitive information to foreign adversaries, the reality is that our personnel security programs have not been able to prevent some cleared U.S. citizens in the most sensitive positions from betraying their trust and committing espionage. (See **Annex VIII, *Selected List of Cleared U.S. Citizens Convicted of Espionage*,** for a list of such cases.) Personnel security efforts have not focused on where they are most needed, nor have they adapted to the changing threat environment. As a result, personnel security has too often been considered an inconvenient bureaucratic intrusion rather than the essential foundation upon which all other security safeguards must ultimately rest.

Security programs have focused on the control of physical access to information and materials, because the spies of the past generally have exploited their physical access to the material they wanted to compromise. However, the practices and tools of physical access control (e.g., access to facilities, controlled areas, or photocopiers) are ineffective against the remote cyber-spy and trusted insider cyber-traitor. Moreover, the damage that can be done by sabotage or manipulation of an information system or network may exceed the harm caused by simple compromise of confidentiality. In the past, a cleared insider might have risked all to bring concealed documents through a controlled perimeter to an off-site copier. Today, he or she can not only download at his or her workstation the information from a computer database, but also penetrate the system or network to bring service to a halt or input bogus commands.

The current personnel and security system also tends to focus primarily on classified information and activities. It is clear today, however, that the classified world is not the only one with a security requirement. DoD has a number of unclassified systems that are, in every sense, "mission critical" (e.g., logistics networks, wartime blood supply management networks) yet essentially unprotected by the existing security system. Moreover, a growing number of people in unclassified positions (e.g., network administrators) have access to, or are indeed charged with the technical protection of, DoD information systems. All are "trusted insider" threats capable of sabotage and

subversion, but all fall outside of the current classification-based personnel security system. So, too, do most of the commercial sector software engineers developing and producing constituent information technologies for military application. Cumulatively, this represents a fundamental shift from as recently as five to 10 years ago, when the majority of people contributing to the design and production of DoD equipment and the day-to-day operations of the DoD enterprise worked under the personnel and industrial security umbrellas.

(**Annex VII, *Globalization and Personnel Security*,** offers a more detailed discussion of the globalization-generated challenges facing the personnel security system and recommendations for meeting them.)

Transnational Defense Industrial Integration

With the U.S. and European defense sectors now contemplating cross-border mergers and acquisitions at the prime contractor level, DoD must weigh the many benefits of such transatlantic industrial integration against the potential risks. While the Task Force generally supports transnational defense industrial integration, there are potential risks of unauthorized or unintended direct or third-party transfer of "sensitive" U.S. military technology. However, the compliance record of foreign firms in the U.S. under FOCI agreements suggests that the potential risks are manageable. Several U.S. Government studies (e.g., those by the General Accounting Office and the Defense Intelligence Agency) suggest that U.S. Government risk mitigation measures have been very successful. Indeed, evidence suggests that regulatory compliance has been of a higher order for domestic subsidiaries of foreign parents than for domestic firms.

If the European defense sector consolidates across intra-European borders, it will challenge—and perhaps require modification of—the existing structure of bilateral security arrangements the U.S. currently holds with individual European companies and governments. This does not, however, affect the *risk* to U.S. security associated with foreign direct investment in the United States. Foreign owners of whatever nationality will continue to be separated from classified or export-controlled U.S. technology under FOCI agreements.

Beyond unauthorized technology transfer, the risks associated with cross-border defense linkages are less clear-cut. To the extent that foreign direct investment in the U.S. defense sector leads to the offshore relocation of development and manufacturing facilities, some are concerned over the potential loss of key domestic defense industrial skills. However, it seems clear at this point that foreign investors are most interested in penetrating the U.S. market, in which case establishing an industrial presence *in the United States* is a top priority. Indeed, viewed in this manner, foreign direct investment could actually lead to the *augmentation* of the domestic defense-industrial skill base, with a higher percentage of U.S. defense workers producing for offshore markets.

Another concern involves potential disruptions in the supply of critical components or subsystems should sole industrial sources move offshore or come under foreign ownership. In the past, the United States has gone to great lengths (such as legally compelling suppliers to remain in business) to preserve at least one domestically owned

and located supplier for certain critical components. Flat-panel displays are a recent example. Yet, this risk would seem to be mitigated by the increasing commercialization of such components. As a result of this trend, DoD can actively maintain and cultivate a much broader supplier network (e.g., by keeping multiple global suppliers defense-qualified so as to avoid potential supply gaps during the qualification period). Indeed, it is quite possible that cheaper and/or better versions of many critical components will be available abroad. With regard to single domestic sources of major systems (almost invariably those producing hugely expensive "capital" systems such as aircraft carriers), DoD constitutes the whole of the consumer base, foreign and domestic, and is not likely to approve the foreign acquisition of such a supplier. Even if DoD were to approve such an acquisition, the only realistic way the foreign owners could stay in business would be to sell to DoD.

Finally, foreign ownership could theoretically erode DoD influence over system design and performance, and perhaps cost. In cases where DoD is the sole consumer of a particular product, it is likely to retain the same influence over the foreign supplier as it does over a U.S. contractor. The exception would be a *government-owned or -controlled* foreign supplier, whose business decisionmaking might be influenced by national political as well as internal economic factors. There exist no outright prohibitions on foreign direct investment by foreign government-owned or -controlled firms. However, consensus exists among Task Force members that DoD should approach with great caution any proposed acquisition of a U.S. defense contractor by a government-owned or -controlled foreign firm.

The risks of a material loss of DoD influence are also low in collaborative projects. Such projects are usually based on the premise that DoD and its foreign partners share both a common military requirement and a desire to spread the financial burden of development and production. As long as these two criteria are adhered to—that is, as long as the proposed project meets DoD requirements while lowering total cost—any risk would be negligible; the Joint Strike Fighter program (in which the United Kingdom is a significant investor) is a perfect example. The calculus may prove different if U.S. and European firms were allowed to merge on the scale seen in the U.S. during the 1990s. Such large-scale transatlantic defense industrial consolidation could theoretically result in a very few large firms selling to dozens of major buying nations. This, some claim, would dramatically reduce DoD's share of the U.S. defense sector's product market and thus greatly curtail its ability to influence system design.

GLOBALIZATION'S IMPACT ON THE INTERNATIONAL MILITARY-TECHNOLOGICAL ENVIRONMENT

From a strategic standpoint, globalization's most significant manifestation is the leveling effect it is having on the military-technological environment in which DoD must compete. Access to commercial technology is virtually universal, and its exploitation for both civil and military ends is largely unconstrained. Many of the most important enabling technologies for information-intensive U.S. concepts of warfare (e.g., access to space, surveillance, sensors and signal processing, high fidelity simulation, and telecommunications) are equally available to the United States, our friends and allies, and

potential U.S. adversaries. In other words, much of the technology the U.S. is most anticipating leveraging to maintain military superiority is that which DoD is *least* capable of denying its potential competitors. The so-called "Revolution in Military Affairs" is, at least from a technology availability standpoint, a truly global affair.

Compounding this narrowing of the U.S. technological advantage are continuing declines in DoD research, development, test and evaluation (RDT&E) and defense industry internal or independent research and development (IR&D) investment. In addition, government and private defense R&D investments are skewed toward near-term priorities (e.g., upgrades to fielded systems and the development of legacy system replacements) and away from fundamentally new capabilities.

The FY99 DoD budget request proposed a 14 percent decrease in RDT&E over the Future Years Defense Program (FYDP). The FY00 budget did propose an overall increase in modernization (procurement and RDT&E) funding. However, while procurement spending was increased from FY99 by $4 billion, RDT&E was actually reduced by $3 billion. Furthermore, over 33 percent of the total FY00 RDT&E request is for modifications to fielded and, in many cases, aging systems, while those RDT&E accounts underpinning the development of new capabilities have been reduced by nearly 25 percent. There is no indication of this trend abating over the FYDP. Both the House and Senate armed services committees, in their FY00 authorization bill reports, stated deep concern that DoD's emphasis on the procurement of and RDT&E investment in current systems was coming at the direct expense of the long-term development of essential military capabilities; the Task Force shares their concern.

Traditionally, defense industry IR&D has funded the development of many of the United States' most advanced military technologies and innovative integrated defense systems. Stealth technology is but one example. Industry has historically put about three percent of the DoD procurement budget back into IR&D. However, with a 70 percent decline in procurement budgets in the past decade, contractors not only have less to spend on IR&D, they appear to be using many of these funds to secure increasingly scarce line-item business and/or maintain profit levels. The result is severely depressed U.S. military-technological innovation when the premium on innovation has never been higher, and a defense industry devoted primarily to the development of what the military says it wants—legacy system replacements—and not necessarily what it needs to meet emerging strategic challenges.

Strategic Implications of Global Technological Leveling

As the technological playing field levels, the United States' potential competitors will be able to modernize their forces and augment their overall capability relative to ours at a much faster rate than was previously possible. One reason is that they will be able to take multiple, concurrent paths to military modernization.

A common path will be through an increasingly permissive and technologically advanced global conventional arms market. The arms market has undergone a striking transformation in the last five or so years, the root cause of which is the contraction in

worldwide defense spending that has increased significantly the pressure on firms to export—and on governments to encourage them to do so.

Three trends can be discerned regarding the characteristics of the equipment available and the manner in which it is being acquired. First, weaponry available on the international arms market is increasingly sophisticated. Exporting countries no longer offer only less-capable versions of their most advanced equipment. Now, in order to gain a competitive advantage, nations are offering state-of-the-art equipment, particularly electronics, sensors and munitions. Indeed, states are willing to part with technologies and systems that, during the Cold War, were among their most highly protected. Further, there exist vibrant "black" and "gray" markets that serve to connect with a willing seller even those states widely targeted for export control. Moreover, many states are actually developing highly advanced products primarily or even solely for the export market. Russia, for example, is reportedly offering the Zhut (Beetle) MiG-29 aircraft radar to foreign customers, though it has yet to enter service with the Russian Air Force. Consumers, meanwhile, are using their newfound leverage to demand the best. The United Arab Emirates, for example, insisted that the F-16 fighter aircraft for which they were negotiating be equipped with an AESA (Active Electronically Scanned Array) radar system, a capability not yet in the USAF inventory. The U.S. Government eventually agreed to the condition, which constituted a significant and controversial concession.

Second, instead of buying new systems, many nations are aggressively upgrading older systems. This provides less affluent states, whose inventories would have otherwise obsolesced, with increased combat capabilities and extended service life at acceptable cost. The upgrade strategy is not new, but the roster of upgrade-prone states is expanding, as newly independent and other cash-strapped nations seek to increase the capability of aging inventories. Significantly, with domestic production markets relatively stagnant, upgrades are of greater relative importance to defense manufacturers. Economic pressures on both supplier and consumer suggest an increasingly robust, technologically advanced upgrade market in the future.

Finally, a new concept known as "hybridizing" is enabling states to combine the best technology from around the globe. For example, it is now possible for a nation to buy through a systems integrator a Russian airframe outfitted with British or U.S. engines, "stuffed" with Israeli avionics, and armed with French precision munitions. Hybridizing also allows states to balance particular countries' technological weaknesses with others' strengths. A French firm, for example, is providing digital signal processing technology for insertion into Russian fighter radars, allowing customers to capitalize on Russia's strength in high-powered radar and surmount Russia's traditional data-processing weaknesses.

In short, the international conventional arms market, once driven and constrained mainly by political imperatives, is now shaped heavily by economic considerations. The resulting trends, described above, suggest that the effectiveness of conventional arms and defense technology export controls will continue to erode, and that most types of conventional military capabilities will be available to those who can afford them.

Beyond the arms market, the general diffusion of technological know-how and commercial availability of so-called "strategic" or "enabling" dual-use technologies (e.g., advanced machine tools, high-performance computing, manufacturing of biotechnology products) will likely yield rapid advances in competitor industrial infrastructure development and, in turn, indigenous weapons production capability. Moreover, the commercial sector will offer an increasingly wide array of both advanced components and subsystems (particularly software and microelectronics) to aid indigenous defense system production and system upgrades, and of full-up systems (particularly information- and communications related) offering direct capability enhancement.

With regard to the latter, states will be able to achieve dramatic increases in military capability by acquiring via the burgeoning commercial space industry whole ranges of C3ISR (command, control, communications, intelligence, surveillance and reconnaissance) capabilities heretofore available only to the great powers. In 1996, commercial space investment for the first time exceeded that of the world's militaries, and the trend will continue. Roughly 1,700-2,000 commercial satellite launches are planned over the next decade, increasing the number of satellites in orbit by an order of magnitude. Satellite communications using low- and medium-altitude constellations will provide reliable wide-band Internet access to all corners of the globe. The surveillance satellite market will evolve fairly rapidly, with four or five suppliers providing, by 2000, visible and multi-spectral images of 1 meter (or better) quality to commercial customers and to military customers in states unable to develop and field the capabilities indigenously. The availability of such precise and up-to-date surveillance information, coupled with reliable positioning and timing data from the GPS (Global Positioning System) or GLONASS (**GLO**bal **NA**vigation **S**atellite **S**ystem), will give potential adversaries unprecedented and relatively cheap cruise/ballistic missile and direct-attack weapons targeting capability. (**Annex V, *Commercial Space Services and their Impact on National Security*,** provides a more complete discussion of emerging commercial space services and their potential impact on national security.)

Moreover, owing to the ready availability of many key military capabilities, states will be able to *time* their investments in order to peak militarily when their forecasted opponent is least suited to engage them. This may present a particularly vexing challenge to the United States, which, by virtue of its commitment to maintaining a large general-purpose force structure, must spread its investment resources much more broadly. Because DoD does not have the resources to modernize all force elements concurrently, it must alternate modernization efforts *between* major force elements, frequently at decade-long (or longer) intervals, making it all but impossible for DoD to maintain state of the art forces across the board. Often, the stated DoD or Service rationale for investing in a particular force element is rooted not in a strategic imperative, but rather in the fact that it is the said force element's "turn" to be recapitalized. This limits DoD's investment agility, and thus its ability to react swiftly to unanticipated strategic military-technical developments. Also limiting DoD in this regard are the lingering cultural and, to a lesser extent, regulatory constraints on tapping the commercial sector—by which potential U.S. competitors may not be similarly shackled. Consequently, and particularly as militaries become more reliant on commercial products and services, adversaries over which the U.S. is otherwise dominant can be expected to achieve superior capabilities in narrow—yet potentially critical—areas.

Furthermore, with virtually the full range of military technologies and capabilities available, competitors will also be able to *tailor* more effectively their investments to their particular geo-strategic circumstances to achieve scenario-specific advantages over potential foes. As previous DSB studies have pointed out, those states preparing for potential conflict with the United States will seek to capitalize on the great distances U.S. forces must travel to engage them, and U.S. forces' near-absolute reliance on unimpeded access to and use of ports, airfields, bases, and littoral waters in the theater of conflict.

To exploit these vulnerabilities, potential competitors are not trying to match DoD ship-for-ship, tank-for-tank, or fighter-for-fighter. Rather, they are *investing asymmetrically*, channeling their more limited resources into now widely-available (and increasingly affordable) capabilities, conventional and unconventional, that could allow them to deny U.S. forces both rapid access to their region and/or and sanctuary once in-theater. The 1995 DSB summer study estimated that potential U.S. regional adversaries spending on the order of only $15-20 billion over a decade in the global marketplace could develop robust theater-denial/disruption capabilities. These include conventional anti-naval forces (e.g., ultra-quiet diesel submarines, advanced anti-ship cruise missiles and sophisticated sea mines); theater-range ballistic and land-attack cruise missiles (with the latter expected to be available in the thousands, and, increasingly, with low-observable characteristics); and nuclear, chemical and biological weapons.

In addition, future U.S. competitors will leverage the commercial space sector to achieve so-called "step function" gains in anti-access capability. Capabilities such as space-based communications, surveillance, navigation services and equipment will become increasingly available through a variety of multinational consortia. Such unobstructed access to space for C3ISR support will allow even the most resource-constrained adversaries to monitor the location of, target and precisely attack U.S. forces in the field, at theater bases, ports and airfields, and moving through critical naval chokepoints. Viewed in this manner, technological leveling—globalization's most strategically unsettling manifestation from a U.S. perspective—is clearly the engine of the emerging "anti-access" threat.

Consequently, there is growing—if uncelebrated—risk inherent in U.S. power projection and force modernization strategy. Strategic risk is defined here as a discernible decrease in U.S. forces' capability to protect vital U.S. interests relative to adversaries' capability to threaten them: a potentially serious erosion of military dominance. At the root of the problem are the inherent limitations—namely, sluggish deployment times and heavy dependence on theater access—of the legacy, primarily short-range general-purpose force elements to which the vast majority of the Services' modernization funding is currently dedicated. Thus, as Under Secretary of Defense for Acquisition and Technology Jacques Gansler told Congress, "It is of the highest priority and greatest urgency that we act now to...make the necessary migration away from traditional weapons systems that were designed to counter a Cold War threat, not the asymmetrical threats we face from terrorists and rogue nations." Viewed in this light, the continued budgetary, strategic and force structuring primacy of legacy systems in DoD budgets has a clear and high opportunity cost: the investment agility necessary to transform U.S. strategy and forces to meet the emerging strategic challenges posed by global military-technological leveling.

Export Controls: An Imperfect Panacea

The United States has sought to prevent or mitigate the strategically detrimental effects of global military-technological leveling by coordinating with its allies (namely, Europe and Japan) the multilateral control of conventional military and dual-use technology exports. This approach worked reasonably well during the Cold War through the Coordinating Committee on Export Controls (CoCom), a NATO-oriented regime that sought to control the export of "strategic" dual-use technology to communist states, namely, the Warsaw Pact states and China. Today, multilateral regimes designed to control enabling technologies for weapons of mass destruction (WMD) and their means of delivery (e.g., the Nuclear Suppliers Group, the Australia Group and the Missile Technology Control Regime) remain arguably effective at slowing, though by no means stopping, the spread of nuclear weapons and longer-range ballistic missile technology.

However, multilateral controls today are for all practical purposes ineffective at manipulating global access to dual-use technology and, for reasons described in the foregoing discussion of the world arms market, have been only marginally more successful in the conventional weapons arena. CoCom's success derived from its members facing a common threat—the Warsaw Pact and, to a lesser extent, China—and thus sharing a common objective: the retardation of Warsaw Pact and Chinese technological advancement. CoCom also benefited from the disproportionate leverage the United States, its leading advocate, held over the other members as the guarantor of Western security. The Cold War's end undermined this cooperative impetus, and the U.S. can no longer count on its allies, its closest competitors in the high-tech sector, to follow the U.S. lead.

The lukewarm success of CoCom's successor, the Wassenaar Arrangement, is testament to the difficulty of multilateral technology controls in the post-Cold War era. Wassenaar's lack of strong central authority and its dearth of explicit target countries is a reflection of the times—the absence of a single large threat and lack of agreement over the nature and seriousness of the smaller threats. This inherent weakness has complicated its development and made it more difficult to achieve consensus among the expanded (from CoCom) membership on which states to which they should control exports. With the exception of a few unanimously-targeted pariah states (namely, Iraq, Libya, Iran and North Korea), for which it has been a reasonably effective control mechanism, Wassenaar is proving, in the words of one observer, little more than a "paper tiger."

China is perhaps the best and certainly the most timely example of the difficulty of coordinating multilateral technology controls in the new environment. Under CoCom, the West had a well-coordinated position on dual-use trade with China. In the wake of CoCom's dissolution, a chasm has developed between the U.S. and many of its Western allies, who no longer view China as a threat and have relaxed or lifted dual-use export restrictions to China accordingly. This, in turn, has rendered many U.S. controls on exports to China essentially unilateral, thus neutralizing their utility as constraints on Chinese acquisition of dual-use technology.

Also limiting the utility of dual-use export controls is the ubiquity of critical technologies and the ease of their transfer. Consider the case of high-performance computing.

Microprocessors, which are the essential ingredient for high-performance computers (HPCs), have long been a commodity product widely available on the world market from a vast range of sources. Chip-maker Intel alone has over 50,000 authorized dealers worldwide. Personal computers are similarly uncontrollable. Each year, U.S. and foreign companies manufacture millions of PCs and sell them the world over, often via mail order and the Internet. The technology to "cluster" these computers (i.e., link them together to multiply their computing power) is also available online. Through clustering, it is possible to create computer systems ranging in computing power from 4,000-100,000 MTOPS (millions of theoretical operations per second)—equivalent to the supercomputers currently under strict export controls. In other words, while the most advanced U.S. stand-alone high-performance computers may be controllable, high-performance *computing* is not.

High-performance computers are a good example of limited controllability, but the same is true for other sectors where the state-of-the-art is advancing rapidly, such as telecommunications, and controlled software. It is somewhat easier for the United States to control the transfer of large capital items, mainly because the customer base is smaller and the products cannot be easily and inexpensively cloned and/or scaled-up in capability (e.g., as PCs are clustered into HPC-level systems). However, as is the case with HPCs, this does not mean the technology will not be available outside the United States. In some of these sectors, such as machine tool and semiconductor manufacturing equipment, the U.S. has a minority global market share and the technology is widely available abroad. In others, such as satellites, the U.S. currently has a strong global position but is under growing pressure from competent competitors seeking to increase market share.

Some argue that the obstacles to effective multilateral controls suggest that the United States should become even more restrictive unilaterally. In some cases, this may be necessary, but doing so broadly in the face of globalization is likely, in the end, to do the United States more harm than good. DoD is relying increasingly on the U.S. commercial advanced technology sector to push the technological envelope and enable the Department to "run faster" than its competitors. DoD is not a large enough customer, however, to keep the U.S. high-tech sector vibrant. Exports are now the key to growth and good health. In the computer and communications satellite industries, for example, between 50% and 60% of all revenues come from foreign sales. Any significant restriction on exports would likely slow corporate growth and limit the extent to which profits can be put back into research and development on next-generation technology. This is particularly true for internal or independent R&D (IR&D) designed to address particular DoD concerns, which, because it is less likely to yield products with near-term commercial demand, would likely receive even lower priority during any IR&D decline. If U.S. high-tech exports are restricted in any significant manner, it could well have a stifling effect on the U.S. military's rate of technological advancement.

If the United States responds to what some parochially and inaccurately view as a preventable hemorrhaging of U.S. advanced technology (vs. the irresistible leveling of the global technological playing field) by unilaterally tightening controls on high-tech exports to states such as China, new competitors in Taiwan, Korea, Japan, and Europe can be expected to move quickly to fill the market void. The U.S. lead in most dual-use

sectors is based not on the United States being the sole possessor of the technology, but rather on the comparatively high quality of U.S. products and the efficiency with which they are produced (which enables competitive pricing). Shutting U.S. industry out of major markets such as China will necessarily create viable competition where little currently exists. As has been demonstrated in other sectors, the increased competition will not be limited to the Chinese market. New competitors will use their market share in China and all its benefits (e.g., accelerated IR&D funding) as a springboard to challenge U.S. dominance elsewhere. In other words, if the U.S. were to unilaterally tighten dual-use controls to China, the loser is not likely to be the Chinese. Rather, the losers will be U.S. industry, whose technological and market leadership will face new challenges, and DoD, whose access to the world's most advanced technologies will be at the very least complicated, and perhaps compromised, by virtue of their being developed and produced by non-U.S. firms.

Furthermore, because the dual-use sector is fully globalized, export control tightening meant to deny single states such as China access to certain technology can do unintended damage to vitally important U.S. business relationships elsewhere. Congress' recent decision to return commercial communications satellites to the State Department's U.S. Munitions List from the Commerce Department's dual-use list—and the U.S. Government's interpretation of Congress' direction—may already be having such an effect. Consider the case of Europe. The U.S. and European space sectors are deeply interconnected. In the midst of the controversy leading up to the decision to move satellites back to State—intended by Congress as a means of tightening controls over satellite exports to China—the U.S. Government has become much stricter in its interpretation of the ITAR, which govern the export of items on the munitions list. This is particularly true of the DoD and its interpretation of ITAR Part 124.15(a), which states specifically that: "The export of any satellite or related item . . . or any defense service controlled by this subchapter associated with the launch in, or by nationals of, a country that is not a member of the North Atlantic Treaty Organization or a major non-NATO ally of the United States always requires special export controls, in addition to other export controls required by this subchapter. . ." DoD has insisted on applying these "special export controls" on our NATO and major non-NATO allies (as is allowed for under Part 124.15(c)); it is this approach that may be proving the most damaging.

Most European satellites contain U.S. components that are also subject to the stricter controls. The U.S. Government's stricter interpretation of the ITAR may also be having a negative ripple effect on the behavior of the U.S. space industry, which has, in turn, ratcheted up its own security procedures. According to some in Europe, this is making it increasingly difficult to do business with the U.S. space industry. Said one European space industry official in a recent media report: "To have a simple telephone conversation with a U.S. customer or supplier, I have to inform him of my wishes 30 days in advance, then fax him an outline of what I want to talk about. The fax gets passed on for clearance by the U.S. State Department: What is the purpose here—national security or protectionism?"

The long-term effects could be damaging. The European Union (EU) is getting involved in the issue through its executive arm, the European Commission, which asked European industry to present them with a list of the trade-damaging effects of the U.S. policy shift.

The EU will then discuss its findings with the United States. EU officials have said that their aim is to express surprise at what must have been a "terrible mistake in the formulation of this new policy" that they claim is harming U.S.-European space industry relations. European satellite and rocket builders, which currently depend on U.S. companies to assure their supply chain, will logically look elsewhere for suppliers if the of doing business with the U.S. remains unacceptably high.

A tightening of dual-use controls could also spawn—or hasten—the development of indigenous R&D and production capabilities where they might not otherwise flourish. For example, China has the capacity to produce high-performance computers indigenously. As of 1997, China had developed at least three HPC systems: the Dawning-1000, Galaxy-II and Galaxy-III. While China cannot currently compete with U.S. companies on the global market, they can produce machines with performance sufficient to provide many of the military capabilities they seek, though perhaps at greater time, effort and cost than would be the case with the highest performance computers. Denying these countries U.S. products could very well encourage their own development and production.

Finally, increased technology protection amidst global technological leveling could well limit the special influence the United States might otherwise accrue as a global provider and supporter of military equipment and services. This includes intimate knowledge of, and access to, military systems that only the supplier would have, and that could prove militarily instrumental in crisis and conflict and is particularly true regarding communications and information systems.

The strategic significance of the ongoing leveling of the global military-technological playing field cannot be overstated. It presents a direct challenge to *the* fundamental assumption underlying the modern concept of U.S. global military leadership: that the United States enjoys disproportionately greater access to advanced technology than its potential adversaries. This assumption also underpins the increasingly strained logic holding that technology controls are the *sine qua non* of U.S. military dominance.

However, such a parochial assumption is simply not consistent with the emerging reality of all nations' militaries sharing essentially the same global commercial-defense industrial base. The resulting erosion of long-standing technical and economic barriers to acquiring advanced militarily-useful technology will increasingly negate enduring U.S. advantages in technology development, namely, superior infrastructure, education and resources. By virtue of its *comparatively* large defense R&D investment—past and present—the United States will likely maintain over the long-term a developmental advantage over its competitors in a limited number of cutting-edge, defense-specific technologies; directed-energy weaponry is one example. However, such niche technological advantages will not sustain a meaningful, long-term military capability gap between the United States and its potential adversaries.

Rather, with the whole world working from essentially the same military-technological "cookbook", the United States will need to rely on its unique strengths as a "chef", that is, as the world's most innovative integrator of militarily useful—though not always U.S.-developed—technology. The U.S. will need to redouble its efforts at out-innovating, out-

integrating and out-investing its competitors. This involves exploiting our currently superior systems integration skills, training, leadership, education and overall economic/industrial wherewithal to translate globally available technology into dominant military capability. To remain dominant, DoD will need to not only "run faster", but also to "pick alternate routes"—that is, respond asymmetrically to its competitors' asymmetrical strategies by intelligently altering its own warfighting strategy and investment plans. Indeed, sustaining military dominance in the face of technological leveling will ultimately come down to the age-old questions of how—and with what—DoD chooses to fight.

4. Findings and Recommendations

4.1 MAINTAINING U.S. MILITARY DOMINANCE AMIDST GLOBAL TECHNOLOGICAL LEVELING

Findings

- It is likely that a majority of militarily-useful technology will eventually be available commercially and/or outside the United States as a result of many factors, all of which are direct manifestations of the globalization phenomena: an increasingly permissive and sophisticated conventional arms market, the commercialization of formerly military technology (e.g., GPS, communications satellites), the increasing reliance of militaries worldwide on commercially-developed technology (e.g., information technology), and the declining effectiveness of defense and dual-use export controls.
- The erosion of long-standing technical and economic barriers to advanced technology will increasingly undermine traditional U.S. advantages in technology development, namely, superior infrastructure, education and resources. This technological advantage is further narrowed by steep declines in DoD research, development, test and evaluation (RDT&E) and defense industry internal research and development (IR&D), and the related skewing of such R&D investment toward near-term priorities and away from fundamentally new capabilities. The result is severely depressed U.S. military-technological innovation at a time when the premium on innovation has never been higher.
- Potential competitors are exploiting their newfound access to militarily useful technology in a manner strategically detrimental to DoD. They are not trying to match U.S. strengths or achieve across the board military parity with the United States. Rather, as the last four DSB summer studies have pointed out, they are channeling their more limited defense resources into widely-available capabilities that could allow them to exploit a fundamental weakness of American power projection strategy: the absolute reliance of most U.S. forces on unimpeded, unrestricted access to and use of theater ports, bases, airfields, airspace and coastal waters. By 2010-2020, potential adversaries, exploiting a truly global military-technical revolution, will likely have developed robust capabilities—conventional and unconventional—for disrupting U.S. homeland preparations to deploy to the theater of conflict; denying U.S. forces access to the theater; degrading the capabilities of the forces the U.S. does manage to deploy; and, in the process, raising, perhaps prohibitively, the cost of U.S. intervention.
- Consequently, there is growing risk inherent in U.S. warfighting and force modernization strategy. If left unchecked, this asymmetric investment by potential competitors may lead to a decline in the U.S. military's utility for influencing events or protecting U.S. global interests at acceptable cost—a serious erosion of military dominance.
- The United States' capability to effectively deny its competitors access to militarily-useful technology will likely decrease substantially over the long-term. Multilateral and unilateral export controls will likely continue to play a primary role in the pursuit

of U.S. foreign policy objectives achieved by restricting access to U.S. technologies, products and services with both defense and dual-use applications. However, the utility of export controls as a tool for maintaining the United States' global military advantage is diminishing—though hardly disappearing—as the number of U.S.-controllable militarily-relevant technologies shrinks. Accordingly, application of these controls must be thoroughly considered with the understanding that they will not stop the eventual acquisition of these technologies and capabilities by a dedicated adversary. At most, they will buy the United States time to engage in the time to engage in the further research, development and acquisition required to maintain its position of dominance.

- A failure by U.S. leadership to recognize this fundamental shift—particularly if masked by unwarranted confidence in broad or even country-specific defense and dual-use export controls—could foster a false sense of security as potential adversaries arm themselves with available technology functionally equivalent to or better than our own. A significant tightening of export controls would also limit the special influence the U.S. might otherwise accrue as a global provider and supporter of military equipment and services. This includes intimate knowledge of, and access to, military systems that only the supplier would have, and that could prove militarily instrumental in crisis and conflict. Furthermore, and perhaps most important, shutting U.S. companies out of markets served instead by foreign firms could inhibit the competitiveness of the U.S. commercial advanced technology and defense sectors upon which U.S. economic security and military-technical advantage depend.
- Accordingly, the more the United States depends on technology controls for maintaining the capability gap between its military forces and those of its competitors, the greater the likelihood that gap will narrow. To hedge against this risk, DoD's strategy for achieving and maintaining military dominance must be rooted firmly in the assumption that controls ultimately will not succeed in denying its competitors access to militarily-useful technology. As a critical early step toward adapting its strategy, DoD must revisit both the extent to which it relies on technology protection for the maintenance of military dominance and the very nature of its technology security policy.
- Future U.S. military dominance will derive less from the protection of individual defense-related technologies and more from proactive measures taken by DoD to retain and/or acquire essential military capabilities (defined as those capabilities DoD must have to defend U.S. global interests at acceptable cost). Accordingly, DoD's strategy for maintaining military dominance should center on the concept of creating and preserving essential military capabilities rather than protecting their constituent technologies. To achieve this objective amidst global technological leveling, DoD will need to rely on, and maintain a robust level of investment in, the United States' strengths. In addition to stronger and more targeted, high-leverage military R&D, this involves exploiting our currently superior systems integration skills, military training and leadership, education and resources to translate globally-available technology into dominant military capability.
- To stay dominant, DoD will need not only to "run faster", but also to "pick alternate routes"—i.e., respond asymmetrically to potential competitors' asymmetrical strategies and investments. Indeed, decisions about *how* and with *what* DoD chooses

to fight will likely be as, if not more, consequential for long-term U.S. military dominance than those regarding *how much* DoD is allowed to spend.

Recommendations

4.1.1 The Deputy Secretary of Defense, with the assistance of the Chairman of the Joint Chiefs of Staff and the Under Secretary of Defense (Acquisition and Technology) should develop a permanent process for determining a continuously-evolving "short list" of essential military capabilities and individual strategies for preserving each essential capability.

The list of essential military capabilities and strategies for their preservation are needed to inform the development of: (1) U.S. warfighting strategy and the forces to underpin that strategy (by identifying how and with what the U.S. will need to fight to remain dominant), (2) DoD positions on technology and personnel security (by helping to identify those capabilities and/or constituent technologies which DoD should attempt to protect and how vigorously they should be protected); and (3) DoD acquisition risk mitigation measures (by identifying those systems that should be the focus of intense effort to ensure system integrity).

The Task Force recognizes that developing this concept into an authoritative, actionable paradigm requires a permanence of effort not consistent with the DSB task force format. Nonetheless, to assess the viability of this critical recommendation, the Task Force developed an *illustrative* list of essential (if somewhat broadly defined) military capabilities and preservation strategies (located in **Annex VI, *Maintaining Military Dominance through the Preservation of Essential Military Capabilities***).

An underlying theme of the Task Force's work was to consider military operations and military preparedness from a coalition perspective. That is, the Task Force did not back away from the need to maintain a unilateral U.S. capability, but considered the coalition capability as the more difficult one to construct. Close attention was therefore paid to those particular difficulties arising out of the coalition context. In addition, the Task Force reached some key conclusions:

- ***Strategies for preserving essential capabilities <u>will not</u> rely heavily on restricting the export of U.S. military goods and services, or the protection of large amounts of military information.*** Rather, the Task Force's strategies identified a few, very specific matters that were both worth protecting and actually protectable (i.e., they or their functional equivalent were neither available outside the U.S. nor easily replicable). These very specific matters, in turn, were deemed worthy of reasonably expensive measures for protection, measures that are too expensive and cumbersome to be applied to large amounts of information spread widely throughout the military establishment.
- ***Essential capabilities are often best preserved by "direct enhancement".*** That is, the opportunities for protecting current capabilities from exploitation by adverse parties are, in many cases, simply so expensive, impractical, ineffective or have such untoward side effects that our best strategy would be to work as hard as we can to stay ahead of our competitors. This is a common business strategy

and has long been a favored development strategy in air superiority fighters, tanks and other weapon systems that engage in head-to-head combat experiences.

- ***The revolution in military affairs (RMA), as embodied in Joint Vision 2010, and the explosion of modern sensors and other information technology that enables the RMA, open up new opportunities to bridge the tension between the opposing desires for collaboration and protection.*** For example, most modern munitions, maneuver platforms, and operational units will be much more effective when coupled to the U.S. C3ISR base than when cut off from it. This opens up the opportunity to complement and enhance the military capabilities of countries to which we have transferred equipment and training well after the transfer has been made.

The Task Force identified four common strategy elements for preserving essential military capabilities:

- ***Direct enhancement:*** Strengthen essential military capabilities through modernization and effective tactical employment in both joint and coalition contexts.
- ***Exploit commercial products and services:*** Identify, advocate, exploit, stimulate, and adapt to commercial sources for defense products and services. Such efforts should include efforts to mitigate the risks of unauthorized disclosure of the capabilities derived from these technologies.
- ***Identify vulnerabilities:*** Identify vulnerabilities, especially those arising from the acquisition of commercial software, to enable DoD to minimize the risk of incorporating commercial technologies in its systems and "systems of systems." Institutionalization of vulnerability analysis is no less important than the institutionalization of advocacy for commercialization.
- ***Protect defense-related technology:*** Protect defense-related technology or knowledge from compromise or hostile exploitation. Though the list of U.S.-controllable technologies is shrinking, the Task Force generally believes that there will likely always be a small number (potentially including certain manufacturing and systems integration technologies) so instrumental to the preservation of an essential U.S. military capability as to merit the highest level of protection. Similarly, there may be systems or components so critical to a particular capability that they must be produced "U.S. only" and/or without commercial components.

Reflecting the prominence of these four pillars:

- all of the essential capability preservation strategies developed by the Task Force relied upon:
  - a strong science, technology and advanced development program for direct enhancement;
  - teams (e.g., "gold teams") to identify and advocate opportunities to enhance military capabilities through commercial acquisition and/or the employment of commercial acquisition practices; and

  - teams (e.g., "red teams") to identify vulnerabilities associated with both defense sector globalization and commercial acquisition (particularly software), and to devise practical methods to avoid and mitigate their consequences.
- most of the strategies relied on only the most selective use of traditional classification and physical security to protect critical information and intellectual property; and
- all of the strategies recognized:
  - the essential role played by systems integration, realistic combat training and continuous product improvement in modern combat systems; and
  - that coalition warfare is both more likely and more complex, and thus should usually be the limiting design consideration, even though force structure and architecture must provide for adequate unilateral capabilities.

Most of the preservation strategies rely on each of the four strategy elements to some extent. The government, in constructing concrete programs to pursue these strategies would, of course, need to be guided by detailed examination as to costs vs. benefits, conformance to statute and other normal programmatic considerations. The Task Force believes that its recommendations are feasible in those regards, but did not have the resources to conduct detailed examinations.

4.1.2 DoD should adapt its technology security policy to the emerging reality of global technological leveling.

The United States has a national approach to technology security, one in which the Departments of State and Defense both play essential roles. The Task Force does not challenge the propriety of the Department of State's statutory obligation to evaluate proposed defense technology transfers against U.S. foreign policy objectives. That said, the leveling of the global military-technological playing field also necessitates a substantial shift in *DoD's* approach to technology security, the principal objective of which is to help maintain the U.S. military-technical advantage.

The Task Force recommends that DoD shift substantially its particular approach to technology security, with the following policy guidelines:

- DoD should attempt to protect for purposes of maintaining military advantage *only* those military and dual-use capabilities and technologies of which the United States is the sole possessor (and for which there are not functionally equivalent foreign counterparts), or which are effectively controlled by like-minded states. Protection of capabilities and technologies readily available on the world market is, at best, unhelpful to the maintenance of military dominance and, at worst, counterproductive in this regard. Where there is foreign availability of technologies, a decision to transfer (or not) need only be made on foreign policy grounds by the Department of State. DoD should no longer review export license applications as part of its role in the arms transfer process when foreign availability has been established. This will allow the DoD licensing review to

concentrate on cases where the availability of technology is exclusive to the United States.

- Military capability is created when widely-available and/or defense-unique technologies are integrated into a defense system. Accordingly, DoD should give highest priority in its technology security efforts to technology integration capabilities and the resulting military capabilities themselves, and much lower priority to the individual technologies comprising both.
- DoD should focus primarily on protecting those technology integration and resulting military capabilities whose protection is deemed necessary to preserve an essential military capability or function. In limited cases, DoD may need to protect aggressively U.S.-unique, cutting-edge knowledge and/or individual military technologies in order to preserve an essential U.S. military capability. In short, DoD should put much higher walls around a much smaller group of essential capabilities and technologies.
- The current level of industrial/personnel security effort and resources should be redistributed to tighten security measures in areas deemed essential and relax measures elsewhere.

4.1.3 The Secretary of Defense, in conjunction with other appropriate U.S. Government agencies, should establish and maintain a real-time, interagency, electronic database of globally available (domestic and foreign) militarily-relevant technologies and capabilities (comprising know-how, components, subsystems, systems and services).

Information on the foreign availability of defense-unique and dual-use technologies, products, and services functionally equivalent to U.S. versions is an increasingly important input to both defense and dual-use technology transfer decisions and weapons development and acquisition choices. Foreign availability is one of the arms transfer criteria identified in the President's Conventional Arms Transfer policy for consideration in licensing decisions. The Task Force views foreign availability (in conjunction with military essentiality) as one of two principal criteria in deciding what the U.S. should attempt to protect through export control and the classification process. The recommended database will be of great value in providing objective information to decision makers concerning what is available on the world market and cannot be controlled in any event when the U.S. Government has to make judgement allowing sale or transfer.

A foreign availability database would serve many communities beyond export control. Weapon system developers would be able to access a broader range of technologies than might otherwise be available domestically. A detailed and comprehensive understanding of foreign technology developments pertinent to military applications is useful to defense planners. If augmented by near-real time intelligence support, the database can enhance law enforcement as well.

There are several existing governmental activities, including those carried out by DoD, the Military Departments, and the Department of Commerce, which support the creation and maintenance of international technology databases that reflect foreign availability.

However, no integrated database exists. This recommendation is designed to fill that critical gap.

Developing and maintaining the recommended database will require non-trivial resources and continuing advocacy. Invariably, such activities become candidates for elimination when resource allocation decisions are made. Such judgements should address the importance and relevance of the database. In this case, the database is required to make balanced judgements about the export of defense and dual-use systems and technologies.

The Task Force does not presume to understand fully the level of effort required to implement this recommendation. The Task Force is, however, confident that the government need not start from scratch. Government agencies currently collect a substantial amount of information pertinent to such a database. The Task Force believes that DoD can make rapid progress in implementing this recommendation if it focuses initially on assembling and managing in a useful manner the data already being collected.

The Task Force recognizes that it will be extremely difficult if not impossible to attain through implementation of this recommendation absolute knowledge of *all* militarily-relevant technologies and capabilities available abroad. Yet, the perfect should not be allowed to be the enemy of the good. The nation will be well-served by any meaningful improvement in the U.S. Government's ability to determine foreign availability in support of export control/arms transfer and developmental decision-making.

4.1.4 The USD(A&T) should establish a recurring, formal review of weapon system developer classification guidelines with regard to weapon system design, development, production and operation.

DoD Directive 5200.39 requires weapon system developers to create and keep a current classification guideline concerning weapon systems for which they are responsible. This guidance is called a Delegation of Disclosure Authority Letter (DDL). On September 9, 1999, the Deputy Secretary of Defense signed a memorandum to those responsible for classifying such information, adjuring them to observe these responsibilities. The USD(A&T) needs to ensure that, as weapon system technology becomes available abroad, weapon system information is declassified accordingly. Thus, USD(A&T) should establish a recurring review of weapon system developers' current classification guidelines with an eye towards broad declassification. This type of review will be of great utility in three principal areas identified elsewhere in this report: improving and streamlining the technology transfer and export control process; fostering cross-border defense industrial collaboration; and strengthening and streamlining the personnel security clearance process.

4.2 COMMERCIAL ACQUISITION

Findings

- The commercial sector offers a wide range of integrated services, systems, subsystems and building block technologies to help DoD meet its modernization and support requirements more rapidly and, in many cases, more cost-effectively than the traditional defense sector. The commercial sector is also a source for leading-edge capabilities and services. Though DoD has already reaped significant benefit from the commercial sector (particularly in the information technology arena), much potential remains untapped.
- To stay ahead of its potential competitors, who can be expected to tap the commercial sector to accelerate their own modernization efforts, DoD must realize fully the potential of the commercial sector to meets its needs. This involves not only *exploiting* available commercial products, but also *stimulating* commercial industry to shape the development of new products and services to better meet DoD needs, and, increasingly, *adapting* DoD requirements to operationally acceptable commercial solutions and developing new concepts that fit commercial availability of products or services.
- Commercialization will make it necessary for the Department to become more agile, and to make more decisions at subordinate levels. Moreover, DoD will have to be more responsive to new ideas, and to accept the loss of complete control over its technological future. The Department will also need to pay close attention to the commercial economy and employ scientists, engineers, computer scientists, and technicians to remain up-to-date in what may appear to be a random process of development.
- The barriers to realizing the commercial sector's potential to meet defense needs are primarily cultural. The risk-averse nature of the DoD acquisition community leads to very conservative engagement with the commercial sector. This suggests a clear need for stronger advocacy of commercial acquisition by the DoD leadership.
- Regulatory barriers to full DoD engagement with the commercial sector also linger. Certain statutes underlying the Federal Acquisition Regulations (FAR) and Defense FAR Supplement (DFARS) restrict DoD procurement of foreign commercial products. The sheer volume, complexity and fluidity of the regulations embedded within the FAR and DFARS discourage commercial firms, U.S. and foreign alike, from doing business with DoD. Accordingly, the Task Force concluded that the statutes underlying the FAR and DFARS constrain DoD's ability to access the global commercial market at a time when such access is critical to the maintenance of U.S. military dominance. The Task Force believes that a comprehensive review of the FAR and DFARS would illuminate the need for a substantial number of statutory changes (repeals or modifications).
- The principal risks associated with commercial acquisition lie in the software area, where heavy reliance on commercial software—often developed offshore and/or by software engineers with little if any allegiance to the United States—is almost certainly amplifying DoD's vulnerability to adversary information operations. The Task Force believes that the risks associated with commercial hardware acquisition

are generally manageable via current testing methods for components, subsystems and systems.

- Commercial software products, within which malicious code can be hidden, are becoming foundations of DoD's command and control, weapons, logistics and business operational systems. Such malicious code, which would facilitate system intrusion, would be all but impossible to detect via traditional testing, primarily because of commercial software's extreme complexity, and the ever-increasing complexity of the systems into which commercial software is being incorporated. Moreover, cyber-aggressors need not be capable of or resort to implanting malicious code to penetrate commercial software-based DoD systems. They can readily exploit inadvertent and highly transparent vulnerabilities (bugs, flaws) in commercial software products that have been incorporated into DoD systems.
- DoD has little if any legal or market leverage with which to compel commercial software developers to build in or guarantee enhanced product security and reliability.
- Risk management of systems incorporating commercial software is not currently practiced assiduously at every stage of a system's life cycle (i.e., from concept development through operations and maintenance). Moreover, accountability for system integrity is neither fixed nor resting at a sufficiently authoritative level. It is likely that accountability should reside with the Department's Acquisition Executives.
- Research on all facets of software security is inadequately funded and the focus is too diffuse. The "customer" for such security research is often hard to identify; the Department's Acquisition Executives should identify themselves as avid customers for this research.
- The foundation for DoD's defensive information operations posture—potential technological breakthroughs in system integrity notwithstanding—is the personnel security system. As currently constituted, the personnel security system is ill-suited to mitigate the growing risks associated with commercial software acquisition. There exists today only a hint of the aggressive, focused counter-intelligence program that is required.

Recommendations

To more thoroughly leverage the commercial sector, the Task Force recommends:

4.2.1 The Secretary of Defense should establish commercial acquisition as the modernization instrument of first resort.

The Secretary of Defense should give commercial acquisition—to include both the acquisition of commercial products and services and the use of commercial acquisition practices—*primacy and broader scope* by establishing it as the modernization instrument of first resort.

To this end, the Secretary of Defense should seek to meet DoD modernization needs, whenever possible, with commercial solutions (including integrated services, systems, subsystems, components and building-block technologies) acquired using commercial

acquisition practices. The Secretary should grant waivers only when program managers can demonstrate that either no commercial options exist or that available commercial options cannot meet all critical performance requirements. Commercial acquisition practices should be employed in all cases. In establishing and advocating this new approach, the Secretary should enlist the support of the "Commercial Acquisition Gold Teams" established by the USD(A&T), as described in recommendation 4.2.2 below.

The Task Force recognizes that many integrated, military-specific systems are not and will likely never be provided by the commercial sector. However, military-specific systems (e.g., attack submarines, fighter aircraft and precision-guided munitions) are composed of increasingly higher percentages of commercially developed components and subsystems. For these systems DoD should meet, whenever possible, its needs with commercial components and subsystems. DoD can and should tap the commercial market to support virtually all of its modernization requirements.

By adopting commercial buying practices across the board, DoD will progressively erode both commercial sector disincentives to doing business with DoD and also the reluctance of DoD developers to engage the commercial sector. In so doing, DoD will necessarily be expanding its mainstream supplier base to include the commercial, and thus global, industry sector. The aim is not for DoD to buy commercially always, but rather for DoD to be able to choose freely, from the widest possible range of sources, for truly optimal solutions to its requirements.

The Task Force recognizes that full compliance with the policy recommended herein is most unlikely, particularly early on. That said, the rate of compliance will increase over time as DoD developers gain greater familiarity and comfort with commercial sector technologies and business practices, and as Task Force-recommended commercial acquisition advocacy activities gain momentum. In any case, such a policy does not require full compliance to be successful. Indeed, inasmuch as trimming a single day off of a system's acquisition cycle or saving a single tax dollar on a system's acquisition cost can be considered a net improvement, the nation is well-served even by partial compliance.

4.2.2 The USD(A&T) should form and employ Commercial Acquisition "Gold Teams".

The USD(A&T) should form and routinely employ "Commercial Acquisition Gold Teams" to provide and manage advocacy for expanded DoD leverage of the commercial sector, from exploiting traditional commercial off-the-shelf products to stimulating the commercial sector (e.g., via early DoD involvement in commercial sector technology/product development) and adapting DoD requirements to commercially-available solutions.

The Task Force believes that Gold Teams should be employed during the earliest stages of the acquisition process (the concept definition phase), where they will have the best opportunity to reduce both the time and cost of developing and fielding new systems. Such teams are to be used when the USD(A&T) or a Service Acquisition Executive

makes an initial determination that program requirements could potentially be met through the integration of commercial technologies, products, services, and/or processes (as contrasted with a traditional DoD development).

The organizational character and composition of the Commercial Acquisition Gold Teams are best determined by the USD (A&T). Teams could be either standing or ad hoc in character. Personnel could be either in-house (i.e., DoD), drawn from the contractor/FFRDC community, or a mix of the two. The Task Force saw no compelling need to recommend a particular composition.

Gold Teams should be focused initially on the commercial industry sectors from which the Task Force believes DoD can derive immediate and profound benefit: (1) air and sea transportation, (2) logistics and sustainment, (3) communications and information systems, (4) space-based surveillance, and (5) high-efficiency ground transportation.

The development and acquisition of the Army's Mobile Subscriber Equipment (MSE) tactical communications system is a good example of where a Commercial Acquisition Gold Team would have proven highly useful. Absent such a Gold Team, the Under Secretary of the Army, the Under Secretary of Defense for Research and Engineering and the program management staff together needed to relentlessly push the Army's requirements and developmental organizations to seriously consider, and then actually develop and field, what essentially amounted to a non-developmental system (MSE was based on an existing French design). The objective was met, but meeting it demanded a much higher level of effort on behalf of senior acquisition officials than would have been required if a Gold Team had been available.

The Task Force believes that Commercial Acquisition Gold Teams will further strengthen existing DoD policy emphasizing the exploitation of the commercial sector's capabilities, services, systems and technology. The Task Force does not envision Gold Teams to competing with, much less replacing, Service developers. The latter would be expected to take the lead once concepts have been defined and joined with technologies, and a development path has been selected.

4.2.3 The USD(A&T) and Service Acquisition Executives should proactively engage in commercial standards management.

The USD(A&T) and the Service Acquisition Executives should expand existing standards management activities (created as part of acquisition reform) to include those used for commercial products and services identified by the Commercial Acquisition Gold Teams described in Recommendation 4.2.2 above.

In general, DoD has been wise in its choice to *use* industry-set commercial standards to the greatest extent possible. At the same time, DoD must collaborate with industry to *set* standards when both DoD performance requirements demand it and when DoD is prepared to invest substantial resources in defining the standards. When both conditions are met (the Task Force recognizes that such situations are more the exception than the rule), DoD should seek to take the lead in setting commercial standards.

One example is the development of radiation-hardened integrated circuits, a nascent component of the overall commercial integrated circuit sector. So-called "rad-hard" chips, required for most of DoD's space-based systems, are of increasing utility to the commercial space industry, where concerns about system survivability are mounting. As radiation-harden chip technology matures and becomes less costly, commercial demand (and thus investment) is likely to increase. However, as the principal investor in rad-hard chips, DoD can and does shape commercial standards.

Other areas where DoD is currently able to influence commercial standards and is likely to continue doing so for some time include: high temperature/high strength materials for high-performance propulsion; microelectromechanical systems, or MEMS; and critical sensor components.

4.2.4 DoD should conduct a comprehensive review of the Federal Acquisition Regulations and Defense Federal Acquisition Regulations Supplement with the specific intent of identifying changes to regulations and statutes that would eliminate 1) barriers to DoD procurement of commercial (domestic and foreign) products and services, and 2) commercial sector disincentives for doing business with DoD.

The Task Force recognizes that there have been previous reviews focused on acquisition reform and streamlining. However, a detailed review focused on statutory and regulatory change that could enhance DoD's ability to access the commercial market is warranted.

The Task Force recommends that, as a first priority, DoD consider the following statutes for modification or repeal, and that the Secretary of Defense provide the Congress with a formal request to that effect:

- *Cost Accounting Standards (CAS).* The government should move strongly toward the objective of price-based contracting rather than cost-based contracting for all contracts, as recommended in the multi-phased (1994-1999) DSB task force on Acquisition Reform. This should be the paramount objective and, of itself, would simplify the process, without any significant risk to the government. The government needs rules to govern how costs are allocated to cost reimbursement contracts in order to prevent abuses of this contract type. The current restrictions included in the CAS statute are significant, and CAS is one of the most onerous barriers to commercial firms desiring to do business with DoD. The Task Force notes that the Department of Defense has submitted legislative changes to reduce the burden associated with CAS requirements, including triggering the applicability of CAS only by receipt of a contract of $7.5 million or more and increasing the current $25 million full coverage threshold to $50 million. This change would eliminate CAS requirements for 46 percent of business segments that are currently covered. In addition, the Department of Defense has proposed that Federal agencies be provided CAS waiver authority, and that price-based contracts be exempt from CAS.

- *Truth in Negotiation Act.* While this statute is well intentioned, its requirement for certified cost or pricing data represents a burden on industry, particularly commercial and foreign firms, which, in many cases, does not yield commensurate benefit. A modification to permit waivers by the Contracting Officer, when pricing data are deemed sufficient to permit a sound business decision, would be preferable to the current requirement for waivers by the Head of the Procuring Agency only in "exceptional circumstances."
- *Federal Acquisition Streamlining Act.* This Act exempts purchases ("micro-purchases") of up to $2,500 ($2,000 in the case of construction) from statutes requiring implementation through a contract. As a result, micro-purchases for needed commercial items can be made directly by government customers, without having to go through a purchasing office, using the government-wide purchasing card. Raising the micro-purchases that could be made to $10,000 would increase the universe of purchases that could be made using the purchase card, thereby further lowering administrative costs for low-dollar transactions and ensuring the timely receipt of goods and services by government customers.
- *Service Contract Act and Davis Bacon Act.* These statutes provide for government contract minimum wages higher than the prevailing local wage rates. The result is a disincentive for commercial companies to work on government contracts that would require a higher than commercial wage rate. The Task Force recommends that DoD request repeal of the Service Contract and Davis Bacon Acts.
- *Berry Amendment.* This amendment restricts DoD to U.S. sources for a number of commodities and products. The product list is constituency-based and in general does not relate to U.S. security interests. Broader waiver authority such as that recently proposed in the Senate would reduce these restrictions on purchases of globally available products.

4.2.5 DoD should field Web-based interactive FAR/DFARS tutorial and compliance software for commercial firms.

The sheer volume of FAR/DFARS regulations and their great complexity serve as daunting obstacles to both international and U.S. firms that could offer commercial or military dual use products to DoD. This applies particularly to small businesses with limited ability to absorb the overhead currently associated with insuring contract compliance. To help mitigate this barrier to commercial participation in DoD procurements, the Department should field on the World Wide Web interactive "distance-learning" software that would allow commercial firms to quickly familiarize themselves with the FAR/DFARS; rapidly determine which regulations apply to their specific contracts; and comply fully with those regulations.

To mitigate the risks associated with commercial software acquisition and the related information operations threat:

4.2.6 The Secretary of Defense should affirm the Assistant Secretary of Defense (C3I) as responsible for ensuring the pre-operational integrity of essential software-intensive systems.

Subsequently, the ASD(C3I) should develop and promulgate an Essential System Software Assurance Program that specifies roles and responsibilities for the following tasks:

- Identify a champion—a point organization for software acquisition review, which will promote the purchase of commercial software, while reviewing and monitoring its security vulnerabilities.
- Update guidance—delineate the responsibility of acquisition program managers and delegate to them proportional authorities; and declare system integrity a Key Performance Parameter (KPP) unless removed by exception.
- Consider more costly "clean room" acquisition of certain essential systems or subsystems, and/or take other steps to raise the bar to would-be saboteurs, such as:
  - secrecy/sterility in essential systems acquisition;
  - strenuous acceptance testing that includes red-teaming; and
  - mix-and-match components from alternate supply sources.
- Introduce "red-teaming" and independent vulnerability analysis procedures into the acquisition process for all essential systems.
- Develop specifications and guidelines for the certification of software trustworthiness at a set of pre-defined levels. This could be done through the National Infrastructure Assurance Partnership (NIAP) or through the Software Engineering Institute.
- Sponsor research at the Defense Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology (NIST) on the following:
  - trust certification and management in software;
  - software design methodology;
  - proof of software correctness;
  - taxonomy of vulnerability; and
  - smart (if non-exhaustive) testing.
- Consider using public (hacker) testing to test the resilience of algorithms, code, and systems.
- Identify unambiguously that point in the process where the operator of a system shall assume responsibility for its integrity throughout its operational life.

4.2.7 The Secretary of Defense should (1) reaffirm the responsibility of essential system operators to ensure the integrity of those systems throughout their operational life, and (2) assign to the OASD (C3I) Defense Information Assurance Program (DIAP) office the tasks of monitoring and establishing incentives to ensure operator compliance, and of overseeing the administration of the resources required for this purpose.

The OASD(C3I) DIAP office should be upgraded (in terms of personnel, equipment and funding) and assigned the full responsibility of overseeing program office/operator identification, programming and execution of the required resources, and submitting a consolidated information assurance budget. In turn, the operators should:

- Ensure that intrusion and anomaly detection systems are in place, current, and operating at peak efficiency.
- Ensure that sufficient excess capacity is available to counter expected denial-of-service attacks, and/or that other measures are taken to improve recovery and reconstitution of essential systems.
- Ensure that systems originally intended as independent backups are still independent given changes in technology and threat. Use of dedicated "red-team" and vulnerability-analysis forces are recommended.
- Ensure adequate configuration control of essential systems.
- Deny unauthorized access—using physical, technical and personnel security measures.

4.2.8 The Director of the National Security Agency (DIRNSA), as head of the NSA's Information Systems Security Organization, should:

- Program for expanded red-team and vulnerability-assessment capabilities as required without affecting the cryptologic mission.
- Advise and support established Service training functions to ensure currency and technical excellence in their training for systems administration and other key skills.

4.2.9 The Services, in accordance with their Title X authorities, should:

- Review and revise accordingly the personnel specialty designators and compensation to ensure a sufficiently staffed, trained, and motivated workforce to meet the challenge of sanitary acquisition and operation of essential systems.
- Focus and enhance security and counter-intelligence functions to deal with the new challenges presented by relying, for essential systems, on commercially purchased systems and subsystems of foreign manufacture.

4.2.10 The Assistant Secretary of Defense (C3I) and the Deputy Director of Central Intelligence for Community Management should be tasked to work together to:

- improve collection and reporting on hostile capabilities and intentions regarding computer and computer network attacks; and
- establish an aggressive, focused counterintelligence program to ensure the integrity of essential U.S. systems.

4.3 GLOBALIZATION OF THE U.S. DEFENSE SECTOR

Findings

- Globalization of the U.S. defense sector—and transatlantic defense industrial integration in particular—has myriad potential benefits for DoD, including:
  - increased access to offshore technology, capital and skilled labor;
  - increased industrial competition (helping to drive down costs and spark innovation);
  - increased pace of modernization through developmental burden-sharing;
  - enhanced U.S.-European interoperability and the narrowing of the U.S.-European technological gap;
  - a strengthened NATO industrial underpinning;
  - a coalescing of NATO political-military interests via mutual industrial dependency; and
  - the avoidance of protectionist, arch-competitive "Fortress Europe-Fortress America" defense trade blocs that could serve to widen the U.S.-European military-technological gap and weaken overall NATO integrity.
- These benefits outweigh the risks most commonly associated with cross-border defense industrial integration (unintended transfer or re-transfer of classified or export-controlled U.S. military technology and products) which can likely be managed through existing, if somewhat modified, risk-mitigation policies and procedures.
- Furthermore, while the U.S. must be prepared to act unilaterally, coalition action is preferred and thus likely in most scenarios. Accordingly, DoD must lay the foundation for effective coalition operations, which require a strong transatlantic defense industrial foundation and well-equipped allies (particularly our European partners) with whom we are militarily interoperable.
- Accordingly, DoD should not oppose mergers and acquisitions and other forms of integration and/or collaboration involving U.S. defense firms and firms from allied and/or friendly countries, so long as security and competition are maintained and there exist no compelling reasons for denial (e.g., if the proposed transaction could potentially result in unacceptable foreign governmental control or influence).
- A range of factors are inhibiting foreign industrial interest in the U.S. defense sector:
  - DoD policy on cross-border defense industrial mergers and acquisitions is not sufficiently understood by defense industry actors on both sides of the Atlantic.
  - ITAR technology transfer and re-transfer regulations are often perceived by potential foreign investors as too restrictive, and the defense export licensing process too sluggish, for effective transnational operations.
  - FOCI regulations and requirements are laborious for and disadvantageous to FOCI firms.
  - Time limits within the CFIUS (Committee on Foreign Investment in the U.S.) review process can potentially delay approval decisions on proposed foreign

direct investments (FDI) when timing is critical to the financial viability of the transaction.

- Left unattended, the existing regulatory structures will offer a robust set of barriers to effective globalization of the U.S. defense sector. The degree to which DoD is able to achieve the potential benefits of globalization is dependent on the ability of the U.S. Government to adapt defense product market and foreign direct investment regulatory structures to changing circumstances.

Recommendations

4.3.1 DoD should publicly reaffirm, on a recurring basis, its position on cross-border defense industrial linkages.

The Department has, in practice, increased its flexibility in allowing enhanced cross-border defense industrial collaboration on a case-by-case basis. It should now publicly reaffirm, on a recurring basis, its willingness to consider a range of cross-border defense industry linkages (from mergers to joint ventures to teaming) that enhance U.S. security, interoperability with potential coalition partners, and competition in defense markets. Special attention should be paid to illuminating, to the extent practicable, DoD's broad criteria for merger and acquisition approval, and DoD's policy rationale (e.g., the national security benefits of cross-border defense consolidation). The aim here would not be to *eliminate* uncertainty; indeed, it can be argued that DoD should retain a small measure of policy ambiguity so as to ensure the greatest amount of case-by-case decision-making flexibility. Rather, the purpose is to minimize the potential inhibition of beneficial cross-border merger and acquisition activity in the absence of a clearer policy.

4.3.2 The Deputy Secretary of Defense should establish and chair a standing Transnational Defense Industrial Consolidation Policy Oversight Committee.

By establishing the recommended committee, DoD can: improve coordination of transnational consolidation policy development and implementation; facilitate rapid DoD response to emerging transnational consolidation-related developments; and ensure that this policy area receives appropriate senior-level attention. To ensure both continuity of DoD policy in this area and that the committee has the requisite expertise and decision-making authority, committee membership should include senior-level representatives from those OSD and Military Department offices (e.g., USD(A&T) and DUSD(Industrial Affairs) whose portfolios already include transnational defense industrial issues.

4.3.3 The Departments of State and Defense should modernize the regulatory and administrative processes associated with the export of U.S. defense products and services and defense technology transfer to facilitate (1) the effective export of defense products/services (consistent with statutory foreign policy obligations) and (2) transnational—particularly transatlantic—defense industrial collaboration/integration.

The Task Force's modernization proposals are detailed in **Annex I,** ***Recommendation 4.3.3—Proposals for Modernizing U.S. Government Regulatory and Administrative Processes Associated with the Export of U.S. Defense Products and Services and with the International Transfer of U.S. Defense Technology***, pp. 55-68.

4.3.4 DoD should modernize the administrative and regulatory processes associated with foreign direct investment (FDI) to facilitate FDI in the U.S. defense sector.

The Task Force's modernization proposals are detailed in **Annex II,** ***Recommendation 4.3.4—Proposals for Modernizing the Administrative and Regulatory Processes Associated with Foreign Direct Investment (FDI) to Facilitate FDI in the U.S. Defense Sector***, pp. 69-74.

4.3.5 Where possible, DoD should adapt existing bilateral security arrangements to address the emergence of multinational foreign defense industrial organizations.

The change in the structure of the defense industry raises a question about whether the existing mitigation practices are appropriate to its inevitable globalization. A likely consequence of globalization is the creation of cross-border defense industrial organizations that include entities in several national jurisdictions. European political integration seeks to blur or eliminate the political and regulatory significance of national boundaries as scope of national sovereignty shrinks. These developments are likely to affect regulatory practices among U.S. allies, increasing the importance of "European" institutions and practices, and reducing the impact of national practices. For example, European (i.e., EU) labor market regulations combined with cross-border mergers, acquisitions, and joint ventures inevitably cause the European work force to be more mobile and largely independent of national regulation. The multinational career path of executives and employees in the defense industrial sector is also likely to make it difficult to manage a global industrial security program in the same manner as has been done in the past. A program built entirely around traditional concepts of companies formally domiciled in nations whose legal and regulatory practices are well understood may no longer suffice. DoD will likely need to refocus its security priorities and practices in order to obtain the benefits of two-way cross border foreign direct investment while mitigating its risks. Domicile may be of diminished regulatory significance in Europe, and hence for U.S. security processes based on domicile.

Separating unauthorized users from controlled technology in a multinational firm is a significant management challenge. These problems are likely to be magnified when the management of multinational defense industrial firms itself becomes multinational. Precedent suggests, however, that security arrangements made on a bilateral basis can be extended into multilateral entities. U.S. experience in the management of SSA/FOCI firms, and UK experience with the management of "UK Eyes Only" information in a multilateral enterprise suggest the practicality of future multilateral security arrangements. The ongoing fundamental review of NATO security procedures may contribute to a more detailed harmonization of security procedures. This in turn could be

helpful in adapting NATO's industrial security infrastructure to the globalization of the supplier base of the alliance.

The U.S. Government has developed a set of institutional practices and diplomatic instruments to facilitate the sharing of classified information with friendly nations abroad. The protection of export-controlled information is managed through the export licensing system, is program-specific rather than a product of general government-to-government agreement(s), and deals primarily with end-use and retransfer matters, rather than information security. Security arrangements designed to protect classified information are almost entirely of a bilateral character and are general in nature. The U.S. Government has created a *de facto* international regime for the protection of classified information from a series of bilateral agreements. These agreements include the General Security of Military Information Agreements (GSOMIA) and the Industrial Security Agreement which normally is an annex or implementing protocol to the GSOMIA. Data Exchange Agreements (DEA), and various bilateral defense industrial and R&D agreements such as Reciprocal Procurement Memoranda of Understanding (MOUs) also contain security provisions.

From a security perspective, these agreements place the responsibility for the protection of classified or export-controlled information and equipment in the hands of friendly governments who have agreed to do so, and have the resources in place to implement those commitments. While it may be impractical to expand the scope of bilateral GSOMIAs to all circumstances relating to international cooperation on a multilateral basis, GSOMIA enhancements and improved procedures within NATO may make it easier to implement program-specific security arrangements on a multilateral basis. Precedent exists for work on a single project by nationals from several countries (e.g. NADGE, MLRS, MEADS, etc.), suggesting that security can be managed despite differing security practices and bilateral GSOMIAs. It may be easier to negotiate an amendment to bilateral GSOMIAs to take into account national participation (whether on a government-to-government basis or a commercial basis between defense industrial firms) in multinational collaborative projects than to attempt to do so on a project-by-project basis. The objective of such GSOMIA enhancements is to assure an unbroken chain of compliance by firms subject to security requirements as the firms regulated by the arrangements participate in multilateral business entities.

4.4 PERSONNEL SECURITY

Findings

- Personnel security is the foundation upon which all other safeguards must rest. New global information technologies create greater vulnerabilities, and there continues to be a real and systemic threat that cleared U.S. Government personnel will violate the trust that has been placed in them.

- The Task Force is convinced that far more information than necessary is classified Secret or Top Secret by the Original Classification Authorities. As a result, the DoD personnel security program is forced to sweep too broadly and is consequently spread thin. Over-classification also leads to an over-allocation of DoD security resources to the protection of classified information at a time when greater resources must be devoted to developing new types of security measures tailored to the challenges created by global information technology. DoD should make a serious commitment to developing a coordinated analytic framework to serve as the basis for classifying information, and implementing that framework rigorously.

- DoD will likely never be able to assure that all military, government and industrial personnel with access to sensitive information or equipment are trustworthy and reliable. Realistically, the security investigative and screening process can do little more than identify individuals with criminal records or other conspicuously irresponsible conduct. For too long, however, government employees and organizations alike have acted as though the granting of a security clearance eliminated the need to remain vigilant or assume responsibility for the conduct of subordinates and colleagues. In short, unrealistic expectations of the clearance process have undermined, albeit unintentionally, the very alertness, accountability and situational awareness that are increasingly necessary to provide security in a networked world.

- Few of the many U.S. citizens who have betrayed their country over the last 50 years entered government service with the intent to commit espionage. People and their circumstances change through time. Thus, while a background investigation may provide solid information regarding an individual's past, it can never reliably predict future conduct. Nor should we expect it to; there is a limited life history and range of experience on which to base a judgment. Inevitably, some public servants will during the course of their careers see their marriages fail, develop a dependence on drugs or alcohol, overextend themselves financially, become disgruntled employees, etc. Of these, only very small percentages—yet still too many in absolute terms—become serious security risks. The five to 10 years between clearance reinvestigations is far too long to wait to detect such developments.

- In the dynamic, networked environment created by global information technology, DoD needs to develop an enhanced situational awareness approach to personnel security that takes account of new vulnerabilities, threats, and response requirements. Many new technologies hold the seeds of effective defensive options. For example, DoD is currently exploring the near real-time data mining of financial and foreign

travel databases, as well as the detection of computer misuse, to be used in concert with other contextual leads. Increased use of information technology can also assist in implementing more effective access controls, automated monitoring and audit capabilities, and stronger identification and authentication of users as well as encryption of data. Taken in concert with a policy of compartmentation, these measures can represent an effective response designed to counter the threat posed by both insiders and outsiders with malicious intent.

- Compartmentation is a valuable instrument in making security work better. DoD should place a premium on protecting information that is properly determined to require control in codeword compartments. New initiatives are underway to move away from the rigid security clearance model in providing personnel security for compartmented programs. These include aperiodic polygraph examinations (rather than a predictable reinvestigation timetable of five-year intervals or longer) and a requirement for self-reporting of changes in the standard security clearance elements as part of annual security awareness training. Emerging electronic access control technology can enable data owners to establish "communities of interest" on a network to enforce need-to-know for access to a particular website. To work properly, program and project managers will have to ask what is essentially a personnel security question: "Who has a need-to-know or a need-for-access?".

- No single set of personnel security countermeasures will suffice. In addressing the insider threat to information systems, DoD must achieve a complementary mix of technical, procedural, human resources management and traditional personnel security measures. DoD must also abandon the inefficient, one-size-fits-all approach to security. For example, DoD often devotes the same investigative resources to a factory worker as to a research engineer with multiple clearances—clearly a sub-optimal allocation of scarce resources. Also needed is an appropriate security program for government and defense industry personnel who occupy "sensitive but unclassified" information technology positions (e.g., those critical for protecting information systems from hostile disruption or manipulation via the global information infrastructure). In this area, monitoring on-the-job performance in critical information technology positions may be more important than full field background investigations.

- In short, although the clearance process provides a vital filter that weeds out individuals with checkered pasts—thus providing a measure of deterrence throughout an individual's career—DoD must increase emphasis on security policies and procedures in the workplace. Personnel security measures should be based on solid, objective research that looks for meaningful measures of effectiveness and improved approaches to evaluating trustworthiness.

Recommendations

4.4.1 DoD should adapt its personnel security system to the new global information technology environment by streamlining the security classification and clearance processes; ensuring that classifications are

justified to mitigate the problem of over-classification; and moving away from a rigid clearance structure.

4.4.2 **DoD should compartmentalize the most sensitive information and activities by employing web-based need-to-know technology, restoring the "need to know" principle for classified data stored on electronic systems (taking advantage of security, privacy and intellectual property rights management developments in the commercial sector), and maintaining access control on electronic systems (to include better authentication and control of disk drives and portable electronic media).**

4.4.3 **DoD should institute a situational awareness approach to personnel security that combines technical monitoring and human resources management tailored to the positions that offer the greatest risks and vulnerabilities.**

In particular DoD should:

- undertake near real-time data mining of financial and foreign travel databases and detection of computer misuse for use in concert with other contextual leads to monitor cleared personnel;
- develop and acquire the tools required to undertake real-time data mining analysis;
- monitor security performance and establish performance incentives; and
- make line managers accountable for security in their organizations.

4.4.4 **DoD should develop a new situational awareness program for DoD information technology personnel.**

Implementation of the situational awareness model for sensitive information technology positions requires innovative management approaches within the established structure of the Office of the Secretary of Defense. An appropriate personnel security program for information technology positions requires the authority and expertise of the security *and* personnel elements of the principal DoD components.

4.4.5 **DoD and the intelligence community should work together to develop more effective situational awareness measures to address the insider threat at the classified level, making greater use of outside research and independent threat/vulnerability evaluation.**

Annex I

Recommendation 4.3.3

Proposals for Modernizing U.S. Government Regulatory and Administrative Processes Associated with the Export of U.S. Defense Products and Services and the International Transfer of U.S. Defense Technology

Introduction

Globalization is a fact, not an alternative for DoD modernization. Nevertheless, the degree to which DoD is able to achieve the potential benefits of globalization is dependent on the ability of the U.S. Government regulatory apparatus to adapt to changing circumstances. The twin imperatives of accessing advanced technology on a global scale, and preserving the security of the tactical and strategic military advantages the technology provides require judicious, and perhaps Solomonic decisions. Left unattended, the existing regulatory structures will offer a robust set of barriers to effective DoD exploitation of globalization. Therefore, the U.S. Government must undertake a complete and systematic reform of the process by which it regulates U.S.-foreign defense industrial collaboration and the export of U.S. defense technology, products and services, namely, the International Traffic in Arms Regulations.

A complete ITAR overhaul would constitute a challenge of enormous proportions and likely take several years to complete and implement. The Task Force felt that near-term progress was both vital and achievable through a more targeted approach. Accordingly, the Task Force analyzed the ITAR for flexibility that might permit specific changes that could be made relatively quickly and easily and that would promote greater export licensing efficiency and international cooperation over the near term. The proposals discussed in detail here reflect implementation opportunities that can be made promptly. A more thoroughgoing set of proposals may require statutory change to facilitate DoD's ability to recognize and implement changes in its processes to accommodate the globalization of the defense market, supplier base, and ownership likely to emerge over the next decade.

The following recommendations fall into five basic categories: policy decision making, personnel, security, Department of State regulations, and technological improvements. Most of the recommendations focus on Department of State export control regulations for U.S. Munitions List (USML) items. The changes described here are not listed in any particular order of importance.

4.3.3.1 Modernize munitions licensing career management practices in the Department of State's Office of Defense Trade Controls (DTC).

The effectiveness of the Department of State in the implementation of its statutory responsibilities is adversely affected by anomalies in its career management process.

Changes are needed at the Office of Defense Trade Controls (DTC) such that those employees who work with skill and dedication are rewarded with career advancement opportunities that will permit their retention within DTC. Such changes are needed to reflect the importance of the function to U.S. foreign and defense policy. Modernization of career management practices includes the establishment of a civil service grade structure comparable to other U.S. Government agencies involved in the export licensing process. A failure to make such adjustments has created disincentives to long-term career development within DTC as experienced DTC personnel take advantages of employment opportunities in other agencies with more advantageous career path and grade advancement.

4.3.3.2 Establish a single authority in DoD for arms transfer decisions.

There are numerous participants within DoD in the arms transfer and arms cooperation arena, often with competing and in some cases, divergent interests. There should be a single DoD office responsible for policy decisions on commercial as well as government-to-government (FMS) arms transfers as well as cooperative arms programs. This office should have a direct channel to the Deputy Secretary or Secretary of Defense since arms transfer policy decisions often involve highly sensitive matters of national security policy.

4.3.3.3 Liberalize ITAR spare parts exemption for NATO countries.

Liberalization of the exemption [(ITAR 123.16(b)(2)] will diminish a licensing burden on both the Department of State and exporters with little value-added to U.S. security or foreign policy interests. Raising the existing limitation for NATO government buyers and for NATO country firms reflects a reasonable balance between the need of the U.S. Government to control the export of spare parts and the managerial burden of licensing.

4.3.3.4 Modify ITAR implementation to facilitate cross-border collaborative relationships.

The ITAR serve two purposes. They provide a regulatory regime to facilitate U.S. Government decisions concerning the foreign policy basis for providing military capabilities to foreign governments. The ITAR also serve national defense purposes as well by protecting the technological lead enjoyed by U.S. military forces. This function is a useful, but is now a diminishing contributor to the larger strategy of protecting U.S. military dominance. Nevertheless, where foreign policy considerations permit, modernization of technology transfer arrangements through the ITAR can be used as an instrument to draw the transatlantic alliance closer together in both political and military terms. The post-Cold War divergence between the U.S. and European defense industrial culture is driving a damaging wedge in transatlantic defense cooperation. The divergence created by differing approaches to defense modernization threatens to undermine the coherence of the alliance at the political level, and exposes it to the risk of a diminished ability for NATO forces to interoperate in coalition operations.

The ITAR reflect a buyer-seller orientation. This was appropriate when most arms transfers were implemented on a government-to-government basis, and the U.S. enjoyed a very substantial lead in military-unique applications of modern technology. Globalization is having a leveling effect on the distribution of advanced technology in a manner that now enables many nations to produce technologies pertinent to U.S. national defense. Creation of a "regulatory compartment" within the ITAR to facilitate collaborative arms development activities could be implemented with only modest regulatory reform. Such a "compartment" would consist of a set of regulations that could be implemented *en bloc* when a collaborative rather than a traditional buyer-seller transaction emerges. This "compartment" could include provisions for the selective use of ITAR exemptions as a vehicle to facilitate collaborative arrangements. Existing National Disclosure Policy Committee decision authorization channels, with decision authority vested in Designated Authorities at various command levels could be used to speed up decisions where government intervention is necessary rather than referring cases to DTC (State) or DTRA/DTSA (DoD). These officials already make such decisions on FMS programs, and should do so on commercial programs as well. The use of the ITAR exemption [ITAR 125.4b(11)] permitting industry involvement without a license when involved in a government program under and international agreement is one example where such an approach is appropriate.

With regard to the ITAR exemptions, several are particularly appropriate to facilitate industry involvement in cooperative initiatives. Exemptions 125.4(b)1 and 125.4(b)11 are suited to those situations in which industry participation is in support of government initiatives as well as for hybrid initiatives involving government and commercial sales. Exemption 124.4(b)11 could be streamlined so that disclosure or export decisions after the signing of an agreement could be made by the Designated Disclosure Authorities as discussed above. The exemption for FMS sales (Part 126.6 of the ITAR) is another that could be easily be exploited by reducing the unnecessary paperwork. The Department of State and DoD should pursue the development of procedural guidance that will assist government and industry in making full use of these exemptions.

4.2.3.5 Improve flexibility of DoD International agreements.

Authority exists in the ITAR to significantly improve the flexibility of DoD international agreements. The DoD does not exploit existing waiver authority in the ITAR to diminish processing time and complexity for participants in international programs. The current ITAR contains an exemption under Part 125.4(b)(11) to provide for the export of technical data, including classified information (but not hardware) for which the U.S. exporter, pursuant to a arrangement with DoD (and other Executive Departments) has been granted an exemption from the Office of Defense Trade Controls in writing from the licensing provisions of the ITAR.

The exemption is granted only if the arrangement directly implements an international agreement to which the U.S. Government is a party and multiple exports are contemplated. The DTC, in consultation with the relevant U.S. Government agencies, will determine whether the interests of the U.S. Government are best served by

expediting exports under arrangements through an exemption. This proposal could be implemented through rationalization with ITAR Part 125.4(b)(3) for which additional licensing for technical data is not required.

As a part of the process to establish an international agreement, DoD will already have in place a Designated Delegation of Authority Letter (DDL), appropriate technology transfer plans, and have addressed the Congressional notification requirements (Section 36 of the AECA), and have co-developed program guidelines with the Department of State. To take advantage of this broader exemption, industry must develop robust compliance programs subject to DoD or Department of State audit, and file annual reports. These annual reports could be managed by the appropriate acquisition offices in each Military Department using a standard DoD-wide format.

Developing policies and guidelines to identify and implement this exemption in support of DoD designated international agreements would significantly expedite the export process, reduce the number of export license issued by DTC for technical data, and enhance the cooperative relationship between the U.S. and its allies.

4.3.3.6 Establish more uniform requirements for the drafting of agreements.

The manner in which Technology Assistance Agreements and Manufacturing License Agreements are drafted often create delays in processing. Some applications exclude commercial items while other include all commercial, regulatory, and other terms in a single agreement that is submitted to the Department of State. The issues raised by inconsistent drafting practices are often irrelevant to licensing policy decisions, and contribute to protracted processing time.

4.3.3.7 Make greater use of industrial non-disclosure agreements to obtain required certifications of compliance of employees, partners, and other entities and individuals.

Non-disclosure agreements (NDAs) are a recognized and enforceable legal mechanism for requiring individuals to comply with legal obligations. Submission to the U.S. Government of NDAs with license applications can be a useful means of obtaining required certifications of compliance in a single procedure.

4.3.3.8 Define "inherently military" products for ITAR regulatory purposes, and add note to USML exempting piece non-inherently military piece parts.

The current ITAR 120.3 definition for designating and determining defense articles and services reaches out and controls all end items, components, accessories, attachments, parts and systems that are specifically designed, developed, configured, adapted, or modified for military application. On the surface, this decision appears simple and clear cut. However, under this definition many thousands of parts, components, accessories,

and attachments that are not inherently military in character are controlled under the ITAR. Simply designing or modifying or configuring a bracket, a fitting, a case, etc. for a military application makes that item ITAR-controlled thus requiring a license. To mitigate this problem, DoD should seek to define "inherently military" products for ITAR regulatory purposes, and to add a note to the "General" paragraph of the USML exempting non-inherently military piece parts. The latter note should read: "Miscellaneous hardware piece parts such as bolts, brackets, bushings and connectors are not USML items."

Prior to July 1993 the ITAR criteria was based "primarily on whether an article or service is deemed to be inherently military in character." No significant public policy purpose is served by licensing requirements that are so broad in scope. Moreover, in a time of limited resources, a return to licensing only those defense articles and services that are inherently military in character would make the best use of those limited resources. The Departments of Defense and State are well positioned to determine what end items, components, etc. is "inherently military" and worthy of license review rather than mechanically extending licensing requirements to content that may not be inherently military. The prospect that commercial-off-the-shelf products could under some conditions become subject to USML licensing requirements might cause suppliers of technology to abstain from offering advanced products to the Department of Defense. Such a development could inhibit the ability of the Department of Defense to exploit the advanced low-cost technologies available in the commercial market.

The increasing role of commercial products in defense subsystems and systems makes it important to develop a useful definition of commercial products and technologies. Doing so will facilitate an orderly separation of products and services that are "inherently military" or developed for military applications from those widely available and not developed for military applications.

The USML captures many standard parts and components that are not inherently military, that are non-lethal and widely available on the international market. These include mechanical, electrical, hydraulic, pneumatic, and fuel systems for land, sea, and air combat vehicles and equipment. These "utility systems" are parts and components that supply fuel, air conditioned/pressurized air, and hydraulic and electrical power to operate other equipment on air, sea, and land vehicles. Approximately fifteen percent of license applications are for utility subsystems parts and components or miscellaneous hardware. Many—perhaps most—of these items can be deleted without engaging U.S. national security or foreign policy interests.

That said, the Task Force acknowledges the dilemma caused by the virtually limitless number of items for commercial purposes that have significant military utility. Commercial communication (cellular telephones), consumer GPS products, and binoculars with laser range-finders are illustrations of devices that can have a material impact on military capabilities, especially in less developed countries. In addition, the dilemma of how to manage the deregulation of obsolescent U.S. defense goods and technology that pose no direct threat to the U.S., but may be destabilizing in some regions of the world. These are not issues of defense technology per se, but can materially affect U.S. interests in regional security and stability.

4.3.3.9 Clarify regulations regarding the scope of dual-citizenship requirements for licensing.

Dual-citizenship affects an increasingly significant fraction of a highly mobile global labor force. The impact of these changes in the labor force is reflected in non-uniform standards related to munitions licensing. Clarification of this issue will be especially important when non-U.S. defense firms, especially those with a multinational presence, participate in the U.S. defense market.

4.3.3.10 Develop processes which permit more routine use of multiple destination licenses.

Third-party arms transfers are an enduring point of reciprocal sensitivity between the U.S. Government and its allies—perhaps too much sensitivity given the fact that most U.S. defense products eventually are sold to multiple destinations. Moreover, there are numerous precedents for the authorization of multiple destination licenses in USML regulatory practice. In a recent case, a multiple destination license was issued for a jointly developed U.S.-South Korean jet training aircraft in advance of product development involving two dozen potential buyers. This decision was made with little risk to U.S. policy objectives since the destinations approved already involved F-16 users. Nevertheless, the decision to provide multiple destination licenses diminished the commercial risk of the transaction, thereby stimulating investment in a project of mutual interest to the United States and the Republic of Korea.

4.3.3.11 Establish an interagency electronic licensing system.

The Departments of State and Defense—the primary agencies involved in the ITAR export licensing process—should establish a common automated arms export licensing process. Currently the only electronic interface is a single DoD provided terminal used to provide a daily report on the position taken by the Department of Defense on cases referred to it by the Department of State for review. Major exporters have already established electronic filing of export licensing applications with the Department of State. However, the lack of an effective interagency electronic license processing system results in the inefficient consumption of scarce personnel resources and processing time. Implementation of an effective interagency electronic licensing system would significantly improve the responsiveness of the munitions licensing system to support foreign as well as defense policy purposes.

4.3.3.12 Move toward one-stop licensing reviews for collaborative projects.

A factor that discourages defense industrial collaboration with allied nations is the layered process used by the U.S. to authorize exports of munitions list equipment and services. The layered, separate authorizations required by the licensing system from

marketing licenses to manufacturing license agreements (MLAs) each have their own process, processing time, and uncertainties. Cumulatively, these circumstances have a chilling effect on collaboration. The layering of the licensing system increases the perception of program risk because approval at one stage of the process does not assure that subsequent steps will be approved, despite substantial investment by the parties. As the policy decision to authorize a specific technology, service, or equipment export involves very similar criteria, it is possible to address the full scope of licensing decisions in a single decision or very few steps. The ability to move toward single step licensing for collaborative projects could be advanced by an internal DoD process that would enable DoD and service components to conduct a one-time review of collaborative projects. Residual Department of State concerns generally relate to foreign policy concerns that change infrequently with major allies likely to be a party to collaborative development programs. By compressing the licensing process into a single, or at most, a few step(s), a substantial dimension of program risk would be mitigated. This could be accomplished without any attenuation of U.S. controls on munitions list exports for policy purposes.

4.3.3.13 Reduction in the requirement for DoD review of technical data and hardware by destination.

Evidence suggests that DoD currently reviews technical data and hardware proposed for export to destinations/end-users that pose a very low risk to U.S. national security interests. In other cases, the export of some types of technical data and hardware may pose little or risk to U.S. national security interests. Unneeded referral of license applications for DoD review where either the end user or the nature of the export (or both) poses little risk to U.S. national security interests diminishes the ability of DoD to bring attention to bear on cases requiring careful analysis. To this end, DoD should define a list of countries/end users and technical data and hardware it no longer needs to review for national security purposes. A similar effort should be undertaken by DoD for DSCA prior to the processing of Letters and Offers of Acceptance (LOAs). Narrowing the scope of license application referrals will permit most licensing decisions to be made on traditional foreign policy interest criteria such as regional stability.

4.3.3.14 Expedite the Exception to National Disclosure Policy process.

The National Disclosure Policy (NDP) process is an important dimension of U.S. arms transfer policy. This DoD-led interagency process makes policy decisions concerning the export of classified information to nations abroad acquiring U.S. defense equipment or services. This responsibility is based on both law and regulation. The Arms Export Control Act, Executive Order (EO 12958), and Presidential directive (National Security Decision Memorandum 119) jointly establish the objectives of the NDP process. A decision concerning the release of classified information frequently becomes entangled in a separate, but related process—a decision to authorize a specific arms transfer. Such a decision in turn, becomes enmeshed in the establishment of regional or country-specific export decisions. The decision process has become increasingly protracted for many "difficult" cases, and is contributing to an unnecessarily drawn out process for defense

exports. Since 1996, the processing time for an Exception to National Disclosure Policy (ENDP) has, for a difficult case, doubled from 135 to 270 calendar days. For routine cases, average ENDP case processing time during the same period grown by more than 25 percent—from 23 to 30 days. Recent reforms that focus ENDP decisions on national security concerns shows promise. Effective and sustained implementation of the reforms and compliance by member agencies with established timelines in the NDP operating procedures may significantly improve the timeliness of ENDP decisions.

National Disclosure Policy has the primary function of assuring that classified information is disclosed to foreign governments only where there is a clearly defined advantage to the United States. This assurance is achieved by the disclosure process which requires that each disclosure meet five essential criteria before the disclosure can be made: the disclosure must be consistent with U.S. foreign policy and national security objectives concerning the recipient country; the disclosure is consistent with U.S. military and security objectives; the foreign recipient will afford the information substantially the same security protection as the United States provides it; the disclosure will result in a clearly defined advantage to the United States; and the disclosure is limited to that information necessary for the purpose for which the disclosure is to be made. These functions must be given equal weight.

In addition, the problem of authorizing disclosure of classified information or approving an ENDP on commercial cases poses an increasingly frequent problem for NDP. Defense exports and defense industrial collaboration are often implemented on a direct commercial sale between exporters and foreign governments and local industry. Such transactions may include classified as well as export-controlled unclassified data. ENDP decisions on commercial sales should entail no more difficulty than would be the case with a government-to-government sale through the Foreign Military Sales (FMS) system. Nevertheless, ENDP decisions for a classified component of direct commercial sales are often subject to protracted delays. These delays may be mitigated by reforms recently put in place. A solution to this problem is inevitably part of a larger problem to improve the management and flexibility of the arms transfer process where mixed FMS and direct commercial sales are involved. A DoD element or organization (DTRA/DSCA) should be responsible for reviewing industry request for ENDPs and, if justified, assuming the responsibility for sponsoring said ENDP.

Improved DoD-industry collaboration in providing and presenting technical, security and administrative information to the NDPC should help mitigate the delays in processing an ENDP. If a timely decision involving complex foreign policy matters cannot be made under established NDPC procedures, the case could be referred immediately to the Under Secretary of Defense for Policy for review and adjudication. The Under Secretary Defense for Policy would have the option to consult with the Under Secretary of State for Arms Control and International Security in cases where significant foreign policy interests are involved. If a decision cannot be made by the Under Secretary of Defense for Policy, the case, in accordance with NDPC procedures, would be referred to the Deputy Secretary of Defense for a decision.

This process of referral to the Under Secretary of Defense for Policy could also serve as a venue for appeal of an ENDP decision by an affected agency in other than foreign policy

matters. This change to the ENDP process should assist in shortening the decision time on difficult ENDP cases and ultimately expedite the entire ENDP process.

4.3.3.15 Increase emphasis on education of officials involved in arms transfer and international cooperative arms programs.

Many government and industry personnel involved in export licensing and National Disclosure Policy decisions have spoken of inadequate training in these functions, and a lack of written guidance. This is true throughout the licensing process, but is particularly true for reviewers who receive license applications from Defense Threat Reduction Agency/Defense Technology Security Administration (DTRA/DTSA) for review. The Deputy to the Under Secretary of Defense (Policy) sponsors a course on security arrangements for international programs. The Defense Systems Management College (DSMC) presents a similar version for program managers, and the U.S. Air Force offers a course on foreign disclosure. Personnel from either DTSA or State DTC generally do not attend these courses. An increased emphasis on education could improve both DoD and U.S. Government effectiveness as the globalization process involves a wider range of defense products and services.

In the case of DTC and DTRA/DTSA officials, another form of training would be beneficial. Licensing officers need familiarization training in the capabilities, hardware, and technology they license. One potential source of such training could be in the form of periodic visits with industrial firms developing or integrating such technology. Such visits could be administered through a central clearing office to assure that opportunities to visit industrial facilities were uniformly available and provided access to a wide variety of firms. Such cooperative training with industry should provide both technical as well as business process knowledge. Similarly, licensing officers from the Department of State would benefit from training opportunities with the U.S. Customs Service to better understand this crucial dimension of the arms transfer process.

It serves the interest of an effective U.S. Government arms transfer process for both government-to-government and direct commercial sales to have a technically as well as administratively informed cadre of officers. Doing so will enable the export licensing process to be responsive to industry and government needs for timely reviews of arms transfer proposals, and to assure that transactions approved or denied serve the foreign policy interests of the United States.

4.3.3.16 Provide specific guidelines to U.S. defense industry concerning information necessary to be included in export license application to facilitate the review process.

The absence of clear guidelines concerning information required to complete processing of license applications expeditiously has resulted in many applicants submitting information that impedes rather than expedites license processing. The information required falls in seven major categories including:

- Overview of technology, system, or data

- Description of technical data including classification and source of information classification
- Purpose of the export (e.g. offset, response to a request for proposal, pursuant to a government program, etc.)
- Description of the state-of-the art of the technology proposed for export
- Foreign availability
- Licensing precedents
- Significance of the export to the exporter

Identifying common information in the required format would facilitate munitions license processing, as well as enhancing implementation of an effective interagency electronic licensing system to significantly improve overall responsiveness.

4.3.3.17 Develop umbrella license structures for major foreign firms who are recipients of U.S. munitions list equipment or technology.

The process of transatlantic industrial consolidation has resulted in a substantial increase in the number of active licenses held by major U.S. defense exporters. The concentration of the defense sector in allied nations in fewer and fewer firms similarly narrows the number of firms receiving U.S. munitions list products. As the compliance prospects of individual offshore firms in allied countries is well understood by the Department of State, an umbrella export licensing arrangement could be made that would significantly diminish the processing burden on the Department of State without adversely affecting compliance. For example, a single license for munitions list exports to British Aerospace from major U.S. exporters (e.g., Boeing, Lockheed Martin, or Raytheon) with common limitations could be offered. Compliance monitoring for the UK firm could be undertaken by the UK government—possibly affirmed through a government-to-government MOU for the purpose.

4.3.3.18 Reform the Non-Transfer and Use Certificate (DSP-83) process.

Reform of the Non-Transfer and Use Certificate process can significantly improve the management of the DSP-83 process without compromising the underlying public policy purposes of the procedure. This can be done by limiting the requirement for a DSP-83 certificate for NATO member states through a waiver process, multi-program commitments to non-retransfer provisions, or the existence of effective enforcement arrangements that render such a commitment superfluous.

4.3.3.19 Examine the options available from advanced technology to prevent or mitigate the consequences of unauthorized or inadvertent transfer of U.S. classified or export controlled technologies to unauthorized end-users.

Protecting U.S. military superiority is a serious challenge in an environment where the leveling effect of commercial technology is facilitating the rapid proliferation of advanced conventional and unconventional military capabilities. Concern about the effectiveness of export control enforcement, even by nations closely allied to the United States, remains an obstacle to effective alliance-wide defense industrial cooperation. DoD should consider sponsoring R&D initiatives designed to identify opportunities and technologies to mitigate the consequences of the transfer to unauthorized end-users of U.S. classified or export controlled technology and equipment.

4.3.3.20 Establish a consultative process within NATO to address defense trade regulatory issues.

Defense trade regulation is a significant source of tension within the alliance. U.S. technology transfer restrictions, especially the Non-transfer and Use Certificate and third country sales policies, are long-standing issues in defense industrial cooperation. U.S. Government concerns with effective allied defense trade regulation and enforcement problems sustain U.S. reluctance to transfer technology in some circumstances. The absence of a suitable bilateral or multilateral forum to address these issues has caused some governments to attempt to influence U.S. Government policy through indirect pressure on U.S. vendors. By making the sale of products by U.S. vendors conditional on changes in U.S. regulatory policy or practice, some allied governments seek to induce U.S. industry to campaign for changes in policy. A government-to-government consultative process within NATO to periodically address defense trade regulatory issues will alleviate such pressures. It will create a process for the periodic modernization of regulation to keep pace with policy objectives and regulatory needs.

4.3.3.21 Provide clear guidance on the ITAR definition of technical data to enable license applicants to know what information must be licensed for export.

Approximately fifteen percent of license applications are for data that are not export controlled. These cases impose an unnecessary burden on the export licensing system. The ITAR definition of technical data needs to be rendered more precise. Information, other than software which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles should be defined. Technical data documents: processes, instructions, procedures, methods, or techniques that explain what to do, how to do it, or why something must be done. This includes information in the form of:

- design processes, procedures, rationale, trade studies and simulations
- engineering drawings and blueprints
- test plans, procedures and reports
- quality control procedures and reports
- manufacturing specifications, processes, methods and techniques
- operations and maintenance technical orders, procedures and instructions

- software documentation including source code

Clarification of the ITAR definition of technical data would decrease the inefficient use of scarce personnel resources and processing time by decreasing unnecessary export license applications.

4.3.3.22 Narrow the focus of ITAR licensing to reflect contemporary technology trends.

The content of defense products is changing. To an increasing degree, defense products are likely to involve the integration of unclassified and uncontrolled components and subsystems. The integration process will create the military application of the uncontrolled and unclassified enabling technology. As discussed elsewhere in this report, the characteristic of arms transfers most germane to U.S. foreign policy and security interests is less involved in the enabling (commercial) technology than the capabilities created by their integration to provide a specific set of military capabilities. The enabling technologies are generally subject to extensive commercial availability. The focus of control for both foreign policy and national security purposes is the capabilities to be transferred to a specific end user or a class of end users.

The ability of the U.S. Government to make such decisions would be facilitated by a sharper and more narrow focus for the crucial elements of arms transfers—the capabilities placed in the hands of users abroad. By focusing licensing decisions on Significant Military Equipment (SME) and classified equipment/data, the licensing system could focus on critical elements. Less critical elements involving commercial or widely distributed munitions list technology could be left to a notification process (while retaining existing requirements concerning retransfer). By distinguishing between SME and non-SME and destinations where unclassified and non-SME have previously been sold to responsible end-users, it may be feasible to develop a licensing approach that can make use of a notification system or similar approaches that will diminish the need for repetitive case reviews of routine USML exports of spare parts. Such changes could be made in a manner that limited risk of the diversion of stocks of spare parts to unauthorized end-users.

Category	Authorization procedure
Significant Military Equipment	Export license required
Classified equipment or data (SME and non-SME)	Export license required
Non-SME unclassified ITAR controlled equipment/data not previously approved for export	Export license required
Non-SME unclassified ITAR controlled equipment/data previously approved for export	New procedures

The aspirations contained in this proposal recognize the enduring interest of the U.S. Government in the management of arms transfers as an instrument of foreign policy. However, the proposal also seeks to modernize the implementation of ITAR in a manner that reflects the changing character of defense-related technology. Eliminating traditional munitions licensing requirements for unclassified non-SME in favor of a notification requirement reflects a compromise over the duality of this kind of technology. This approach would not require abandoning other U.S. Government controls on USML exports imposed for foreign policy or other national purposes. The notification system could be implemented without loss of oversight by maintaining a list by country of certified end-users and end-uses. The munitions licensing system is complex with numerous policy and regulatory considerations that must be taken into account. These issues will be the subject of additional study.

4.3.3.23 Provide adequate resources to support a munitions licensing system that will provide timely and effective controls on USML exports whose control is essential to protecting U.S. national security and foreign policy interests.

The protracted period of time required for some license processing is not always a consequence of resource shortfalls, but resources are an important explanatory variable. Adequate numbers of trained personnel are important. So to are the number of military officers detailed to serve in the Office of Defense Trade Controls in the Department of State whose expertise can contribute substantially to compressing the time required for license application review. Sufficient resources to monitor and evaluate trials of new licensing concepts or processes can also speed the modernization of the munitions licensing system.

Annex II

Recommendation 4.3.4

Proposals for Modernizing the Administrative and Regulatory Processes Associated with Foreign Direct Investment (FDI) to Facilitate FDI in the U.S. Defense Sector

Introduction

Foreign direct investment (FDI) is the least developed dimension of globalization in the defense sector. This reflects the substantial regulatory barriers to FDI in the past. Since the 1980s, these barriers have been gradually diminished, although significant obstacles remain to routine foreign investment in the U.S. defense sector. FDI offers a number of benefits to DoD. FDI brings new resources—human, material, and financial—to the U.S. defense market. In doing so, foreign participants in the U.S. market can contribute to the pool of technical innovation available to DoD, while strengthening competition in the defense market. Risk negation or mitigation remains a crucial aspect of FDI in the United States. The compliance record of FOCI firms in the U.S. suggests that the incremental risk posed by FDI is modest. No data are available on the compliance record of firms not cleared for classified information who may be suppliers to DoD.

DoD experience with FOCI firms suggests that this dimension of the risk of foreign direct investment is manageable. The potential risk to U.S. security interests may arise as the ownership model in Europe's defense sector diverges from the expectation that allied government regulation of firms domiciled under a national jurisdiction will be able to effectively monitor compliance with security obligations derived from bilateral agreements. The likelihood that European defense industrial restructuring will evolve along multinational lines is a challenge to existing structure of bilateral security arrangements. This does not, however, affect the risk to U.S. security associated with foreign direct investment in the U.S. since the U.S. Government security management of FOCI entities is not affected by the restructuring of Europe's defense industry. Foreign owners of whatever nationality will continue to be separated from classified or export controlled U.S. technology under FOCI agreements.

Notice needs to be taken of the security issues likely to emerge as Europe's defense sector is restructured along European rather than national lines. Prior to the emergence of Europe's plans to restructure its industry, U.S. risk negation or a mitigation effort associated with FDI has emphasized bilateral arrangements. In general, the U.S. Government's long-established security relationships with the major English-speaking allies—Australia and New Zealand, Canada, and the UK—reinforced bilateralism in the regulation of foreign direct investors. Firms from these nations, especially the UK, became the primary investors in the U.S. defense market. The well-developed bilateral security relationship encouraged the development of parallel approaches to the legal framework for insuring compliance, and an intense level of collaboration on defense and foreign policy issues. As these nations, particularly the UK, become immersed in the European consolidation process, the degree to which adherence to a strictly bilateral

approach will sustain U.S. security objectives is unknown. UK firms are likely to be allied with a variety of firms from several European states. Entities created in the consolidation process are likely to emerge under a mixture of national and European law. Management of the entities is likely to include a number of nationalities, and is likely to be less identified with the national domicile of its corporate headquarters.

Moreover, even the nations with whom the U.S. has the closest relationship (e.g. the Anglophone countries plus the Netherlands and Norway) have had significant, though episodic compliance problems. A UK entity was involved in illicit commerce with Iraq; a Norwegian entity was involved in the transfer of nine-axis machine tools to the former Soviet Union's nuclear submarine program; and a Dutch entity was involved in the transfer of night vision equipment to Iraq. Confidence in compliance needs to extend beyond the country-of-domicile and focus on the behavior of the company itself.

The commercial and financial incentives for a substantial change in equity participation in the defense market, both in Europe and the U.S., by foreign investors are significant. As a consequence, substantial restructuring in the defense markets of both North America and Europe is underway in earnest. These circumstances provide an opportunity for DoD to review the existing regulatory infrastructure surrounding the security management of the participation of FOCI firms in the United States.

Virtually all capital intensive industries and the service sector are or have already undergone cross-border consolidation. The incentive to do so relate to capturing scale economies in manufacturing, marketing, and services, and the need to raise capital on a large scale to sustain market leadership. The defense sector is among the last to face the choice of cross-border consolidation. If the infiltration of commercial technologies for military applications can be prevented or limited, then the prospects for the defense sector resisting pressures for cross-border consolidation improve. However, if this is not practical, then it is likely that the leveling effect of access to commercially traded advanced technologies will raise the level of technology employed throughout the international defense industry. As has been the case with most other sectors, the need for size, capital, access to skilled labor, etc. will drive the industry toward cross-border consolidation. The effectiveness of security arrangements for DoD to manage a global supplier base will be crucial.

An important policy change in the U.S. in 1993 diminished the role of the Secretary of Defense in the regulation of FOCI firms in the U.S. defense market. Executive Order 12829 (January 1993) created the National Industrial Security Program. The EO requires that decisions to change polices, practices, and procedures for the involvement of FOCI firms in classified work must be made in consultation with 24 executive departments and agencies. In addition, changes must also be made with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission, and the Director of Central Intelligence. These changes must be incorporated in the National Industrial Security Program Operating Manual (NISPOM), the controlling regulatory regime for U.S. industrial security arrangements.

However, the Secretary or Deputy Secretary of Defense can amend FOCI negation and mitigation arrangements and attendant practices so long as such amendments are

consistent with the NISPOM. These circumstances provide an opportunity for useful changes that may be made administratively without a requirement for either a change in the NISPOM or extensive interagency consultation. Proposals for reform offered here reflect this more limited scope of proposed changes. Finally, the policy should be written so that it is transparent to all who need to apply it. Transparency is not a characteristic of the mode of expression in the existing NISPOM.

4.3.4.1 Eliminate low value-added security procedures

Current policy for FOCI firms includes visit and contact approval and extensive reporting requirements. The visit reporting is largely redundant for foreign visitors, and of little real value in recording contacts by U.S. persons visiting affiliates of the foreign parent. It should be eliminated. The firm's security officer grants approvals for foreign visitors from the parent firm. These visit and contact approval and extensive reporting requirements are layered over the normal requirements prescribed for non-FOCI firms. For example, the firm's security officer grants approvals for foreign visitors from the parent firm, even though an approved visit request or other authorization may already be in place. The additional procedures offer little security value since other DoD and Department of State compliance requirements dealing with classified and unclassified export controlled data and technology provide such information. Existing practice involving participation of DSS-approved non-executive members of the board of directors offers a proven basis for assuring that security is a day-to-day concern of senior management officials. If DoD is unprepared to eliminate FOCI-related visit reporting entirely, the process should nonetheless be reformed substantially. At a minimum, FOCI visit reporting should only be required for visits or contacts by senior management of the foreign parent and its affiliates.

4.3.4.2 Reform the National Interest Determination (NID) process

Under the NISPOM, "a company cleared under an SSA [Special Security Arrangement] and its cleared employees may only be afforded access to 'proscribed information' with special authorization...manifested by a favorable national interest determination (NID)" [Section 2-309a]. The NISPOM states that an NID must be "program/project/contract-specific," and that access to proscribed information must be "based on compelling evidence that release of such information to a company cleared under the SSA arrangement advances the national security interests of the United States." The NISPOM further provides that the authority to make this determination should not be permitted below the Assistant Secretary (or comparable) level.

In practice, some government officials hold to the view that NIDs may only be granted in extraordinary circumstances where the national interest requires utilization of the SSA-cleared entity because no U.S.-owned and controlled firm can be found to perform the work. This view is inconsistent with the NISPOM provisions.

As noted above, the NISPOM states that access to proscribed information by a company cleared under an SSA must be based on evidence that release of the information to the

SSA firm "advances the national security interests of the United States." An agency need not demonstrate the national interests "requires" utilization of the SSA firm, but only that the national interest would be "advanced" by release of the information—that is, that the national interest is advanced by possible award of the contract to the SSA cleared firm. It is true that this finding must be based on "compelling evidence," but the evidence need only demonstrate that the national interest is advanced by release of the information. It is reasonable to say, where an award to an SSA firm is otherwise justified, or where access to proscribed information facilitates competition, that the award—or the competition that access makes possible—presumptively advances the national interest. Otherwise, there is no point in going forward.

Moreover, the NISPOM does not state that an NID is only possible when no U.S.-owned and controlled firm can be found to perform the work. These factors clearly recognize that FOCI-cleared U.S. firms are U.S. companies—not foreign companies—managed by resident citizens of the United States. Nowhere does the NISPOM state that an agency must find that there are no available U.S.-controlled firms to do the work.

The NISPOM only states that a proposed NID must include a statement concerning "the availability of any *other* U.S. firm with capacity, capability, and the technical expertise to satisfy acquisition, technology base, or industrial base requirements, *and the reasons any such company should be denied the contract...*" [Sec. 2-309b(4)]. The NISPOM therefore presupposes that there will be other U.S. firms capable of doing the work, and only requires an explanation why an award to the other U.S. firms is inappropriate—for example, because the cost is too high, or because the quality or expertise of the SSA-cleared firm is higher than its domestic competitors. The NISPOM does not require agencies to go to the lowest common denominator, nor does it require agencies to accept a less favorable proposal from another domestic firm.

The NISPOM also requires an evaluation of "any alternative means available to satisfy the requirement." This provision has also been interpreted to require selection of alternative means—if available. But the NISPOM does *not* require selection of such alternative means. Rather, it requires a statement of the "reasons alternative means are not acceptable."

The misapplication of the NISPOM's NID standards does not advance the national interest. Rather, it damages the national interest by artificially limiting competition for government contracts and denying the U.S. Government access to the technologies and expertise of SSA-cleared companies.

The NISPOM lends itself to misinterpretation because, under the NISPOM, access to "proscribed information" by SSA firms is presumptively denied absent special authorization "manifested by a favorable National Interest Determination." It is not hard to understand how this presumption against access has been translated into a bias against award to firms cleared under an SSA. Moreover, the demands of the NID process discourage (and may even prevent) agencies from making contract awards that would necessitate an NID.

Therefore, as currently administered, the NID process frustrates competition and runs contrary to public policy—promoting entry to the Department of Defense supplier base. All of this would be justified if there were evidence that the NID process protects national security. But there is no reason to believe that the current NID process does anything more than restrict competition for government contracts.

Nevertheless, it is possible within the parameters of the NISPOM, to reform the NID process so as to foster competition and protect the national security interests of the United States. To this end, we recommend that the Department of Defense issue policy guidance to make it clear that, pursuant to Section 2-309 of the NISPOM, award of a contract to a U.S. firm cleared under a Special Security Agreement will be presumed to advance the national security interests of the United States if the proposed awardee has a record of service to the U.S. Government and has demonstrated its ability to protect classified and controlled unclassified information from improper disclosure, and the foreign owner is located in a country that is allied with the Untied States, and has been determined by the Department of Defense to present a low risk of economic and industrial espionage. The presumption, of course, should be refutable on evidence that award of the contract to the SSA cleared company would (on balance) hurt the national interest notwithstanding the presence of factors that otherwise justify award—for example, where specific security concerns with a particular contractor militate against award.

The DoD policy guidance should also make clear that the "availability of any other U.S. company with the capacity, capability, and technical expertise to satisfy the acquisition, technology base, or industrial base requirements" of a contract does not require award of a subject contract to the "other U.S. company" rather than the SSA-cleared U.S. company. Where there is presumptive evidence that award of a contact to an SSA company would advance the national security interests of the United States, the SSA company's proposal should not be rejected simply because other non-SSA companies are available to perform the work. Rather, the SSA company's bid or proposal should be considered on a equal footing with bids or proposals from other U.S. companies. If the SSA company's bid or proposal is the best, award to the SSA company clearly advances the national interest.

The policy guidance should also make clear that, where there is presumptive evidence that award of a contract to an SSA company would advance the national security interest of the United States, "alternative means" are *not* acceptable if they are more costly or if they provide inferior products or services.

Competition serves the national interest by enabling the government to obtain the best products and services at the best prices and terms. To protect the national security and ensure effective competition for U.S. Government contracts, it is critical that the NID process not be employed as a barrier against competition from SSA contractors that have a record of past performance of compliance with U.S. national security requirements. Adherence to these policies will facilitate the NID process, and serve the national security interests of the United States.

4.3.4.3 Increase the flexibility of the CFIUS review process.

The Committee on Foreign Investment in the United States (CFIUS) has a crucial role in a decision to authorize foreign investment in the U.S. defense sector. The CFIUS makes recommendations to the President as to the degree to which a proposed foreign investment would adversely affect U.S. national security interests. A decision on whether or not to conduct an investigation that would ultimately require a decision by the President is made during a 30-day review. In some cases when one or more agencies participating in the CFIUS review are unable to complete their review, an investigation is often undertaken. The entire process can take 90 days to complete. As timing on FDI is often critical to the financial viability of the transaction, the 30-day constraint sometimes has the unintended consequence of extending rather than expediting the CFIUS review. Questions raised during the initial thirty day review can cause a case to be withdrawn from consideration requiring the "clock" to be restarted after questions are resolved. Allowing a brief extension of the 30-day review period (e.g., ten days) could mitigate this problem.

Increasing the 30-day review period, even to allow a brief extension would require an amendment of the law. Alternatively, the Treasury Department (on behalf of the CFIUS) could administratively provide for expedited investigations of cases where a full (45-day) investigation is not warranted. By statute, any acquisition that became the subject of a formal 45-day investigation must be presented to the President for final consideration (up to fifteen days) but Presidential review cases could also be expedited in appropriate cases. The statutory deadlines are intended to be an outer bound, not a routine.

Annex III

Taking Full Advantage of the Commercial Sector to Meet DoD Needs

Introduction

The Department of Defense must take advantage of the vast global, commercial capabilities with application to the development and integration of military systems as a major element of its strategy for maintaining military dominance. It is no longer feasible, within a resource-constrained environment, for DoD to rely as extensively as in the past on a defense industrial base characterized by private development and manufacturing, private infrastructure providers, and the service sector. The products required and procured by DoD covered a broad spectrum in application and technology and were often the leading edge of performance and sophistication. In many respects, the commercial sector was the indirect beneficiary of scientific and industrial advances made in the defense sector. The civil air transportation industry is one of the best known examples of this phenomenon.

Prior recommendations on commercialization and acquisition reform by the Defense Science Board and others provide the basis for the Commercialization Panel's investigation. There are, to be sure, many alignments in objectives. The differences arise from a combination of the environment addressed and implementation means having a different character in some cases than those previously proposed.

These will be discussed in detail in what follows. These are simply summarized here:

a) In areas where commercial sector capabilities overlap with DoD needs, it is a much larger sector, is increasingly global and is modernizing much faster than DoD. To gain benefit from these circumstances, DoD must adapt and stimulate along with traditional exploitation.
b) The DoD's forte has been in integration of complex hardware, software, concepts and processes. The commercial sector now offers much more in the way of integrated capabilities, means and technologies. The DoD should solve integration challenges to meet its needs by giving primacy to solutions which employ commercial capabilities, means and technologies, not just technologies. Primacy should extend to and be derived from DoD teams tasked to provide capability solutions derived from commercial building blocks. This is inherently an *advocacy* activity, and one requiring constant vigilance. Simply directing traditional Service teams to "use commercial" will not accomplish the objective or have the payoff that an independent and intellectually competitive effort will produce.

Commercial Sector Potential to Meet Near-Term DoD Needs

Over the past half-century, circumstances relating to commercialization have changed markedly. Defense, still a world-class performer and developer of advanced technology products, is now but one of many sectors in the United States with such characteristics. The commercial sector, driven by demand and competition, is providing world-class products or services, many of which are or could be adapted for military application.

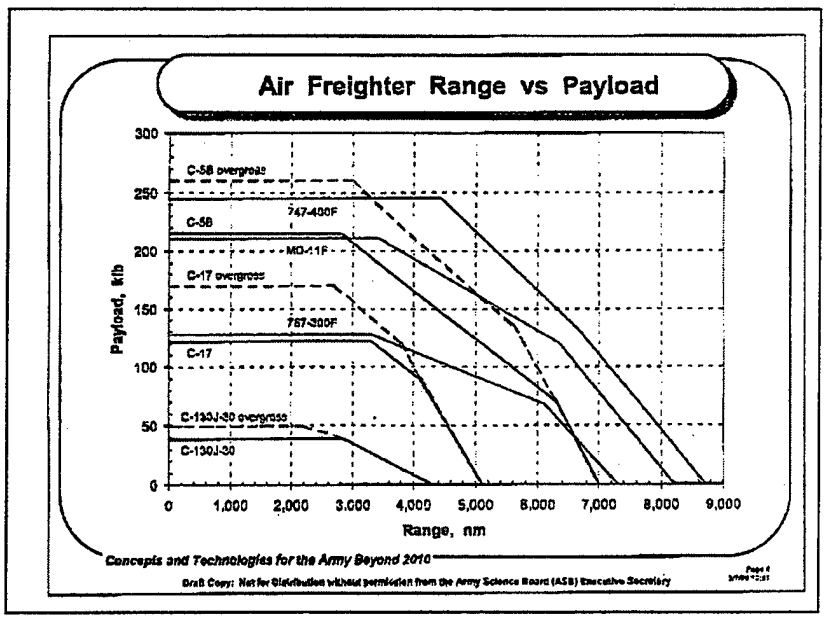
Areas where DoD can exploit advanced technology developments in the commercial sector include:

- air and sea lift;
- logistics and sustainment;
- communication and information systems;
- surveillance; and
- high-efficiency ground transport.

Air and Sea Lift

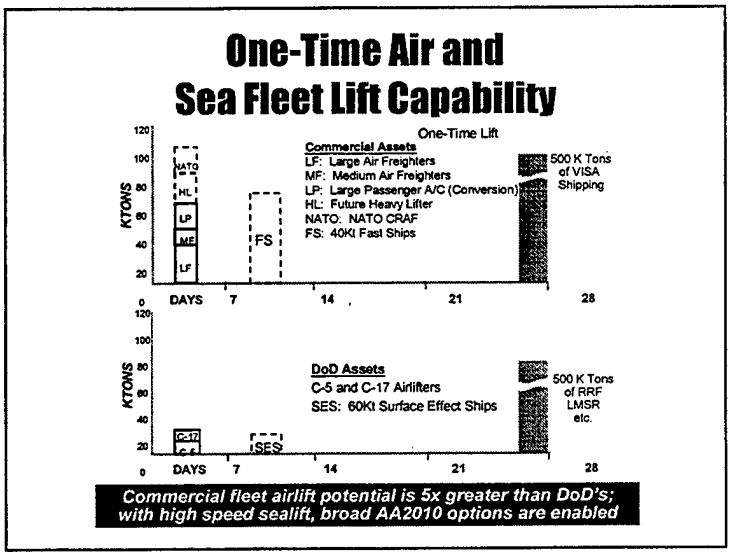
The DoD provides power projection in a variety of ways to establish U.S. presence and to exert control and influence to shape circumstances involving U.S. interests in geographically-remote areas. Power projection requires some transportation capabilities—air, land, sea. At one time, DoD led the way with the most advanced aircraft and large fleets. While the Department still has substantial transportation capabilities—especially for tactical operations and outsized cargo—these are steadily being dwarfed by the growing commercial air transport sector, which is largely global. Figures 1 and 2 illustrates this trend, with a comparison of current range-payload characteristics and anticipated fleet size for defense and commercial air and sea assets.

Figure 1: Air Freighter Range vs. Payload



Today TRANSCOM, which is dominated financially by the personnel and operating cost of its air component, is a $7 billion per year cargo movement activity. The volume of global air-freight business exceeds $50 billion per year in annual revenues. The global passenger business is twice that—exceeding $100 billion. The global fleet of commercial aircraft is in excess of 15,000 (over 60% of it is U.S. owned or controlled). By contrast, DoD's fleet of similar aircraft numbers only a few hundred, under the most appropriate comparison, but could be as large as one thousand with very liberal counting rules. Throughput—passenger miles per day and freight tons per day—also illustrates a tremendous gap between defense and commercial capabilities.

Figure 2: One-Time Air and Sea Lift Capability



Logistics and Sustainment

This is a broad topic, but its breadth is probably greater in the commercial sector than in defense. DoD must deliver and sustain forces globally. Just as in transportation, there is a strategic component and tactical component—the tactical component often referred to as the "last mile," though the actual distance may be greater. Commercial sustainment and logistics are similar to DoD's in many cases.

A commercial example, particularly relevant to DoD's requirements, is that of Caterpillar®, known internationally for its state-of-the-art practices in parts distribution. Caterpillar® has manufactured, sold and sustains a fleet of over two million heavy earth moving machines throughout the world. Over half the fleet is legacy (over 30 years of age). DoD's inventory is younger now, but may reach or exceed this age in the next decade.

The Caterpillar® fleet is sold and sustained by an integrated centralized and decentralized organization. Caterpillar® provides the centralized portion, its customers and dealers form the decentralized portion, and a global transportation network provides most of the physical infrastructure. Caterpillar® provides the information infrastructure.

Caterpillar's® equipment performs tasks in the field which cost hundreds to thousands of dollars per hour. Thus, time urgency is a necessary element in sustaining this fleet and is

crucial to customer confidence, satisfaction, and repeat business. The replacement value of the Caterpillar® "fleet" is about $1 trillion. The replacement value of DoD's fleet is between $2 to 3 trillion.

Worldwide delivery of parts and services, supplied by both local dealers and U.S.-based Caterpillar®, is accomplished with world class performance: 83% of all requests are satisfied in 6 hours or less, and 99.7% in no more than 48 hours. And incorrect deliveries are small in percentage.

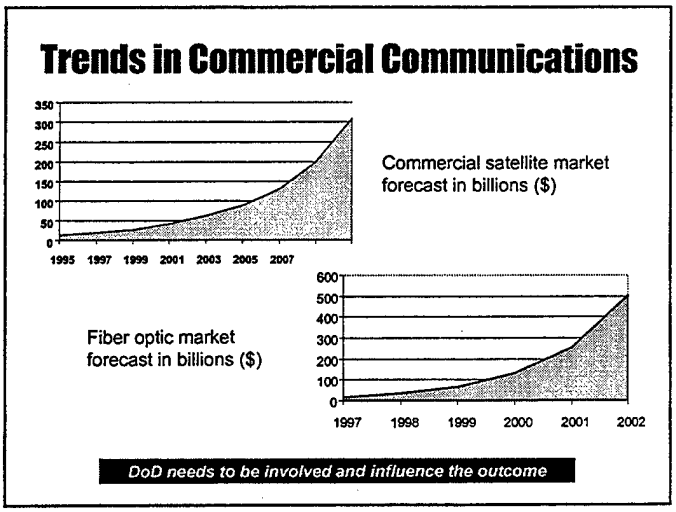
While all of DoD's circumstances are not identical—particularly in tactical ground combat situations—where there are similarities, DoD performance is far from the standard achieved by Caterpillar®. The point to be made is that the global commercial economy has substantially outperformed DoD in this sector on a scale comparable with that of DoD.

Commercial Communications and Information Systems

Planned space-based communications for the next decade will have capability that exceed DoD theater and lower level needs by at least two orders of magnitude. Commercial investments in fiber optics and available bandwidth are even greater, as illustrated in Figure 4, exceeding DoD's needs by three to four orders of magnitude.

While available communication and information capabilities exist in the commercial sector, DoD faces obstacles to using these assets that include: (1) applicability in the tactical last mile; (2) susceptibility to soft and hard countermeasures, such as jamming and nuclear weapons effects; (3) lack of complete control over the asset/service, (4) asymmetric threats, terrorist attacks, or chemical or biological agents; and (5) obstacles created by uncooperative nations. Despite these obstacles, the benefits to DoD of using these assets in terms of cost avoidance and modernization are so great that the Department should seek innovative approaches—using both commercial and traditional DoD solutions—to overcome the *real* obstacles.

Figure 4: Trends in Commercial Communications



Global communications was once a domain where DoD was the indisputable leader. Now and into the future the global commercial sector will dominate because its resources and investment capability are so much larger than those of DoD for this sector. Moreover, the growth in commercial development and deployment of information services useful for military applications overwhelms the scale of the defense market. DoD is not likely to create its own Internet or develop logistic tracking systems, for example, that are isolated from the commercial sector.

Surveillance

Space surveillance is becoming multi-national and commercial at the same time. Individual nations (France, India, China), multinational organizations (European) and commercial consortia and partnerships plan to deploy space-based high-resolution imagery and hyperspectral imagery systems in the next decade. Again, such capabilities existed exclusively in the military arena and only in the United States and Soviet Union in the past.

Rapid commercial advances create both opportunities and risks. On the positive side much more mapping data should become available for military applications, with improvements to systems such as the French SPOT. Additional high-resolution capability can be brought to bear during possibly troubled circumstances to augment military surveillance capabilities. While staring capabilities (such as those expected with the DARPA-USAF-NRO Discoverer II) are not likely to be found in the global commercial market, other commercially available capabilities may be useful to DoD. In particular, greater access to some regions of the world with multiple commercial systems and hyperspectral mapping and change detection are two examples of commercial capabilities with application to military purposes. Exploiting commercial technologies can also provide DoD with a means to monitor the degree of security that U.S. countermeasures provide to deployed forces against hostile surveillance.

Should DoD arrange to have such information? The answer would seem to be "yes" even if DoD does nothing more than use it to determine how "visible" its own operations are both in the United States and around the world.

High Efficiency Ground Transport

The oil shocks of the 1970s started a trend in developing and fielding transport systems of increasing efficiency. Much has been done but there is still substantial room for improvement. Since the 1970s, overall fuel consumption for the United States' fleet of commercial automobiles has remained constant although the fleet has grown in size by over 20% and in miles traveled by more than 50%, according to statistics from the Department of Energy. Sport and utility vehicle (SUV) fleets are growing much more rapidly than other market segments and using more fuel as vehicle weight has increased.

Pressure from corporate average fuel efficiency (CAFÉ) requirements is starting to change things. Manufacturers are developing hybrid propulsion to provide greater fuel

efficiency. There are now innovative vehicle designs, employing lightweight aircraft-like designs that offer a doubling of vehicle payload fraction.

What is the benefit to DoD of an aggressive commercialization program? DoD operates one truck for every three people in the armed forces. By adopting high propulsion efficiency vehicles and adapting them for military use, DoD could carry the same unit operational payload in half the number of trucks when cargo is measured in terms of weight (not limited by specialized size or volume constraints). Conservative estimates suggest savings of at least 20% of the total number of trucks in a unit. Commensurate savings in fuel, spares and people (in several skill categories) could be realized. Preliminary estimates suggest a personnel reduction of at least 15%.

A New Approach to Commercialization

The examples discussed above illustrate commercial products and services that could materially benefit DoD in both performance and cost avoidance. Other examples of sectors that can provide benefits to the Department are personal information systems, interactive entertainment (that can be used through a training simulator), and biotechnology, including gene-based medical assessment and treatment.

Moreover, there are technical innovations under development whose commercial character will drive the market. Commercial development of MEMS (a byproduct of the chip revolution), self-organizing networks, and bio-mimetics are several examples. DoD will be able to make use of these technologies, but will have little influence over the evolution of these markets except for a few highly specialized items (such as radiation-hard electronics). This is similar to the microchip market today: DoD consumes about one percent of the $200 billion commercial market.

New technologies such as pharmaceuticals, nanofabrication, and quantum coupling will have an unpredictable effect on defense capability. Nevertheless, the potential for breakthrough, capability-enhancing or even capability-establishing technology should not be ignored in commerce. These represent the phenomenon of technology *emergence*, which should be encouraged and fostered by DoD. More and more emergent ideas will be coming from commercial enterprises—some of which will have important defense applications. DARPA is the institution in the Department likely to be the most effective advocate for the use of such emerging technology and to identify and assess its military applications.

In the past, DoD has exploited commercialization, though in a very limited manner. Commercial products were sought only when the developer was prepared to adapt the product to DoD use. There are few successful examples of this approach and DoD's ability to extend this approach in the current commercial environment is rapidly vanishing.

An example where DoD did choose to adopt an off-the-shelf system for its own use was the procurement of wide-area communications, the Army's Mobile Subscriber Equipment. The Department elected to procure a suitable and affordable system by adapting an existing alternative. Two candidates were available—the French *RITA* or the

British *Ptarmigan* system—and both offered significant advantages over indigenous development. In particular, two advantages were a short fielding time—18-24 months compared to 60-72 months for a system requiring research and development—and access to continuing improvement of one to two generations over a military system. In the end, the French system was chosen. It was $2 billion cheaper than the UK alternative, and at least $4 billion less than an indigenous alternative. The fielding schedule was met as were affordable modernization and support goals.

These benefits were achieved as a consequence of dogged and persistent efforts of the U.S. Army's Acquisition Executive (Under Secretary James Ambrose), the Under Secretary of Defense for Research and Engineering (Dr. Dick DeLauer), and a dedicated program management team. The traditional product development and program management community opposed the approach. However talent, diligence, advocacy, and support at senior level leadership made the approach possible. These circumstances reflect the needed bureaucratic ingredients in successful commercialization. Senior level leadership and advocacy are crucial enablers.

Exploiting commercial opportunities is important and useful. *But DoD needs to go beyond exploiting commercial the commercial sector and make commercialization a primary instrument of modernization.* The Department must stimulate commercialization (even though it is not the major buyer) for both operational and economic reasons. Adapting available commercial products (by making modest changes on its side of the requirements equation) through scrapping requirements and developing new concepts that fit availability of commercial products or services are two elements of such a process.

Accepting the commercial sector as a major participant in developing military capabilities means that DoD must accept at least a diminishing degree of control over the technology. The commercial-industrial sector of the economy will be generating the ideas and technology that will form the basis of U.S. defense capabilities. Thus, DoD will be required to act much more quickly than it has in the past to influence these ideas. It will also need to pay close attention to the commercial economy and employ scientists, engineers, computer scientists, and technicians to remain up-to-date with the latest developments in what may appear to be a random process of development.

The impact of commercialization on DoD makes it necessary for the Department to become more agile and to make more decisions at subordinate levels. Moreover, DoD will have to be more responsive to new ideas and to accept the loss of *complete control* over its technological future. But without substantial change, DoD will become increasingly irrelevant to a world undergoing rapid and dynamic change.

Recommendations contained in Chapter 4 (4.2.1-4.2.5), pp. 39-43.

Annex IV

Vulnerability of Essential U.S. Systems Incorporating Commercial Software

Introduction: The Seeds of the Problem

The need to control the cost of defense acquisitions has forced the Department of Defense into accepting considerable security risk, which is not well quantified.

The acquisition strategy of the U.S. Department of Defense is to make maximum use of commercial sources for goods and services. Whenever possible, commercial-off-the-shelf (COTS) products are to be used. This is supposed to provide considerable savings, inasmuch as the best fair price, especially for high-demand, standardized standardized items when the DOD is not the dominant buyer, is the "market price." The market price for such "commodities" is established by competition and presumed to be the marginal cost to produce the item.[1]

The irreversible trend, worldwide, is for industry to become globalized. As a result of these two trends, much of what the Department of Defense procures—indeed, much of what it depends on for essential systems—may have been designed and/or built by, or within reach of, a potential adversary. Many believe that our core warfighting systems are not acquired in such a way as to jeopardize them thusly. Even if that were true, or if we could reverse the global-commercial trend for systems so-identified, the craft of warfare as practiced by the U.S. is so interdependent upon a multiplicity of supporting systems, that the liability is real.[2]

Another contributing factor is the increasing complexity of systems. Systems are more complex for several reasons. They are designed to have more functionality, for example to include embedded training and simulation in an otherwise combat-oriented system. They are increasingly built upon general-purpose computers and operating systems, which, themselves, have added functionality. The systems are more likely to be networked together into an ever more complex "system of systems." And, as the cost of computing and storage falls, there is no incentive to produce functionally lean systems—problems are invariably fixed by adding more corrective layers rather than fixing the underlying logic or implementation. All of these things make exhaustive testing of today's systems nearly impossible, and wholly impractical.

By way of recapitulation, more commercial procurement of essential U.S. defense systems from a globalized industrial base places the manufacture of these systems within

[1] Curiously, the Department of Defense is not uniformly convinced of the soundness of this economic theory. In fact, a considerable bone of contention between commercial vendors and U.S. Government contracting officers is the insistence on seeing cost data and subjecting these data to a price analysis.

[2] This was demonstrated, *inter alia*, by the now-famous exercise, *ELIGIBLE RECEIVER*, which showed that even if we were able to hold harmless the Global Command and Control System (GCCS), vulnerabilities in the more accessible supporting systems of the GCCS effectively neutralized portions of our warfighting capability.

the reach of a potential adversary who might emplace hostile features, which defy detection because of the complexity of the systems themselves.

Why Software is Different

Software is complex and its per-copy cost, unlike hardware, is independent of size, complexity and functionality, which encourages opacity and bloated code, both of which favor the saboteur.

The traditional experiences with the acquisition and control of hardware components are not necessarily applicable to software. Software is vastly more complex than hardware. Indeed, we add complexity to composite systems *via* software (sometimes, "embedded" software) because it would be nearly impossible to produce so complex a hardware system. Because of this complexity, software is virtually untestable. Exhaustive testing may even be theoretically impossible. In any case, its cost would be prohibitive. We blithely accept this: manufacturers depend on users to debug the products, and neuter warranties. Software, being more easily changed than hardware, is frequently changed, and strict configuration control is a costly and under-practiced art. Software can be perfectly copied at almost no cost, and can easily be transmitted worldwide over communications networks. And, critically, software replication cost is independent of size, complexity and functionality so there is no incentive to simplify or to remove vestigial code. These fundamental differences between the world of bits and the world of atoms may argue for special consideration of software in issues of globalization and security.

Software constitutes an increasing portion of commercial and defense systems. As complexity and functionality continuously increase, much of that complexity takes the form of software (sometimes as unheralded embedded software). A typical systems software program today contains more than a million lines of source code. For example, the Microsoft operating systems for personal computers are derived from source codes of tens of millions of lines. Complexity on that scale is in a real sense unknowable. It is virtually impossible to test exhaustively to determine either performance or trustworthiness of code on this scale. If the source code is not available, as is often the case with programs purchased in the commercial environment, it takes considerably more effort to deconstruct and understand the code than it did to write the program in the first place. Even were source code available for inspection, given the negative incentives for simplification and streamlining, certification would be daunting.

Recently, the National Research Council of the National Academy of Sciences commented on the dangers that may be inherent in use of commercial software components in large system design. According to the Committee on Information Systems Trustworthiness:

> COTS software offers both advantages and disadvantages [to a system developer]. COTS components can be less expensive, have greater functionality, and be better engineered and tested than is feasible for customized components. Yet, the use of COTS products could make developers dependent on outside vendors for the design and enhancement of important components. Also, specifications of COTS components tend

> to be incomplete and to compel user discovery of features by experimentation. COTS software originally evolved in a stand-alone environment where trustworthiness was not a primary concern. That heritage remains visible. Moreover, market pressures limit the time that can be spent on testing before releasing a piece of COTS software. The market also tends to emphasize features that add complexity but are useful only for a minority of applications.[3]

The problems of complexity and changeability are getting worse. Complexity is being driven by Moore's Law, which observes that semiconductor technology doubles its cost effectiveness every 18 months. This exponential increase in capability leads inevitably to more and more functionality being placed in software. Moreover, there is a technological trend towards the use of mobile code, where programs are downloaded from the network on the fly when functionality is needed (e.g., Java applets). The increasing use of mobile code exacerbates the problems of software security.

Computer chips and other application-specific integrated circuits (ASICs) constitute a middle ground between software and hardware. These chips are produced from software designs that may contain upwards of a million devices. This level of complexity, while daunting, is less than that of most software. Moreover, chips are less subject to change than software, and may be controlled physically.

Why Globalization in Software is Necessary

> *Global demand for software and the minimalist competitive advantages inherent in software—little capital or infrastructure is required and many U.S.-educated computer scientists are foreigners, anyway—means software will be produced where it will.*

There are both practical and conceptual reasons why globalization in software is inevitable and even desirable. The practical reasons have to do with capability and economics. India, in particular, is graduating software engineers at a rate of about three or four times that of the United States. At the current rate, in ten years India will have more software capability than the rest of the world combined. Given the differences in standard of living, it is likely that software produced abroad will be considerably cheaper than that produced in the United States. Today most large corporations rely on outsourcing from India for the purchase of custom software and to do upgrades such as that involved in the Y2K certification.

Software has the property that it often is subject to the law of increasing returns. That is, the more users that share a given program, the more valuable the program becomes. This law leads to a lock-in phenomenon, where the winner takes the entire market, and the loser almost none. Since the defense market is small relative to the commercial market, this means that the defense industry must "ride the wave" of the most popular commercial products for much of the systems software that it needs. To have its own special programs would cut it off from the mainstream of innovation in the worldwide market

[3] Committee on Information Systems Trustworthiness, Computer Science and Telecommunications Board, National Research Council, *Trust in Cyberspace*, ed. Fred B. Schneider, Washington, D.C., 1999, p. 245.

and seriously degrade both the economics and capability of its environment. Moreover, the law of increasing returns means that the United States must in many cases share its software with the rest of the world.

Not many years ago DoD had its own communications protocol suite, called GOSIP, and its own milspec microprocessor, and don't forget JOVIAL and ADA. Imagine the situation if the proprietary development of hardware and software to support a very small user community had continued. Like any intelligent buyer today, DoD has to follow the market closely and anticipate the winners, so its equipment will be interoperable with the mainstream of commercial activity—a mainstream that will necessarily be global.

The Perceived Threat

> *DoD computers are "attacked" daily, and many Nation-States are known to be interested in Computer Network Attack technology, but little hard evidence exists to link the two.*

The U.S. Intelligence Community is the logical place to find out about the reality and severity of the threat that foreign suppliers, responsive to their respective governments, might be compromising U.S. systems. Without revealing classified sources, we may generally conclude that many countries are familiar with, and some actively exploring, the dimensions of information warfare—the larger rubric under which we catalog such subtle sabotage to systems. Probably taking their lead from U.S. pronouncements such as *Joint Vision 2010*, a number of countries have espoused the usefulness of information operations as an adjunct to conventional warfare. Beyond a suspected, isolated incident or two, there is relatively little evidence of foreign state actors targeting U.S. systems manufactured abroad today.

We distinguish State from non-State actors in this discussion. The vulnerability of the highly developed U.S. civil infrastructure tempts an "asymmetric" foe such as a terrorist organization, *i.e.*, a non-State actor. But, in the case of acquisition of hardcore U.S. warfighting systems, we more likely need to be concerned with a different kind of asymmetric adversary—one who expects to be engaged across the conventional spectrum of conflict and would like to even the odds by downgrading U.S. technology, allowing the tide to turn on manpower.

To summarize, U.S. Intelligence acknowledges little hard evidence of such attacks, but we may conclude that with the skills available to would-be attackers, we would not find the evidence—without collateral indications—until it bit us. Indeed, consulting with professional "hackers" leads to the same conclusion. According to them: "If you were to let us design and code your software, we would 'own' your system. Our mischief-making modifications would not be detectable."

Trustworthy Software

"Risk Management", though shopworn, is still the best advice.

How can we trust software written abroad? The answer is that we can't. However, like anything else this is a risk management issue. There is risk even in software produced in the most secure U.S. environments. The only question is how much risk and at what cost.

Experts agree that it is not feasible to test thoroughly software for "violations of trust", such as backdoors, that would enable unauthorized access. Nor is it at all likely that such tests will be possible in the future. However, there is also a prevailing opinion that the bar can be raised appreciably, so that some degree of assurance can be attained. There are tests today that ascertain code coverage and detect "unused" or suspicious code. We need to develop better tools for this purpose.

Industry has had little incentive to fund the research and development of trust management tools, since there is large cost and little reward for such efforts. Thus the burden rightly falls on government to provide seed funding for research in this area, which is surely an aspect of critical infrastructure protection. Research should be facilitated in the specification and testing of code for trustworthiness, in addition to the management of trust in its operation. Based on policy and credentials, who should be allowed to do what? Academic researchers in particular would very much like to have the opportunity and motivation to work in this fundamental area.

In addition to funding research, the trustworthiness of purchased software could be increased by promulgating (or, at least, stimulating and embracing) standards for certification of trustworthiness, much like the CMM (Capability Maturity Model) for software quality. Ideally, there would be industry-accepted guidelines and certification at various levels of trustworthiness, which would presumably also be available to foreign suppliers. Contracts could specify the necessary level of trustworthiness, with the highest—and most expensive—levels reserved for the most critical software modules. The trustworthiness of a given module would have to include consideration of all included programs, as well as compilers and other programs that are able to affect the final object code.

The Software Engineering Institute at Carnegie Mellon University, a federally-funded R&D center, has successfully promoted standards for software quality, and serves as a good example of government leadership in a related area. Currently, there is a joint program between NSA and NIST, called the National Information Assurance Partnership, which is developing specifications for security functionality and assurance requirements, with a focus on security products, such as firewalls.

Software is also a "People Problem"

The great majority of all security breeches today involve the cooperation of insiders.[4] Although the fear is the seemingly anonymous attack through a network, the much more

[4] In the recently released 1999 CSI/FBI Computer Crime Survey, of 521 companies asked about the likely source of any attacks, 53% of the respondents cited U.S. competitors, 74% (also) cited independent hackers, and 86% (also) cited disgruntled employees.

likely source of attack is from the inside. System administrators and operators, installers, network administrators, and other people who maintain computers and networks are the weakest links in the chain of trust. The most cost-effective route to system security is probably not in testing and reverse-engineering software products, but in maintaining security checks on the personnel who develop and maintain the software and networks, and in strong policies on secure operation and administration of these networks.

The vulnerability of people is a factor in the risk management decision of whether a network should be opened to the outside or closed. Obviously, the risk of an attack from the network is (largely) eliminated if the network is not connected to the outside, but the inside threat remains, and such a decision needs to be taken in light of the value of lost connectivity. Metcalfe's Law says that the "value" of a network grows as the square of the number of people connected (the number of possible connections). Although this may not be literally true for a given application, today's computer world increasingly relies on distributed computing and information. Cutting a system off from this capability should be done only as an informed decision.

Potential Ameliorative Measures

Diplomacy and Deterrence: The United States may choose to exert moral leadership and condemn computer and network intrusions as "acts of war" that would be met with punishing conventional force—e.g., military strike and/or economic sanction. Russia is already on record as proposing an information operations "arms-control" regime.[5] As with nuclear disarmament, the initial U.S. reaction was to treat the Russian offer as disingenuous and more favorable, in any case, to the Russians. Disingenuous, almost certainly. But, the aforementioned asymmetries would appear to favor the U.S. and not the Russians. Distinguish this case from their proposals to legislate away our Strategic Defense Initiative (SDI, a.k.a. Star Wars). In that case, the enormous investment needed to achieve success on SDI favored the U.S., who appeared willing and able to bear the cost, *vice* the Soviet Union, which could not. Here, the cost of development of Information Operations (IO) weaponry is within reach of most countries. It requires a minimal capital stock of computers, and a cadre trained in the newest information technologies—which training the U.S. happily provides for all and sundry.[6]

Would the prospect of moral leadership and U.S. advantage convince us to step back from the threshold of information operations? The appeal of such "weaponry" as a bloodless alternative to conventional ordnance—another arrow in the quiver—is strong. However, maintaining a credible ability to use force, in cyberspace and elsewhere, is lawful, under accepted international law, and a fundamentally important aspect of deterrence and international peace and security. Any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state

[5] Shades of 1899, it was the Russians, at the First Hague Peace Conference, who proposed a prohibition on "the discharge of any kind of projectile or explosive from balloons or by similar means."

[6] By one account, over 70% of the Computer Science PhDs granted by U.S. universities were granted to "foreigners."

is an unlawful use of force within the meaning of UN Article 2(4) that may produce the effects of an armed attack prompting the right of self defense.[7]

Operational Measures: There are a number of steps that can be taken to reduce the effects of such subtle sabotage. Anomaly detection refers to techniques, generally used for intrusion detection, which search for departures from normal behavior of and on a computer system. There is considerable effort to improve such techniques, which currently suffer from a very high false alarm rate—i.e., very frequently, intrusion/anomaly detection systems are triggered by perfectly normal activity.[8]

Interestingly, the knee-jerk response to suspected intrusion is to sever connectivity between the target system and other, perhaps more publicly accessible, systems. Generally, the effect this has is to take the target system out of service. Note, however, that "denial of service" is often an attacker's goal, which we may have unwittingly satisfied. The simplistic prescription is to caution against over-reaction. More useful is the generalization that, for detection systems with a high false alarm rate to be of any value, steps must be taken to reduce the "cost", i.e., the effect, of a false alarm. Most useful, is to realize that excess capacity—true redundancy—is the touchstone for resisting such onslaughts. Indeed, characteristic of many denial-of-service attacks is an attempt to "busy" all the system's resources. Excess capacity makes it just that much harder to do, and incidentally makes the attempt that much more anomalous—that much more noticeable.

We have already touched on redundancy and the requirement for independent backups. In systems, as in democracies, however, the cost of independence is eternal vigilance. As systems are integrated, as computers are ever more capable, there is an unconscious conspiracy between the designers and the cost-conscious acquisition process that strips out the redundancy. An errant backhoe, the most usual and effective denial-of-service tool, repeatedly uncovers the fact that communications circuits thought to be independent channels have somehow migrated onto the same cable bundle, or the very same fiber. Capable and skeptical designers—the "red team"—must be constantly searching for single-point failures.

Another category of operational defense measures centers on systems administration and system maintenance. Perhaps as important as it is difficult in today's large, complex systems is configuration control. Unapproved modifications seem to show up in all but the most aggressively managed systems. And, finally, the three keys to most mischief are access, access and access. So, it only stands to reason that blocking access is a key defensive measure. Strong user-authentication and closed networks are quite resistant. There is, however, continuous pressure to open networks, to interconnect, and to permit data exchanges between, say, classified and unclassified networks. This is pressure that should be continually resisted. However, that requires some changed paradigms for the way such systems are used.

---

[7] For an expanded view of these and similar thoughts in this paper, see *CyberSpace and the Use of Force*, by Walter Gary Sharp, Sr., Aegis Research Corp. 1999.

[8] A serious limitation to anomaly detection is inherent in the nature of general purpose systems. The more functionality a system has, the harder to detect anomalies. Anomaly detection should be a design goal of the system!

Finally, we cannot overstate the importance of having a corps of systems administrators who are healthy, wealthy and wise. They need to be selected based on criteria that appreciate their importance, be trained well, and be compensated appropriately for self-esteem and retention. Too often, recognition for the systems administrators comes when the system fails, not when it works.

Acquisition Advocacy: In the acquisition process, there must be an empowered advocate for safe design and procurement. Current incentives must be changed to counter relentless pressure to meet schedules and reduce costs at any cost. A sound starting point is review of acquisition policies and directives. To begin with, the essentiality of a system should be declared as soon as it is so designated (perhaps as early an the concept definition phase) so that special measures can be applied if necessary. Here, we can take a lesson from the Y2K remediation process that flushed out, if slowly, those essential systems in use today. An acquisition security plan should be completed and approved up front, if not for all system acquisitions, then at least for those deemed essential. A critical stricture for the design, and even earlier for the requirements phase, is to limit the functionality to that essential to perform the mission. Excess functionality is the hacker-devil's playground. But, whatever the prescriptions, the message is our favorite: there needs to be a "red team" whose job it is to find vulnerabilities that exist, and to imagine them before they exist.

Certified Products: In some cases it may be desirable to spend considerable effort in certifying products, to assure that they perform as advertised and only as advertised. This will increase the cost, to be sure, and is properly viewed as "overhead." However, we have considerable experience with this practice in terms of U.S. Government cryptographic systems, where it is clear that the possible consequences justify the measures. A similar cost benefit equation pertains to a broad class of security products—proxy servers, firewalls, secure routers, etc.—and responsibilities for these products should be reaffirmed. Presumably the DIRNSA will be charged with this product assurance as a natural part of the COMSEC-INFOSEC mission.

Public (Hacker) Testing: It is clear, given the state of the art today, and the complexity of the systems under discussion, that exhaustive testing of all systems to be acquired will be prohibitively costly, as well as generally ineffective. To re-institute such acceptance testing would return us to the bad old days of MilSpecs and $400 screwdrivers, and commit us to always using outdated, no-longer-on-the-shelf versions of software. Below, we discuss some ways to improve the state of the testing art, and suggest also that some really, really essential systems might stand the overhead of special acquisition processes for quality assurance. Here, however, we make a more controversial proposal, based on a universal observation: published (i.e., "open") systems are mercilessly tested by individuals of exceptional skill and fortitude, who work for satisfaction and without remuneration. The pudding that provides the best proof is the collection of encryption algorithms. Internet browser security runs a close second, neck in neck with operating systems.

The challenge, of course, is the willingness to publish details of the essential system, which might, itself, give aid and comfort to a potential adversary who might otherwise have to engage in time-consuming, not-always-successful, reverse engineering even if they can acquire a copy of the system. Of course history has shown that once systems

enter the inventory (and sometimes long before) good intelligence services have a way of getting copies, more often than not. But, in the present context, where it is believed that the adversary could have had contact with the system during design and build, further exposure may not increase the risk. As ever, risk management isn't easy.

Indeed, for essential *non*-Defense systems outside the penumbra of classification, we may expect pressure to make the systems open. This will be particularly true for essential civil infrastructure systems on which most citizens depend—citizens who may be increasingly reluctant to take for granted their government's (or commercial provider's) assurances. Note that the real risk, here, is the possible exposure of vulnerabilities that we may be *unwilling* to fix because of cost—in which case the responsible party would be rightly accused of "maintaining a public nuisance" and be liable therefor.

Basic Research: There was a time when considerable funds, including Defense funds under DARPA cognizance, were expended on software design methodology. The goal, *inter alia,* was "provably correct" software. This effort needs to be reinvigorated, and the related theorem proving areas are also research-worthy. Another fertile but fallow research area has to do with a more fundamental understanding of system "bugs". It has been claimed that a high-level taxonomy of discovered vulnerabilities would number less than a dozen. These are all quite familiar to the *cognoscenti* but still get designed in to new systems with depressing regularity. "Buffer overflow" is a good example, fixed hundreds, if not thousands, of times. Unquestionably, fundamental work on vulnerability classes will lead to better system assurance procedures, starting with better software design and coding. Indeed, the whole field of "smart testing" is an awakening one, and should be the subject of an adequately funded DoD research thrust.

Really (Really) Essential Systems: There are sure to be cases where many of the old rules for system design and acquisition apply: a vetted workforce, secrecy, procurement "sterility", intensive "red teaming" to expose weaknesses at every stage of the acquisition as well as in the intrinsic design and subsequent execution. Another old trick still worth trying in exceptional circumstances is a modularized design, known in its entirety to very few, with multiple independent modules acquired for later mix-and-match operation.

Additionally, where the existence of the essential system is unclassified, consideration should be given to so labeling it—i.e., by declaring that intrusion into that system shall, by the essential nature of that system, be presumed to be a demonstration of hostile intent. Therefore, the right to respond in anticipatory self defense shall apply presumptively to such sensitive systems, which are critical to a state's vital national interests.

Aggressive, focused Counter Intelligence (CI): The disappointing truth about many of our Technical Surveillance Counter Measures (TSCM) is their near-universal inability to find bugs we didn't already know about or suspect from collateral information. The lesson, while costly to learn, has application here. If we are the subject of such subtle sabotage efforts, we are likely to discover their technical manifestations only when we already suspect them and have some knowledge of the type and source of attack. We need to re-energize efforts to this end. The Intelligence Community must be tasked, with meaningful authority and priority, to meet this challenge. New skills will be needed by

case officers, who will need to recruit new sources; SIGINT collection will need to be similarly refocused.

There is another reason for wanting to know as much as possible about the doctrine, intentions, and practices of other states. Studying state practice is the best way to accurately predict (and *ex post facto*, rationalize) what may be considered an armed attack within the meaning of UN Article 51 which acknowledges the inherent right of a member state to individual or collective self defense. However, the right of self-defense under customary international law may not always justify an armed response (or a response in kind.)

Maintain Offensive IO Capabilities: For purposes of deterrence, the broadest spectrum of capabilities may provide the best array of responses, to include responses "in kind". Rules of engagement (ROE) will have to be honed. The right to respond in self defense—indeed, the right to respond in anticipatory self defense—may not apply to the penetration of all U.S. Government systems during peacetime, but surely can apply presumptively to those sensitive systems that are critical to a state's vital national interests. Such rules of engagement would be consonant with, and enhanced by, an espoused policy of deterrence and the signaled degree of sensitivity of systems from which evidence of hostile intent shall be inferred in the case of intrusion.

Personnel Security: Last, but far from least, we need better personnel security practices, the subject of a separate section of this report.

Conclusions

- Globalization seriously adds to the risks inherent in commercial procurements. We do not have good metrics to calibrate the incremental risks, nor do we have good metrics by which we can judge the essentiality of our systems.
- Risk management is not currently practiced assiduously at every stage from design, through manufacturing, to acquisition, installation and operations and maintenance. Accountability is not fixed, and authorities are not commensurate with responsibilities. It is likely that the proper locus for that accountability is with the acquisition executives.
- Those who work on the defense against computer and computer network attacks are too few and there is a paucity of tools at their disposal. The first line of defense are the systems administrators who are under-trained, over-worked, and under-appreciated.
- The foundation for our defensive posture, despite any technological breakthroughs we might make, is our personnel security system, which is not especially geared to these new threats. There is only the shadow of the aggressive, focused counter-intelligence program that is required.
- Research on all facets of this problem is inadequately funded and the focus is too diffuse. The "customer" for such security research is often hard to identify; the acquisition executives (per a previous conclusion) should identify themselves as the avid customer for this research.

- The National Research Council of the National Academy of Sciences has recently published the following conclusions,[9] which we endorse:
  - "The design of trustworthy networked information systems (NIS) presents profound challenges for system architecture and project planning. Little is understood, and this lack of understanding ultimately compromises trustworthiness.
  - "To develop an NIS, subsystems must be integrated, but little is known about doing this. In recent years, academic researchers have directed their focus away from large-scale integration problems; this trend must be reversed.
  - "It is clear that networked information systems will include COTS components into the foreseeable future. However, the relationship between the use of COTS components and NIS trustworthiness is unclear. Greater attention must be directed toward improving our understanding of this relationship.
  - "Although there are accepted processes for component design and implementation, the novel characteristics of NISs raise questions about the utility of these processes. Modern programming languages include features that promote trustworthiness, and the potential may exist for further gains from research.
  - "Formal methods are being used with success in commercial and industrial settings for hardware development and requirements analysis and with some success for software development. Increased support for both fundamental research and demonstration exercises is warranted.

Recommendations from this section of the report contained in Chapter 4 (4.2.6-4.2.10), pp. 44-46.

[9] Committee on Information Systems Trustworthiness, Computer Science and Telecommunications Board, National Research Council, *Trust in Cyberspace*, ed. Fred B. Schneider, Washington D.C., 1999, pp. 244-246.

Annex V
Commercial Space Services and their Impact On National Security

Projected Environment

- In the next ten to fifteen years, there will be an industry that depends on space with a turnover worth several hundred billion dollars a year. It will include not only space communications, but space observations, navigation, weather forecasting and space tourism.

- The industrial teams that will provide the services will be multinational consortia consisting of most of the current and new builders of space hardware, operators, as well as new service providers (Table 1).

- The initial deployment of satellite constellations will use current launch vehicles, while placing demands on expanded capabilities for multiple launches. Not only will there be full utilization of Titan, Delta and Atlas EELV families, but also Russian, Chinese, Japanese, and multinational consortia vehicles such as Ariane and SeaLaunch (Tables 2-5).

- By the end of the 2010 decade, the replacement market will require smaller vehicles for launches of single or multiple spares. This will provide the basis for initial utilization of smaller two stage to orbit fully reusable vehicles (Table 6). Future reusable projects are being proposed (Table 7).

- Satellite communications using low and medium altitude constellations will provide reliable wide band internet access to the most remote parts of the globe, leading to the evolution of personal communication as well as massive data transfers for business. Synchronous altitude systems will be saturated, and fiberoptic cables will supplement the ever increasing commercial traffic demand (Table 8).

- The surveillance satellite market will evolve fairly rapidly with four or five suppliers providing visible, multi-spectral and SAR images of 1 meter or better quality to commercial customers as well as military customers of many smaller nations interested in their neighbors. Everybody will want to know what is going on the other side of the border. Using space will become a legitimate and uncontestable means of gathering information (Table 9 - Remote Sensing Service Providers and Table 10 - Proposed Remote Sensing Service Providers). Weather information will be continuously demanded, and more accurate, reliable prediction will be commercially available.

- There will be a continuing demand for positioning and timing information with the assurance that the service is provided without threat of interruption. DoD will either find ways of delivering this service to the world reliably, or there will be alternative means provided by commercial enterprises. The argument in favor of providing this capability to the world is the continuous assertion of U.S. presence and primacy; however, the availability of adequate and timely surveillance information, coupled with reliable positioning and timing data from GPS, will give potential enemies unprecedented and relatively cheap weapons targeting capability.

Vulnerabilities

- Given the utilization of distributed constellations, most communication systems are not vulnerable to individual satellite attack, except for an all-out nuclear or space war.
- The ground entry points for the commercial space systems might be vulnerable to terrorist attack, but because of their large proliferation, there appear to be adequate alternate opportunities for entering the communications networks.
- A serious danger exists from the attack of hackers or other terrorist attacks on the software of the systems.
- Since most of the LEO and MEO constellations spend a lot of time crossing the magnetic regions of the Van Allen Belts, the entire constellations may be vulnerable to attack by high altitude nuclear explosions. An explosion of only a few kilotons would create enough trapped radiation to greatly curtail the lifetime of the commercial satellites.

Conclusions

- Point-to-point and broadcast communications and most of the low-resolution surveillance will be available to all at a reasonable price and will be most reliable and uninterruptable because of the very large multinational assets involved.
- The U.S. military will not be a large and important customer for commercial services. The military objective is to "Own the Information Battlefield" while the rest of the world is going on about its business.

Suggestions for DoD

- Select critical functions, which are necessary for U.S. protection and military superiority, and find ways to design and build them in ways to make them as resistant as possible to deliberate or accidental interference.
- Use as much as possible of the commercial systems for the rest and rely on multiple sources and paths to provide statistically adequate availability and reliability.

- Focus DoD developments and acquisition only to accomplish absolutely critical military functions such as:

  - Strategic offense and defense.
  - Defense against biological and chemical weapons.
  - Highly dependable multi-path capability to command and control deployed forces.
  - Jam resistant communications capability for major conflicts in the event that commercial capability becomes disrupted.
  - Jamming architectures and equipment for communications and navigation.
  - High-resolution reconnaissance for technical intelligence collection.
  - Sigint/Masint systems for operational support.
  - Surveillance for missile defense.
  - Moving target detection capability for air and ground targets using a system of air and space systems for local theater operations
  - Surveillance information processing and utilization by commanders in the field capable of receiving data from various sources.
  - Delivery capability of special payloads to space in low orbit when they are needed to control the information battlefield by means of a reusable launch vehicle.
  - Space control with flexibility ranging from denial to destruction of adversary systems.

Table 1 - Telecommunications Market Participants

AeroAstro, LLC, Aerospatiale, Alcatel Telspace, Alenia Spazio SpA, American Mobile Satellite Corporation, Applied Physics Laboratory, Ball Aerospace Systems Group, Boeing Company, Computer Resources International, Daimler Benz Aerospace (DASA), Final Analysis, Inc., Gazkom Joint Stock Company, Great Wall Industry Corporation, Hughes Space and Communications Co., Indian Space Research Organization (ISRO), INPE, Israel Aircraft Industries, Kayser-Threde, Khrunichev State Research and Production Space Centre, Lockheed Martin Corporation, Loral Space & Communications, Los Alamos National Laboratory, Matra Marconi, Mitsubishi Electric Corporation (Melco), Moscow Institute of Thermotechnics, Motorola, Inc., National Aeronautics and Space Administration (NASA), National Space Development Agency of Japan, NEC Corporation, NPO Applied Mechanics, NPO Lavotchkin Vabakin Engineering Research Centre, NPO Yuzhnoye, OHB Systems, Orbital Imaging Corporation, Orbital Sciences Corporation, Polyot, RKK Energia, Shanghai Institute of Satellite Engineering, Spar Aerospace, Spectrum Astro, Swedish Space Corporation, Telespazio, TGI, TRW, Inc., TsNPO Kometa, University of Surrey, and VNII-Elektromekaniki. Related Companies include: Aerospace Corporation, AirTouch Cellular, Alcatel Telecom, Alliant Techsystems, Inc. Defense System, AlliedSignal Aerospace Company, Arianespace, Inc., Bell Atlantic Corporation, COM DEV International, CommQuest Technologies, Inc., Constellation Communications, Inc., Cubic Corporation, Dacom Corporation, European Space Agency, Fokker Space and Systems, France Telecom, Inc., GE Americom, Globalstar, Goddard Space Flight Center, Harris Corporation, Honeywell Incorporated Satellite Systems Division, Hyundai Electronics Industries, Iridium, Inc., ITT Aerospace Communications Division, Jet Propulsion Laboratory, KB Photon, Korea Mobile Telecommunications Corp., Leo One USA Corporation, L3 Communications Conic, MAN Technologies, Mitsubishi Heavy Industries, Ltd. Space Systems Department, Mobile Communications Holdings, Inc. (MCHI), Motorola, Inc. Government & Systems Technology Group, Motorola, Inc., Space & Systems Technology Group, Nagoya University, Nissan Motor Co., Ltd. Aerospace Division, NPO Machinostroenye, Odyssey Telecommunications International, Inc., ORBCOMM, PO Polyot, QUALCOMM, Inc., Rantec Microwave & Electronics, Inc., Raytheon Canada, Rocket System Corporation, Saab Ericsson Space, Sea Launch, Societe Europeenne de Propulsion, Space Imaging EOSAT, SpaceVest, SPOT Image Corporation, Sprint, STET sta Finanziaria telefonica PA, Technical University of Berlin Institute for Aeronautics and Astronautics, Technion Institute of Technology, Teledesic Corporation, Thiokol Corporation, Space Operations Division, Toshiba Corporation, United Technologies Government Engines & Space Propulsion, Universidad Politecnica de Madrid Centro de Investigacin y Dessarrollo Espacial, University of Alabama-Huntsville, University of Colorado-Boulder, and Vodafone Group PLC.

Table 2 - Current U.S. Launch Vehicles

	Atlas IIAS	Conestoga	Delta II (7925)	LMLV-1	LMLV-2	MM II (MSLS)	Pegasus
Country	**USA**	**USA**	**USA**	**USA**	**USA**	**USA**	**USA**
Organization	Lockheed-Martin	SSI, Inc.	Boeing	Lockheed-Martin	Lockheed-Martin	Lockheed-Martin	Orbital Sciences
IOC	Operational	Operational	Operational	Operational	Operational	Operational	Operational
Vehicle	ELV	ELV	ELV	ELV	ELV	ELV	ELV
LEO (lb)	19,050	2,600	11,300	1,750	4,350	300	440
GTO (lb)	7,700	---	4,120	---	---	---	---
Max. Payload Size	13.7' x 39.4'	Ø6.0 x 16.0 ft	10.0' x 26.0'	Ø7.6 x 17.3 ft	Ø9.7 x 22.4 ft	n/a	Ø3.8 x 7.0 ft
Launch Site	CCAS	Wallops Island	CCAS/VAFB	VAFB/CCAS	VAFB/CCAS	VAFB/Kodiak	Air (L-1011)
Latitude/Longitude	28.5°N 80.5°W	37.9°N 75.5°W	28N80W/35N120W	28N80W/35N120 W	28N80W/35N120 W	28N80W/58N52W	Variable
Site Security	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Reliability	100% (11/11)	0% (0/1)	97% (60/62)	50% (1/2)	---	100% (2/2)	100% (8/8)
Throughput	60 days	n/a	40 days	9 days	14 days	30 days	12 days

	Pegasus XL	Scout	Taurus	Titan II	Titan IV	Titan IV-B
Country	**USA**	**USA**	**USA**	**USA**	**USA**	**USA**
Organization	Orbital Sciences	NASA / DoD	Orbital Sciences	Lockheed-Martin	Lockheed-Martin	Lockheed-Martin
IOC	Operational	Operational	Operational	Operational	Operational	Operational
Vehicle	ELV	ELV	ELV	ELV	ELV	ELV
LEO (lb)	600	560	2,450	8,200	39,000	48,000
GTO (lb)	---	---	---	---	14,000	19,000
Max. Payload Size	Ø3.8 x 7.0 ft	Ø3 ft	Ø4.0 x 9.2 ft	10' x 30'	16.7' x 86'	16.7' x 86'
Launch Site	Air (L-1011)	Wallops/VAFB	VAFB	VAFB	CCAS/VAFB	CCAS/VAFB
Latitude/Longitude	Variable	35N120W/38N75 W	34.7°N 120.4°W	34.7°N 120.4°W	28N80W/35N120 W	28N80W/35N120W
Site Security	Medium	Medium	High	High	High	High
Reliability	63% (5/8)	88% (102/116)	---	100% (18/18)	95% (18/19)	100% (2/2)
Throughput	12 days	30 days	8 days	90 days	60 days	60 days

Table 3 - Future U.S. Launch Vehicles

	Atlas III	Delta III	Eagle	EELV (Med.)	EELV (Heavy)	LMLV-3	PA-1	Scorpius	Zenit 3-SL
Country	**USA**	**USA**	**USA**	**USA**	**USA**	**USA**	**USA**	**USA**	**Ukraine/USA**
Organization	Lockheed-Martin	Boeing	E'Prime	DoD	DoD	Lockheed-Martin	PacAstro	Microcosm	Sea Launch, Inc.
IOC	1998	1998	1998	2001	2003	2000	2001	2000	1998
Vehicle	ELV	ELV	ELV	ELV	ELV	ELV	ELV	ELV	ELV
LEO (lb)	n/a	18,280	3,000	17,000	41,000 (Polar)	9,010	100	2,200	---
GTO (lb)	8,700	8,400	---	6,100	8,500	---	---	---	11,576
Max. Payload Size	13.7' x 42.4'	13.1' x 26.0'	Ø9.2 x 9.8 ft	Ø16 x 86 ft	Ø16 x 86 ft	Ø11.7 x 25.6 ft	Ø3.0 x 4.0 ft	n/a	n/a
Launch Site	CCAS	CCAS/VAFB	Ascension Island	VAFB/CCAS	VAFB/CCAS	VAFB/CCAS	VAFB/Wallops	White Sands	Pacific Ocean
Latitude/Longitude	28.5°N 80.5°W	28N80W/35N120W	7.9°S 14.2°W	28N80W/35N120 W	28N80W/35N120 W	28N80W/35N120 W	35N120W/38N75 W	32°N 106°W	≈ 0°N 152°W
Site Security	Medium	Medium	Low	High	High	Medium	High / Medium	Medium	Low
Reliability	---	---	---	---	---	---	---	---	---
Throughput	60 days	n/a	n/a	45 days	90 days	25 days	n/a	8 hours	27

Table 4 - Current Foreign Launch Vehicles

	Ariane 40	Ariane 42L	Ariane 42P	Ariane 44L	Ariane 44LP	Ariane 44P	Ariane 5
Country	**ESA**	**ESA**	**ESA**	**ESA**	**ESA**	**ESA**	**ESA**
Organization	Aerospatiale	Aerospatiale	Aerospatiale	Aerospatiale	Aerospatiale	Aerospatiale	Aerospatiale
IOC	Operational	Operational	Operational	Operational	Operational	Operational	Operational
Vehicle	ELV	ELV	ELV	ELV	ELV	ELV	ELV
LEO (lb)	10,140	15,430	13,230	15,430	15,430	14,330	39,680
GTO (lb)	4,640	7,670	6,460	10,625	9,305	7,640	14,990
Max. Payload Size	2120-3037 ft^3	2120-3037 ft^3	2120-3037 ft^3	2120-3037 ft^3	2120-3037 ft^3	2120-3037 ft^3	Ø15.0 ft
Launch Site	Kourou	Kourou	Kourou	Kourou	Kourou	Kourou	Kourou
Latitude/Longitude	5.2°N 52.8°E	5.2°N 52.8°E	5.2°N 52.8°E	5.2°N 52.8°E	5.2°N 52.8°E	5.2°N 52.8°E	5.2°N 52.8°E
Site Security	High	High	High	High	High	High	High
Reliability	100% (5/5)	100% (8/8)	90% (10/11)	96% (23/24)	94% (15/16)	100% (9/9)	0% (0/1)
Throughput	18 days	18 days	18 days	18 days	18 days	18 days	6 days

	H-2	J-1	M-3SII	M-5	Rokot	Shavit
Country	**Japan**	**Japan**	**Japan**	**Japan**	**Russia/Germany**	**Israel**
Organization	NASDA	ISAS	ISAS	ISAS	Eurokot	IAI
IOC	Operational	Operational	Operational	Operational	Operational	Operational
Vehicle	ELV	ELV	ELV	ELV	ELV	ELV
LEO (lb)	22,000	1,920	1,720	4,400	4,400	344*
GTO (lb)	8,800	—	—	1,765	---	---
Max. Payload Size	Ø15.1 ft	Ø4.6 ft	Ø4.6 ft	Ø7.2 ft	Ø14.3 x 26 ft	n/a
Launch Site	Tanegashima	Tanegashima	Kagoshima	Kagoshima	Tyuratam Silo	Palmachim
Latitude/Longitude	30.4°N 131.0°E	30.4°N 131.0°E	31.2°N 131.1°E	31.2°N 131.1°E	63.0°E 45.2°N	31.9°N 34.8°E
Site Security	High	High	High	High	High	High
Reliability	100% (4/4)	100% (1/1)	88% (7/8)	100% (1/1)	100% (1/1)	100% (3/3)
Throughput	≈ 45 days	≈ 30 days	≈ 30 days	≈ 30 days	n/a	n/a

Table 4 cont'd - Current Foreign Launch Vehicles

	Cosmos	Molniya	Proton (D1/SL13)	Proton(D1e/SL13)	Soyuz	Start	Volna	SS-18	Tsyklon 2	Tsyklon 3
Country	**Russia**	**Russia**	**Russia**	**Russia**	**Russia**	**Russia**	**Russia**	**Ukraine**	**Ukraine**	**Ukraine**
Organization	NPO Polyot	TsSKB	NPO Krunichev	NPO Krunichev	TsSKB	STC Komplex	K.B. Makeyev	Yuzhkosmos	NPO Yuzhnoye	NPO Yuzhnoye
IOC	Operational	Operational	Operational	Operational	Operational	Operational	Operational	Operational	Operational	Operational
Vehicle	ELV	ELV	ELV	ELV	ELV	ELV	ELV	ELV	ELV	ELV
LEO (lb)	3,000	4,500	46,000	---	15,400	1,420	250	9,700	6,200	7,900
GTO (lb)	---	---	---	10,584	---	---	---	7,700	---	---
Max. Payload Size	Ø5.9 x 7.9 ft	Ø8.7 x 12.1 ft	Ø13.5 x 52.1 ft	Ø14.3 x 26 ft	Ø7.7 x 29.5 ft	Ø5.9 ft	45.8 ft^3	Ø9.9 x 17.4 ft	7' x 46.4'	8.9' x 31.3 ft
Launch Site	Plesetsk	Plesetsk	Baikonur	Baikonur	Plesetsk/Baikonur	Plesetsk	Submarine	Baikonur	Baikonur	Baikonur
Latitude/Longitude	40.1°E 62.8°N	40.1°E 62.8°N	63.3°E 45.9°N	63.3°E 45.9°N	40E 63N/63E 46N	40.1°E 62.8°N	Variable	63.3°E 45.9°N	63.3°E 45.9°N	63.3°E 45.9°N
Site Security	High	High	High	High	High	High	High	High	High	High
Reliability	96% (403/421)	88% (273/296)	89% (24/27)	89% (24/27)	97% (1041/1075)	67% (2/3)	100% (1/1)	100% (1/1)	98% (121/123)	99% (110/111)
Throughput	15 hours	6 days	15 days	15 days	6 days	n/a	n/a	n/a	3 days	3 days

	Zenit 2	LM-1D	LM-2C	LM-2E	LM-3	LM-3A	LM-3B	LM-4	PSLV	VLS
Country	**Ukraine**	**China**	**China**	**China**	**China**	**China**	**China**	**China**	**India**	**Brazil**
Organization	NPO Yuzhnoye	China Great Wall	China Great Wall	China Great Wall	China Great Wall	China Great Wall	China Great Wall	China Great Wall	ISRO	CTA
IOC	Operational	Operational	Operational	Operational	Operational	Operational	Operational	Operational	Operational	Operational
Vehicle	ELV	ELV	ELV	ELV	ELV	ELV	ELV	ELV	ELV	ELV
LEO (lb)	30,300	1,590	7,040	20,240	11,000	15,840	29,900	8,800	6,614	441
GTO (lb)	---	440	2,200	7,430	3,100	5,500	9,900	2,430	992	---
Max. Payload Size	12.8' x 44.8'	6.7' x 13.1'	7.2' x 10.3'	13.8' x 39.2'	9.8' x 23.9' dual	13.1' x 39.4' dual	Ø13.8 ft	11' x 27.8'	Ø9.5 ft	3.9' x 3.9'
Launch Site	Baikonur	Jiuquan	Jiuquan	Xichang	Xichang	Xichang	Xichang	Taiyuan	SHAR Ctr.	Alcântara
Latitude/Longitude	63.3°E 45.9°N	40.6°N 99.9°E	40.6°N 99.9°E	28°N 102°E	28°N 102°E	28°N 102°E	28°N 102°E	37.5°N 112.6°E	13.7°N 80.2°E	2.3°S 44.7°E
Site Security	High	Medium	Medium	Medium	Medium	Medium	Medium	Medium	High	Medium
Reliability	87% (26/30)	---	100% (14/14)	67% (6/7)	75% (9/12)	100% (3/3)	50% (1/2)	100% (2/2)	75% (3/4)	0% (0/1)
Throughput	16 days	n/a	n/a	30 days	30 days	30 days	n/a	n/a	55 days	n/a

Table 5 - Future Foreign Launch Vehicles

	Angara	Rikscha	Shtil -1N	Shtil - 3A	Vysota	Space Clipper
Country	**Russia**	**Russia**	**Russia**	**Russia**	**Russia**	**Ukraine**
Organization	NPO Krunichev	K.B. Makeyev	K.B. Makeyev	K.B. Makeyev	K.B. Makeyev	NPO Yuzhnoye
IOC	2002	2000	1998	1998	1998	1998
Vehicle	ELV	ELV	ELV	ELV	ELV	ELV
LEO (lb)	57,200	3,750	948	2,094	250	5,000
GTO (lb)	---	---	---	---	---	---
Max. Payload Size	Ø16.4 x 73.8 ft	n/a	52.9 ft^3	127 ft^3	24.7 ft^3	Ø7.0 x 15.7 ft
Launch Site	Plesetsk	Submarine	Plesetsk	Air (An-124)	Submarine	Air (An-124)
Latitude/Longitude	40.1°E 62.8°N	Variable	40.1°E 62.8°N	Variable	Variable	Variable
Site Security	High	High	High	Medium	High	Medium
Reliability	---	---	---	---	---	---
Throughput	n/a	n/a	n/a	n/a	n/a	n/a

	GSLV	E-4	Capricornio	Vega K-0	Vega K-3	H-2A
Country	**India**	**France**	**Spain**	**Italy**	**Italy**	**Japan**
Organization	ISRO	Aerospatiale	INTA	BPD Defense	BPD Defense	NASDA
IOC	1998	2002	1999	1999	1999	2000
Vehicle	ELV	ELV	ELV	ELV	ELV	ELV
LEO (lb)	11,023	700	310	750	1,450	22,050
GTO (lb)	5,512	---	---	---	---	8,800
Max. Payload Size	Ø10.1 ft	n/a	Ø2.9 ft	n/a	n/a	Ø13.1 ft
Launch Site	SHAR Ctr.	Kourou	Canary Islands	San Marco	San Marco	Tanegashima
Latitude/Longitude	13.7°N 80.2°E	5.2°N 52.8°E	28°N 15°W	2.9°S 40.3°E	2.9°S 40.3°E	30.4°N 131.0°E
Site Security	High	High	Medium	Medium	Medium	High
Reliability	---	---	---	---	---	---
Throughput	»45 days	n/a	n/a	n/a	n/a	n/a

Table 6 - Planned Reusable Launch Vehicles

Company or Country	Vehicle	Configuration	Payload to LEO in pounds	First Scheduled Launch
Kistler Aerospace	K-1	Two Stage To Orbit	11,000	?
Rotary Rocket	Roton	Single Stage To Orbit	7,000	?
Pioneer Rocketplane	Pathfinder	TSTO	5,500	2001
Kelly Space	Astronliner	TSTO	9,000	2001-2002
Space Access	SA-1	TSTO or three stage to GTO	[proprietary]	2001-2002
Lockheed Martin	VentureStar	SSTO	50,000	2004-2005?
Japan	HOPE-X	TSTO	?	2001?

Table 7 - Other Proposed Reusable Space Vehicles

1. Boeing Reusable Space Vehicle [based on DC-XA]
2. X-33 as first stage RLV, Lockheed Martin
3. Pegasus follow-on [based on X-34], Orbital Sciences
4. Liquid Fly Back Booster [Space Shuttle upgrade]
5. Hyper-X and future airbreathing or Future-X vehicles, NASA
6. Space Maneuver Vehicle, X-40 (DoD) [upper stage]
7. Crew Return Vehicle (from X-38 program) [return only from space station], NASA
8. Crew Transfer Vehicle (Europe) [ascent and return, based on Crew Return Vehicle]
9. FESTIP configuration (Europe) [study concluded 1996, further study planned)
10. HOTOL (Great Britain)
11. Sanger (Germany)
12. HOPE-XA [based on HOPE-X, launched by H-2A]
13. Japan RLV [long range plan]
14. MAKS (Russia)
15. Mig-31 as first stage (Russia)
16. Other Russian proposals
17. Zegrahm Space Voyages Inc., Space Cruiser, TSTO, Aero Astro and Vela Inc.
18. Space America Inc., TSTO
19. Military Space Plane (DoD), SSTO? TSTO?

20-36. X-Prize entrants [three entrants also have commercial RLVs]

Table 8 – Planned Communications Projects

Name	Operator	Prime Contractor	Orbit	Capability	Operational satellites plus on-orbit spares
COURIER	Elas Courier Complex	NPO Elas	700 km, 76 deg	UHF	8 + 0
ECCO	Constellation Communications	Matra Marconi Space	2,000 km, 0/62 deg	L-band	46 + 7
ELLIPSO Borealis	Ellipsat (MCHI)	Spectrum Astro	520 x 7846 km, 116 deg	L-band	8 + 2
ELLIPSO Concordia	Ellipsat (MCHI)	Spectrum Astro	8,060 km, 0 deg	L-band	6 + 1
FAISAT	Final Analysis Comm.	Final Analysis Inc.	1,000 km, 83 deg	VHF/UHF	26 + 0
GLOBALSTAR	Globalstar LP	Space Systems / Loral	1,414 km, 52 deg	L/S-band	48 + 8
GONETS D/ R	Smolsat	AKO Polyot	1,400 km, 82.6 deg	UHF and S/L-band	81 + 0
ICO	ICO Global Comm	Hughes	10,355 km, 45 deg	S-band	10 + 2
IRIDIUM	Iridium LLC	Motorola	780 km, 86.4 deg	L/S-band	66 + 6
IRIS (LLMS)	SAIT Systemes	OHB System	1,000 km, 83 deg	UHF	2 + 0
LEO ONE USA	LEO One USA	TBD	950 km, 50 deg	VHF	48 + 0
M-STAR	Motorola	Motorola	1,350 km, 47 deg	Ka-band	72 + 0
ORBCOMM	ORBCOMM	Orbital Sciences Corp.	785 km, 45 / 70 deg	VHF/UHF	28 + 0
SAFIR	OHB Teledata	OHB System	680 km, 98 deg	UHF	6 + 0
SIGNAL	RKK Energiya	RKK Energiya	1,600 km, 74 deg	L-band	48 + 0
SKYBRIDGE	Skybridge	Alcatel	1,457 km, 55 deg	Ku-band	64 + 4
TELEDESIC	Teledesic Corp	Motorola	1,357 km, 85 deg	Ka-band	288 + 12
TEMISAT	Telespazio	Kayser-Threde	938 km, 82 deg	UHF	7 + 0
VITASAT	Volunteers in Tech. Assistance	Various	1,000 km, 83 deg	VHF/UHF	3 + 0
WEST	Matra Marconi Space	Matra Marconi Space	10,000 km	Ka-band	9 + 0

L, S bands: Telephony; VHF / UHF: Messaging; Ka, Ku-bands: Broadband communications

Table 9 - Remote Sensing Service Providers

Satellite	Data Provider / Prime Contractor, Country of Contractor	Launch date	Panchromatic Resolution in meters /swath width in km	Multispectral Resolution in meters /swath width in km	Radar Res. m /swath width km	Repeat Cycle in Days
Landsat 5	Space Imaging EOSAT/Lockheed Martin (GE), U.S.	March 1984	-	30-80 / 185	-	16
SPOT 1	SPOT Image /Matra-Espace, France	Feb 1986	10	20	-	26
SPOT 2	SPOT Image /Matra-Espace, France	Jan 1990	10	20	-	26
SPOT 4	SPOT Image / Matra Marconi Space, France and United Kingdom	March 1998	10	20	-	26
ERS-1	Eurimage (multiple European companies) /Dornier, Germany	July 1991	-	-	26 / 102	168
ERS-2	Eurimage	April 1995	-	-	26 / 102	35
IRS-1B	Space Imaging EOSAT/ISRO, India	August 1991	-	36.25 - 72.5 / 148	-	22
IRS-P2	Space Imaging EOSAT/ ISRO, India	Oct 1994	-	36.25 / 131	-	22
IRS-1C	Space Imaging EOSAT/ISRO, India	Dec 1995	5.8 / 70	23.5 - 70.5 / 142	-	24
IRS-1D	Space Imaging, EOSAT/ISRO, India		5.8 / 70	23.5 - 70.5 / 142	-	24
RADARSAT 1	Radarsat International / Space Aerospace, Canada	Nov 1995	-	-	7.6 - 100 / 50-500	24
Kosmos 2349	Russia and SPIN-2, U.S.	Feb 1998 [reentered April '98]	2-10 / 165-300	-	-	-

Table 10 - Proposed Commercial & Civil Remote Sensing Satellites (1 of 2)

Satellite	Data Provider /Prime Contractor, Country of Contractor	Scheduled Launch	Panchromatic Resolution in meters / swath width in km	Multispectral Resolution in meters /swath width in km	Radar Res. m /swath km	Repeat Cycle in Days
CBERS-1 (Zi Yuan 1)	TBD /China Aerospace Corp and INPE, Brazil	mid-1998	20 / 120	20-160 / 120	-	26
Ikonos 1 [failure]	Space Imaging EOSAT / Lockheed Martin, U.S.	April 1999	1 / 11	4 / 11	-	11
Ikonos 2 [on-orbit]	Space Imaging EOSAT /Lockheed Martin, U.S.	Sept 1999	1 / 11	4 / 11	-	11
Landsat 7 [on-orbit]	Space Imaging EOSAT /Lockheed Martin U.S.	April 1999	15 / 185	30-60 / 185	-	16
EarlyBird 2 [cancelled Ap '98]	EarthWatch, Ball Aerospace	mid-1999	3 / 6	15 / 30	-	not available
CartoSat 1	Space Imaging EOSAT? /ISRO, India	June 1999	2.5 / 30	10 / 40	-	26
QuickBird 1	EarthWatch / Ball Aerospace, U.S.	mid-1999	0.8 / 21	4.5 / 21	-	not available
Kompsat 1	TBD (KARI, South Korea) / TRW, U.S.	1999	10 / 40	20 / 40	-	not available
OrbView 3	OrbImage / Orbital Sciences, U.S.	1999	1-2 / 4-8	4 / 8	-	@ 3
Ofek 5 (EROS)	Israel Aircraft Industries (IAI) and Core Software/ IAI (MBT Systems), Israel	June 2000	TBD	10 / 40	-	not available
ResourseSat1	Space Imaging EOSAT? / ISRO, India	June 2000	TBD	10 / 40	-	22
GDE	GDE	TBD	2000	1 / 15	-	16
Nemo	TBD (U.S. Navy) / Space Systems Loral, U.S.	2000	-	not available	-	not available
Orbview 4	OrbImage / Orbital Sciences, U.S.	2000	1-2 / 4-8	4 /8	-	@ 3
Resource 21	Resource 21 /Boeing, U.S.	2000	-	10-20 / 205	-	7 (4 days for 4 sats)
Aries 1	Acres / TBD	2000?	TBD	TBD	-	TBD

Table 10 Cont'd - Proposed Commercial & Civil Remote Sensing Satellites (2 of 2)

IRS-2A	Space Imaging EOSAT /ISRO, India	2000?	5-10 / 70	23.5-70.5 / 142	-	24
QuickBird 2	EarthWatch /Ball Aerospace, U.S.	2000?	0.8 / 21	4.5 / 21	-	1
SkyMed/ Cosmo	TBD (Italian Space Agency- ASI) / Alenia Spazio, Italy	2001	1-2.5 / 15	5 / 15	3 / 23-43	5 (w/ 7 satellites)
RADARSAT 2	McDonald Dettwiler /McDonald Dettwiler, Canada	March 2001	-	-	3-100 /10-500	24
SSR-1	TBD (INPE Brazil) / TBD	2001	-	100-300 /2,200	-	not available
LightSAR	TBD (NASA) /TBD	2001?	-	-	?	not available
SPOT 5	SPOT Image / Matra Marconi, France and United Kingdom	late 2001	2.5-5 /117	10 /117	-	26
Ikonos 3	Space Imaging EOSAT /Lockheed Martin, U.S.	2002	1 /11	4 / 11	-	11
3S	SPOT Image/ Aerospatiale?, France	late 2002	2-2.5 / 40	TBD	-	13
Alos 1	TBD (NASDA) /NASDA, Japan)	Jan 2003	2.5 /35	10 / 70	10-100 /70-360	45
ResourceSat 2	Space Imaging EOSAT? /ISRO, India	June 2003	TBD	TBD	-	22?
CartoSat 2	Space Imaging EOSAT? /ISRO, India	2003	TBD	TBD	-	26?
SSR-2	TBD (INPE)/ INPE, Brazil	2003	-	100-300 /2,200	-	not available
IRS-3	Space Imaging EOSAT /ISRO, India	2005	TBD	TBD	-	24?
David	OHB System (Germany) and GAF (Germany) /OHB and El-Op, Israel	TBD	-	5 / 30	-	not available
SAC-C	TBD (CONAE, Argentina) / Invap, Argentina	TBD	-	150 / 315	-	9

Note: Does not include weather or military remote sensing satellites.

Organizational abbreviations:

- **CONAE** Comision Nacional de Actividades Espaciales (Argentina)
- **ESA** European Space Agency
- **GAF** Gesellschaft fur Angewandte Fernerkundung mbH (Germany)
- **INPE** Instituto Nacional de Pesquisas Espaciais (Brazil)
- **ISRO** Indian Space Research Organization
- **KARI** Korean Aerospace Research Institute (South Korea)
- **NASDA** National Space Development Agency (Japan)

Sources: International Space Industry Report (Launchspace Magazine), April 9, 1998, p. 18 and ANSER research, April 1998.

Annex VI

Maintaining Military Dominance amidst Globalization through the Preservation of Essential Military Capabilities

Introduction

The ability of the United States to field superior defense capabilities has been a major strength— a critical component of the success of U.S. foreign policy. Today's professional military forces reflect five decades of broad political support, substantial financial resources, cutting-edge technology and outstanding human talent. DoD's investments in research and development and systems development and integration have produced technically capable weapons unmatched by any other military force. DoD's capabilities in intelligence, surveillance, reconnaissance, command, control, and computer and communication skills dominate. Moreover, the armed forces have learned how to maintain a level of training in combat skills that is unmatched as well.

The globalization of modern technology makes sustaining military superiority a more difficult task. The United States is facing a security environment with new threats and new risks that are individually and collectively difficult and challenging. Many enabling technologies, important to military capabilities, are no longer unique to the military. Instead, they are increasingly available on the commercial market worldwide. *This global leveling makes it possible for an adversary with a relatively small budget to field "good enough" military capabilities not available to them in the past without substantial resources and/or industrial capability.*

While the United States still maintains a formidable advantage, the rapid pace of development in advanced commercial technology and its potential to produce powerful military capabilities will increasingly challenge U.S. military superiority. To maintain its edge, DoD must go beyond the current approach that focuses primarily on "developing advanced technology for military applications" and "protecting lists of critical technologies." Moreover, the reduction in the DoD procurement budget, plus lower independent research and development expenditures in industry, call for a strategy that embraces a broader approach.

A Strategic Approach

A new approach to sustaining military superiority is based on maintaining and enhancing essential military capabilities rather than the individual technologies from which they are built. Thus, the Department needs to establish a process to: 1) identify essential military capabilities and 2) develop a tailored strategy for preserving and enhancing these capabilities well into the future.

An important element of strategy must be the recognition that the U.S. defense posture depends on relationships with allies. Future military operations and military preparedness will most likely be conducted in the context of coalition operations. This does not imply that the United States should or will not maintain a unilateral capability.

The Task Force did not attempt to determine the wisdom, affordability or likelihood of the U.S. maintaining a unilateral capability across the operational spectrum. That said, the Task Force does believe the United States can achieve a greater set of objectives with fewer resources by collaborating—developmentally and operationally—with allies and friends. Moreover, embracing the benefits of globalization can reinforce alliance-building goals as well.

Identifying Essential Military Capabilities. The Task Force sets forth a set of essential military capabilities that the U.S. would need to maintain and enhance well into the future. The emphasis, in developing this set, was on the essentiality of the capability in the future security environment, rather than on the comprehensiveness of the list.[10]

Essential Combat Capabilities

1. Nuclear Weapons
2. Project and Sustain Military Forces Worldwide in a Timely, Efficient and Protected Manner
3. Global Capability for Intelligence, Surveillance and Reconnaissance
4. Counters to Biological and Chemical Weapons
5. Computer-based Command and Control of Forces, Logistics, and Information
6. Precision Fires, Particularly at Long Range

[10] Note on Composition and Order of the List:
Some readers may wonder why the Military Superiority Panel listed "Systems Integration Processes" as an essential military capability. To be sure, it does not fall into place entirely easily. But the Panel chose to include it after examining Joint Vision 2010, the recent doctrinal statements of the Services issued contemporaneously with Joint Vision 2010, and our own appraisal of what makes a difference in military application of the current explosion in information technologies. The Panel concluded that the U.S. ability to apply system integration to the design, manufacture, training and use of military equipment represents an essential military capability for U.S. national security. To some, this is known as employing "systems of systems," a term we chose not to use since it appears to presume that systems integration is only a "plug and play" matter, whereas the Panel sees systems integration as a much richer endeavor.

Other readers may wonder why the Panel listed nuclear weapons at a time when many advocate and all observe that our reliance on nuclear weapons is diminishing. One reason is the panel's conviction that nuclear weapons will remain an essential military capability for the foreseeable future, particularly should we come to face a "peer competitor." A second reason is to describe the rather elaborate strategy that has been established and implemented to preserve and enhance the U.S. military capability in nuclear weapons in the face of globalization (nuclear weapons proliferation) and commercialization (nuclear power generation).

As to the order of the list, the panel chose to place nuclear weapons first because many elements of the strategy for preserving nuclear weapons have analogs and extensions useful for strategies for other essential military capabilities. Many elements of the preservation strategy for nuclear weapons are not known outside of the nuclear weapons community. Similarly, the Panel listed systems engineering processes last, in order to discuss that strategy after all the others.

7. Maneuver for Land, Sea, Air and Space Forces in the Face of Determined, Clever Opposition
8. Protection of the U.S. Homeland from Direct Attack
9. Essential Enabling Capabilities:
   - Robust Technology and Development Institutions and Processes.
   - Realistic Training for Combat and Related Military Activities
   - Systems Integration Processes

These capabilities are aimed at a middle ground of aggregation and allow for different levels of aggregation from capability to capability. This set of capabilities also illuminates various decision opportunities open to the Department. Strategies to preserve these capabilities involve taking advantage of the opportunities afforded by globalization and commercialization to enhance the military aspects of national security as well as identifying actions to mitigate or avoid deleterious impacts of globalization.

To improve the ability of the Department to address the problem, DoD should structure an iterative process between the warfighter, the Services and Agencies, and industry to match needed operational capabilities with the possibilities technology makes available. This process would identify essential capabilities and develop tailored strategies to address each capability. In addition, this on-going process would focus on specific elements of each strategy including exploiting commercial products and services and identifying vulnerabilities, as described below. The value of an institutionalized process is that it provides an ongoing mechanism to revisit these issues as they change in today's dynamic international environment.

Developing a Tailored Strategy. The Task Force recommends that each segment of essential military capability be addressed with a strategy developed from four mutually supporting elements. Each element contributes to the success of the strategy, but none is sufficient without the other components.

- Direct enhancement. Strengthen essential military capabilities through modernization and effective tactical employment in both joint and coalition contexts.

- Exploit commercial products and services. Identify and advocate, exploit, stimulate, and adapt commercial and global sources for defense products and services. Such efforts should include efforts to mitigate the risks of unauthorized disclosure of the capabilities derived from these technologies.

- Identify Vulnerabilities. Identify vulnerabilities, especially those arising from globalization and commercialization, to enable DoD to minimize the risk of incorporating commercial technologies in its systems and "systems of systems." Institutionalization of adversary analysis is no less important than the institutionalization of advocacy for commercialization.

- Protect Defense-Related Technology. Protecting defense-related technology or knowledge from compromise or hostile exploitation will remain an important element

of preserving military capabilities. Straightforward control of technology with military application is no longer a sufficient or practical approach. Rather, a process to mitigate risk by balancing cost, reward, and effectiveness is more appropriate. The approach to protection needs to be narrowed to focus only on the most important technologies or knowledge.

How the elements of this strategy are applied will differ for different capabilities. Some capabilities will be preserved best by "direct enhancement" rather than relying unduly on "protection" of current capabilities. In many cases, the opportunities for protecting current capabilities from compromise are not robust or attractive—they are too expensive, impractical, or ineffective. In other cases, exploiting commercial products and services or building up certain industrial capabilities, either in the United States or abroad, will allow the Department to achieve the greatest capability. Most strategies will rely on developing all four elements to some extent, and need to consider cost-benefit tradeoffs.

What is most important is that each strategy will lead to a set of actions that the Department will pursue to maintain each essential capability— investments decisions in research, development, and modernization, technology strategies, industrial strategies, coalition strategies, diplomatic actions, and others. The value of this approach is that it is based on a disciplined process that leads to a coherent set of actions that support DoD's geopolitical goals as defined in Departmental strategy and guidance. In essence, this set of actions becomes a business strategy for maintaining essential military capabilities.

Conclusions

To maintain military superiority in an environment of globalization, the Task Force concludes:

- DoD should develop strategies for maintaining essential military capabilities that emphasize direct enhancement of military capabilities and coalition relationships over technology protection as the preferred approach to sustaining U.S. military superiority. Concurrently, DoD should make necessary protective measures more effective.
- The Department should establish a permanent process for identifying essential military capabilities consistent with U.S. military strategy, developing strategies for maintaining these capabilities, and identifying vulnerabilities. DoD should structure an iterative process between the warfighter, the Services and Agencies, and industry to match needed operational capabilities with the possibilities technology makes available.
- The revolution in military affairs, as embodied in Joint Vision 2010, and the explosion of modern sensors and other information technology that enables this revolution, open up new opportunities to bridge the tension between opposing desires for collaboration and protection. For example, most modern munitions, maneuver platforms, and operational units will be much more effective when coupled to the U.S. C3ISR base than when cut off from it. This creates the opportunity to influence

the military capabilities of countries to which the U.S. has transferred equipment and training well after the transfer has been made.

- Much of the impetus for controlling the transfer of military goods, services, and information across national boundaries rests on U.S. foreign policy goals of enhancing regional stability and building a strong base of common security interests. There are national security considerations here as well, but the following strategies for enhancing and maintaining essential military capabilities do not rely very heavily on restricting the export of U.S. military goods and services. Moreover, these strategies do not rely on protecting large amounts of military information, but rather identified a few, very specific matters worth protecting. These very specific matters, in turn, were deemed worthy of reasonably expensive measures for protection, measures that are too expensive and cumbersome to be applied to a large amount of information spread widely throughout the military establishment.

Strategies for Preserving and Enhancing Essential Military Capabilities

The discussion that follows presents a set of strategies for preserving and enhancing the essential military capabilities identified by the Task Force. Each capability is described, and opportunities for fruitful use of globalization and commercialization are identified. These involve exploiting existing capabilities, stimulating the non-defense world to provide more useful capabilities and adapting current military equipment, doctrine, and practices to better use global and commercial sources. The discussion also highlights risks inherent in the strategies and the risk that will be run whether or not the strategy is undertaken.

1. Nuclear Weapons Design, Production, Safety and Employment

President Clinton has described U.S. nuclear weapons as a "supreme national interest." This recognition ratifies a half-century of leadership appreciation of the need to sustain a superior national posture. The U.S. interest in nuclear weapons endures despite the collapse of the former Soviet Union. The globalization of nuclear weapons and other weapons of mass destruction (WMD) through the process of proliferation has reinforced the importance of a highly effective and responsive deterrent. Unlike other aspects of globalization, the process of globalization associated with WMD undermines U.S. interests. The diplomatic arrangements (e.g. the Nuclear Non-Proliferation Treaty, restrictions on nuclear testing, Chemical Weapons Convention, and Biological Weapons Conventions) have been insufficient to prevent the globalization of WMD capabilities.

2. The Ability to Project and Sustain Military Forces Worldwide in a Timely, Protected Manner

The projection of military power was a crucial military capability throughout the Cold War. U.S. military power was used to support U.S. diplomacy by confronting challenges to national interests at their source. The projection of power must be timely and effective in performing its intended mission. Forces projected into a theater of operations must be sufficiently equipped to be well-protected from efforts to prevent their insertion or to dislodge early-arriving forces. Some power projection events have taken place in the

theater or operations where the U.S. has existing treaty commitments and associated deployed forces. However, in many instances, power projection is required with little warning to areas where no local infrastructure exists.

The advent of advanced technology in the commercial sector can leverage U.S. power projection capabilities. Exploitation of commercial aviation sector's vast and expanding capacity to move materiel can leverage specialized military capabilities in theater airlift and the movement of outsized cargoes and the insertion and support for military forces into contested areas. Similarly, the exploitation of advanced commercial propulsion for logistics vehicles and the use of "Federal Express-like" support for deployed forces can reinforce the trends in precision strike systems that are diminishing the logistics demands of power projection. The integrated effect of the vigorous prosecution (supported by institutionalized Red/Gold teams) of the opportunities created by advanced technologies will further diminish the tactical footprint and vulnerability of forward deployed forces.

3. Global Intelligence, Surveillance, and Reconnaissance

Global intelligence, surveillance, and reconnaissance (ISR) includes a vast set of technologies and capabilities. The capability produced by a high performance ISR provides the U.S. armed forces with the opportunity to conduct military operations within the decision processes of its adversaries. The situational awareness provided by global ISR tightens the coupling between diplomacy and military power, and enhances the effectiveness of both.

The process of globalization has a number of consequences for U.S. superiority in Global ISR. Many of the core developments pertinent to ISR superiority—optics, signal processing, sensors, materials, computation, and telecommunications—are largely in the commercial domain. While the absolute performance of U.S. ISR remains at a high level and is unmatched for its comprehensiveness, many "good enough" capabilities are available on the international market to allies and adversaries alike. This factor diminishes the relative advantage in ISR the U.S. is likely to have over potential adversaries in the future.

The readiness of the U.S to share access to its ISR has been a central ingredient in its ability to develop a diplomatic consensus for concerted coalition action, and to facilitate effective coalition military operations. Future U.S. capability to exploit its ISR superiority and degrade those of its adversaries will be an important diplomatic and military challenge in the future. It may be the case that the ability of the U.S. to integrate its ISR capabilities in a "system of systems" sense to strike systems and maneuver forces may be at the heart of an ability to sustain the unique diplomatic and military properties of U.S. global ISR. The ability to transfer target information from an ISR sensor (or system of sensors) to a weapon system seeker may be a competitive discriminator for U.S. ISR. Sustaining alliance cohesion by making this available to allied platforms/weapon systems on an exclusive basis, analogous to the manner in which the U.S. has shared signals intelligence in the past.

4. Defenses against Chemical and Biological Weapons

The need for chemical and biological defense extends far beyond the immediate need to protect forward deployed forces from chemical and biological weapons attack. The characteristics of biological weapons make them particularly well-suited to attacks—overt and covert—against U.S. interests at every level. The underlying knowledge of agents and weapon effectiveness are largely in the commercial and scientific-industrial domain. The U.S. does not intend to use either lethal chemical or biological agents as weapons of war. As a result, it has a profound interest in increasing deterrence of the threat or use of chemical and biological weapons. An important dimension of a deterrent posture is the proliferation of countermeasures to chemical and biological weapons. Ready worldwide access to chemical and biological weapons countermeasures will devalue adversary investment in these types of weapon systems, and diminish their appeal as a diplomatic or military instrument.

The capabilities needed to address the creation of chemical and biological weapons defense are largely in the commercial sector. This arena is a particularly promising one for collaborative multinational arrangements. Indeed, an intra-alliance initiative to develop chemical and biological weapons countermeasures could draw on a deep reservoir of support based on widespread rejection of these weapons by the international community.

5. Computer-based Command and Control of Military Forces, Logistics Support, and Information

Highly effective computer-based command and control of all engaged elements of the U.S. defense establishment is indispensable to exploit the full potential of U.S. military capabilities. The underlying technology is largely in the commercial sector. The risks inherent in using commercial hardware and software are most acute in the command and control arena. The sources of supply for such technology are global. Basic software such as the Windows NT operating system, for example, has a large fraction of its 23 million lines of code written abroad. It is not feasible to vet the software for malicious code, nor is it a simple matter to prevent grave damage from trusted insiders. These risks are inherent given the inability to develop system-wide software and hardware that is unique (and hence, controllable) by the Department of Defense.

In this environment, the need to undertake appropriate risk mitigation measures is urgent. It is not feasible to protect all DoD computer hardware and software; protecting mission-critical systems is the most practical approach to risk mitigation. This approach to risk mitigation can be derived from models created in the protection of special knowledge and access in the U.S. nuclear weapons program and associated nuclear delivery systems. A "performance-based trustworthiness" regime derived from the "nuclear surety" program used by the armed services offers some useful guidance about the development and management of a suitable risk mitigation measure.

A parallel to a "performance-based trustworthiness" program for personnel is a "trusted factories" initiative for essential hardware. Use of field-programmable gate arrays, for example, enhances the probability of uncorrupted hardware. While this hardware will be more costly than its commercial counterparts, focusing its use on mission-critical applications will render it affordable.

Establishing levels of trustworthiness for software access can also be employed, based upon the processes to write the software. Such an approach has been widely used in U.S. nuclear programs to produce nuclear-certified software. This scheme has a useful parallel to the commercial "levels of reliability" for software development established by the Software Engineering Institute. Critical systems requiring the highest levels of trustworthiness will necessitate very costly micro-code development on unique hardware platforms. As the level of required trustworthiness declines, greater reliance can be placed on commercial software, development tools, and operating systems.

6. Long-Range Precision Strike

The technology is now available to make weapon delivery accuracy independent of range. The effectiveness of systems so equipped has a crucial dependence on U.S. global C3ISR. The underlying technologies are largely in the commercial arena, but augment crucial military-unique capabilities such as advanced conventional payloads.

Precision strike systems development offers an opportunity to strengthen alliance cooperation. Propagating long-range precision strike (LRPS) systems among U.S. allies creates an opportunity to assure the availability of munitions with equal effectiveness, thereby enhancing the effectiveness of alliance coalition warfare. Such weapon systems would be useful in an autonomous mode by individual U.S. allies, but the systems' effectiveness could be magnified by engineering options from the U.S. for their interface to the U.S. global ISR system.

From the U.S. perspective, a capability to strike with a high order of precision throughout the depth of a theater of operations remains an essential characteristic of an effective power projection capability. The U.S. capability to do so exploits universally available commercial technology (e.g., GPS). As a result, it is essential to leverage the U.S. leadership in unique military capabilities such as small turbofan engines, advanced conventional warheads, and sophisticated countermeasures to adversary defense systems. The manner in which this capability is improved should be protected to mitigate the consequences of dependence on commercial technology.

To employ LRPS, precision target-acquisition systems, tightly coupled to U.S. Global ISR (to which precision target-acquisition systems are closely related but from which they are distinctly different), are essential. Precision target-acquisition requires timely and reliable target detection, identification, location, and estimate of target vulnerability as deployed. Precision strikes delivered to the wrong targets may create more damage in coalition warfare than having not fired at all. An additional and extremely important function of precision target acquisition is timely, accurate post strike damage assessment. Wartime implementation of precision target-acquisition must be architecturally compatible with the chosen forms of weapon guidance, weapon types (particularly for loitering weapons), and the overall conduct and character of the operation.

7. Maneuver for Land, Sea, Air, and Space Forces in the Face of Determined and Sophisticated Adversaries

The ability of the U.S. to exploit its capabilities in global ISR and precision strike require an ability to maneuver effectively to achieve the classical military objectives of the concentration and economy of force, and to minimize vulnerability to counterattack. The need to maneuver effectively applies with equal intensity to all environments where military conflict takes place.

Effective maneuver requires an appropriate mix of platforms and ISR systems to support fire and maneuver operations as well as countermeasures and active defense to limit vulnerability. The ability of the U.S. to operate freely is at risk due to the proliferation of ISR technologies derived from commercial sources. Unique military technologies are a potential source for effective countermeasures and active defense to protect the ability of U.S. (and in some circumstances, allied forces as well) to maneuver in support of military operations.

The proliferation of technologies associated with entry to space is a particularly worrisome characteristic of globalization. Space-based capabilities provide opportunities for asymmetric responses (e.g., ASATs, EMP attacks, etc.) to U.S. military power that may be difficult and costly to offset or contest.

The need to maintain an effective capability to assure freedom to maneuver provides opportunities to exploit foreign developments and to create intra-alliance collaborative development opportunities. For example, Russian development of multi-axle off-road vehicles could be useful for surface-to-air missile systems and other large-scale systems that require off-road maneuver capability. Similarly, Russian air defense innovations (e.g., optical adjuncts to air defense engagement radars) can be mined for their utility in supporting U.S. maneuver requirements.

Signature management technology, processes, and employment constitute an important military capability that provides substantial leverage for other capabilities produced by U.S. defense investment. Some aspects of signature management deserve special measures to assure protection of the capability—perhaps a "stealth surety" program analogous to the nuclear surety program would reinforce existing efforts to protect this important dimension of U.S. military superiority. At the same time, improvements in allied signature management will serve the interests of the U.S. in coalition operations by enhancing the survivability of allied platforms. The export of some signature management capabilities is already authorized. A coherent policy approach to provide allied access to some fraction of these capabilities is desirable.

8. Protection of the U.S. Homeland from Direct Attack

The proliferation of the technologies of WMD and long-range ballistic and cruise missiles is expanding the scope of the prospective risk to the U.S. freedom of action by exposing the U.S. homeland to direct attack. A Congressionally mandated study (*The Commission to Assess the Ballistic Missile Threat to the United States)* led by former Secretary of Defense Donald Rumsfeld concluded that the threat posed to the Continental United States by ballistic missiles and WMD was maturing more rapidly than earlier intelligence estimates suggested. Moreover, the nature of several foreign ballistic

missile/WMD programs are such that the Commission concluded that the U.S. might have little or no warning when a threat was posed to the U.S. homeland.

Short- or medium-range conventionally and unconventionally armed ballistic missiles already pose a serious risk to U.S. expeditionary operations. The impact of these developments could be seriously compounded when nations hostile to the U.S. acquire capabilities that enable them to threaten the U.S. homeland with direct attack. North Korea, for example has had its medium range *No Dong* ballistic missile in series production since 1993 with perhaps hundreds of missiles produced, and has exported the system to Iran and Pakistan. The scope of the potential threat over time is substantial. Effective countermeasures to a foreign missile threat to the U.S. homeland involving active defense and other measures will be needed to eliminate a direct threat to the U.S. homeland from non-peer competitors.

9. Essential Enabling Capabilities

The ability of the United States to develop, deploy, operate, and sustain essential military capabilities is in turn dependent on a set of enabling scientific and industrial competencies and institutional arrangements. As part of the process of developing strategies for maintaining essential military capabilities, the Department must also preserve the critical skills that enable their development. The most important of these skills include:

- Robust technology development institutions and processes. Technology development institutions, supported by adequate funding, will be essential if the Department is to be successful in identifying and adapting fast-breaking commercial technologies to leverage existing DoD military capabilities. Because commercial technologies are universally available, skill sets and institutional arrangements that allow such technologies to be adapted in a manner that creates superior military capabilities will be a critical determinant of national power in the 21st century.

- Realistic training for combat and related military activities. Effective training is a fundamental discriminator in the ability of U.S. forces to bring superior military capabilities to bear. Advanced technology can make a substantial contribution to this function and needs to be thoroughly exploited.

- Systems integration processes. The ubiquitous character of advanced, and in some cases, enabling commercial technologies makes system integration skills and processes a crucial discriminator in the ability to create superior capabilities from widely distributed technologies. This capability needs to be both encouraged and protected.

Annex VII

Globalization and Personnel Security

Introduction

The globalization of defense information technology has outpaced the defense personnel security system, which evolved over many decades to protect classified information against traditional espionage threats. Our military capabilities now depend heavily on global, unclassified, commercial information systems that are produced in a world marketplace. Critical military functions derive substantial benefit from the efficiencies of web technology and advanced commercial components. However, the tremendous gains that result from military use of globalized information technology have created new kinds of risks. In responding to those risks, the personnel security dimension is as important as—and in some cases more important than—the technical security solutions supplied by software and hardware designers.

Two points underlie the change from traditional personnel security approaches.

The first point is the dependence of essential military capabilities on unclassified systems and networks. The threat is not just to the confidentiality of classified information. Much military information is properly unclassified and should remain so. Instead of espionage, the new dangers include the disruption or sabotage of the information system supporting a critical mission, or tampering with data to subvert the integrity of the information. Sabotage and subversion are not new concerns—but in the past they were considered isolated destructive acts or covert political influence. Today they take on new importance because of the potential that a hostile information operations attack could have a systemic impact on information systems and networks that sustain vital military missions.

The second point involves human flaws. Information systems and networks depend on the reliability of military and civilian specialists and administrative personnel who are not always within the traditional personnel security system for protection of classified information. Moreover, all the inside users of advanced information technology have vastly greater capabilities to exploit system vulnerabilities for espionage, sabotage, and malicious data manipulation. Inside users pose the greatest risk when their terminals link them with a network or networks—as is increasingly the case today for defense personnel.

In this new risk environment, the personnel security measures developed to protect classified information are ill-suited to the task of assuring that essential military capabilities are not compromised, disrupted, or distorted. New personnel security programs should shift from a security clearance model based primarily on background investigations for access to classified material to a situational awareness model which has been used in the past primarily for personnel with access to nuclear and other specialized weapons systems.

The security clearance model is focused primarily on the espionage threat and seeks to protect the confidentiality of classified data through a combination of personnel security clearances and physical access controls. The situational awareness model would concentrate on the threat to the integrity and availability of mission critical information—classified or unclassified. This threat from hostile information operations is magnified by the actual or potential access to sensitive systems and databases from global commercial networks.

Globalization is not the only reason for this change, but it exacerbates trends that have become more visible over the past two decades. Simply put, the security clearance model has failed to prevent or detect a regrettably large number of spies in the U.S. Government who have compromised classified information over the years. (See **Annex VIII, *Selected List of Cleared U.S. Citizens Convicted of Espionage*,** for a summary of prosecuted cases.) Armed with new information technology tools, the spies and saboteurs of the future will be able to compromise far more data and do far greater systemic damage. Only a fundamental reorientation of personnel security can mitigate the extraordinary vulnerabilities that can be exploited by adversaries aware of advanced information technologies.

Refining the Security Clearance Model

Personnel security concentrates on the insider threat. When espionage is considered the primary danger, the first factor in managing personnel security is to identify what information should have the greatest protection against unauthorized disclosure. Confidentiality is the main goal. The more sensitive the information, the higher the level of classification—Confidential, Secret, Top Secret. The requirements for a security clearance differ greatly depending on whether the clearance is at the Secret or Top Secret level. Under national policy a Top Secret clearance requires a full field background investigation and a periodic reinvestigation at (ideally) five year intervals. In addition to the national classification structure, special controls are established for Sensitive Compartmented Information (SCI) in the intelligence community, Special Access Program (SAP) information in the military, or Restricted Data (RD) in the nuclear world. These controls reduce the number of people with access to codeword-protected information and add further security requirements such as separate clearance adjudication, polygraph examinations or annual financial disclosure reports.

Unfortunately the personnel security clearance system to protect the confidentiality of information does not have an unblemished record of success, as demonstrated by the espionage cases of the past two dozen years—from Boyce-Lee and Kampiles to the latest disclosures of compromises of Energy Department secrets. After the Ames case broke in 1994, Executive Order 12968 tightened traditional personnel security clearance requirements. Background investigation and clearance adjudication criteria were standardized across the government, and clearance requirements for the millions of Secret-level positions were increased to include checks of credit and local law enforcement records. The Secretary of Defense and the Director, Central Intelligence were allowed to impose additional requirements for special access programs.

Despite the new Executive Order, resource and management challenges have dogged the Defense Department's primary personnel security investigative agency, the Defense Security Service (DSS). DSS is seeking to implement a complex and difficult nationwide automation upgrade while instituting a fee-for-service system to provide a stable source of funding—at the price of having to compete in future years with commercial firms that offer investigative services. The primary measure of DSS effectiveness is sometimes considered to be the length of time it takes to get a clearance. Instead, the greatest emphasis should be placed on identifying people who should not have access to the most sensitive information.

In the past, the security clearance program has had more success at excluding clearly unreliable people with criminal histories than at preventing or detecting espionage. Even with the authority to use polygraph examinations in periodic reinvestigations, the CIA has suffered serious espionage compromises. The Task Force does not question the need for a security clearance program to screen and re-evaluate personnel with access to the most sensitive information—such as identities of human intelligence sources, truly covert technical intelligence methods, and unacknowledged weapons information that provides a critical battlefield edge.

The clearance program, however, sweeps more broadly by attempting to protect too much "classified" information. The Task Force is convinced that *far more information than necessary is classified Secret or Top Secret.* The result is that too many security resources are devoted to the protection of classified information under the security clearance model—in comparison to the growing need for new types of security measures tailored to the challenges created by globalized information technology. The solution to unnecessary classification goes beyond the general policy guidance in an Executive Order. The Defense community must make a serious commitment to developing a systematic and coordinated analytic framework to serve as the basis for classifying information—and implementing that framework rigorously in all components.

The Task Force believes that the analysis of essential military capabilities recommended in this report provides the right methodology for classification and compartmentation decisions throughout the Defense Department—as well as for determining the parameters of other security policies and programs. The responsibility for applying this analysis to the classification system should be assigned to a dedicated Joint Staff element under the authority, direction, and control of the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence.

Compartmentation is a valuable instrument in making the security clearance model work better. Protecting confidentiality for information that is properly determined to require control in codeword compartments should have high priority. The Secretary of Defense and the Director, Central Intelligence have established oversight systems to ensure that compartments are justified. The DoD Special Access Program Oversight Committee and the DCI's Controlled Access Program Oversight Committee conduct annual reviews that require DoD components to justify their SAP and SCI controls. Once a SAP or SCI program has survived this scrutiny, it should have the most effective personnel security protection available, consistent with reasonable budget constraints and respect for individual rights that have clear legal protection. The measure of effectiveness of

security background investigations in providing security for compartmented programs should be whether such investigations produce the information needed to make sound judgments of trustworthiness.

The Task Force supports new initiatives underway to move away from the rigid security clearance model in providing personnel security for compartmented programs. These initiatives include aperiodic polygraph examinations, rather than a predictable reinvestigation timetable of five-year intervals or longer, and a new requirement for self-reporting of changes in the standard security clearance forms as part of annual security awareness training. *Compartmented programs should require the continuous evaluation of personnel*—beyond periodic clearance updates that may be delayed by shortfalls in investigative resources.

Better research is also needed to do the security clearance job. While adequate investigative resources and continuous monitoring are important, new approaches to the security clearance task should be explored and tested. Personnel security measures should be based on solid, objective research that looks for productive measures of investigative effectiveness and better means to evaluate trustworthiness. DoD is collaborating with an Intelligence Community personnel security research initiative that seeks to fill this gap. Defense and Intelligence Community leaders should be willing to change security clearance and investigative procedures when research results point in new directions. Nowhere is the need for change more compelling that in responding to the impact of global information technology.

The Situational Awareness Model

The use of global information technologies has increased the damage that a single spy can do. Compare downloading from computer databases today with the 1985 picture of a Jonathan Pollard removing paper documents in a briefcase every day to be photocopied at an offsite apartment. The risk from insider access to computer databases is compounded by classified use of web technology that links a single workstation to websites populated with classified databases from scores if not hundreds of components and offices.

The malicious or hostile disruption or manipulation of information systems by sabotage or subversion is a concern equal to the insider threat. The term more widely used now is hostile information operations. Within the classified world this risk is mitigated to some extent by the current personnel security system. In both the classified and unclassified worlds, however, recent research indicates that malicious insider manipulation of information is not likely to be detected or deterred by traditional personnel security practices.

Situational awareness is an alternative model. *Much greater emphasis is needed on continuous management supervision of personnel in critical information technology positions*. This is not just a job for security officers. It requires supervisors to have the training and the incentives to monitor reliability and exercise firm discipline. Today, the incentive structure is very different. Managers want the benefits of new information technology immediately, without waiting for the implementation of time-consuming security procedures. The incentives are clear. Performance is measured by getting the

new capability on line, not by adherence to the security procedures that protect information against hostile attack. This incentive structure must be changed so that security performance is rewarded, not penalized.

DoD is now seeking to identify new ways to reduce the risk that personnel in critical positions will either undertake malicious acts themselves or degrade security by their lax performance. The Task Force applauds this initiative led by OASD(C3I). It takes the unprecedented step of bringing together representatives of personnel security programs, personnel management programs, counterintelligence programs, and technical information security programs from major DoD components to merge their expertise. Too often, personnel security, personnel management, and information security technology have occupied different worlds, with little interaction and less collaboration. The new DoD insider threat initiative requires high-level support to prevent fragmentation and develop a coherent set of related actions that cut across functional boundaries.

Fortunately, commercial information technology is now providing new security tools to manage these risks more effectively. Financial transaction can be monitored, with appropriate consent, on a continuing basis. Audit and identification systems are available to ensure that an insider does not gain access to data he or she has no need-to-know and to detect attempts to masquerade electronically as a different user. Electronic access controls can enable data owners to issue certificates through a public key infrastructure. These "communities of interest" need not be formal compartments, but rather a means to enforce need-to-know for access to a particular website. To work properly, however, program and project managers have to make essentially personnel security decisions—who has a "need to know" or a "need for access" to a website on the network? Security policy guidance for these decisions may become as important as oversight of formal SAPs and SCI compartments.

The challenge for DoD and the Intelligence Community is to manage the use of these tools consistently, with resources allocated in accordance with consistent and enforceable requirements. This means stronger Defense-wide and Intelligence Community direction. Without such administrative leadership, the efficiencies of interconnected information networks will be degraded—because holders of valuable sensitive information will not risk letting it be shared on the network. The Task Force recommends that OASD(C3I) reach agreement with the DCI's Community Management Staff on a common situational awareness program to address the insider threat at the classified level in the defense and intelligence communities.

Another challenge is to develop an appropriate security program for personnel in government and in defense industry who occupy sensitive but unclassified positions that are critical for protecting information systems from hostile disruption or manipulation via the global commercial network. The first task is to identify the key positions. To some extent the need is similar to the identification of positions for DoD's traditional Nuclear Personnel Reliability Program (PRP) and other sensitive military assignments. The second task is to define the security goals and objectives that apply to those positions. Should foreign nationals be disqualified, even if they are a defense contractor's most skilled experts and do not require access to classified information? What kind of security

background investigation, if any, should be conducted? Are resources better assigned to continuous evaluation of performance and reliability? Should the criteria for evaluation be the same as adjudication for a security clearance for classified information? Or should they be more like the reliability criteria for the nuclear PRP and other sensitive assignments?

In this area the Department must be prepared to establish policies that achieve a new balance between security and employee privacy. Monitoring on-the-job performance in critical information technology positions may be more important than a full field background investigations. Audit technology that indicates misuse of a network may be more important that a polygraph examination. Security measures still have to be cost-effective because risk avoidance is not affordable. Again, research is key—testing alternative security approaches in simulated and even real-life situations.

Implementation of the situational awareness model for sensitive information technology positions requires innovative management leadership within the established structure of the Office of the Secretary of Defense. OASD(C3I) is responsible for personnel and information security, and OUSD(P&R) has parallel responsibility for personnel management. An appropriate personnel security program for information technology positions requires the authorities and expertise of both organizations, working in concert with the security and personnel elements of the principal DoD components. The component that appears to have made greatest progress in identifying critical information technology positions and designing new security approaches is the Air Force. *The Task Force recommends that the a joint team be formed in the Air Force, under the concurrent authority, direction, and control of the USD(P&R) and the ASD(C3I), to develop and lead implementation of a new situational awareness program for DoD information technology personnel.*

As discussed elsewhere in this report, both personnel security and information security would benefit from outside vulnerability assessments, including "red team" tests, that are not bound by the administrative interests of any one Defense organization. The lessons of vulnerability assessment and "red team" testing are as important for the design of new safeguards against the insider threat as they are to our defenses against outside penetration and the hostile exploitation of commercial products.

In summary, the Task Force recommends adapting personnel security to the new global information operations threat by streamlining traditional security classification and clearance practices, compartmenting the most sensitive data, stressing situational awareness, focusing on critical information technology positions, and making greater use of outside research and independent threat/vulnerability evaluation.

ANNEX VIII -- Selected List of Cleared U.S. Citizens Convicted of Committing Espionage

Convicted	Surname	Given Name	Clearance	Affiliation	Type of Information Passed
1975	Dedeyan	Sahag Katcher	Top Secret	Johns Hopkins Univ.	NATO and Navy Sealift Enhancement documents
1977	Boyce	Christopher John	SCI	TRW	Cryptography, Technical research, satellites
1979	Madsen	Lee Eugene	Top Secret	USN	CIA confidential doc re drug trafficking
1980	Barnett	David Henry	Secret	CIA	Soviet Missiles, Soviet submarines, info re agents
1981	Bell	William Holden	Top Secret	Hughes Aircraft	radars, technical research, esp re Quiet radar
1981	Cooke	Christopher Michael	Top Secret	USAF	Nuclear plans/preps, intl re Soviet nuclear, Titan II secrets
1981	Helmich	Joseph George, Jr.	Top Secret	USA	Crypto, Instruction Manuals, KL-7 rotors & KW-26 crypto
1976	Kampiles	William	SCI	CIA	Satellite reconnaissance capabilities
1983	Schuler	Ruby Louise	Secret	Systems Control, Inc.	Documents pertaining to U.S. missile defense
1984	Cavanagh	Thomas Patrick	Secret	Northrop	technical research to B-2 bomber
1984	Cordrey	Robert Ernest	Secret	USMC	Compromised, NBC info offered
1985	Chin	Larry Wu-Tai	SCI	CIA	Foreign Intelligence re Far East
1985	Howard	Edward Lee	SCI	CIA	Intelligence re agents, Soviet intelligence
1985	Pollard	Jonathan Jay	SCI	USN	Cryptography, Foreign Intel, Naval Intel
1985	Scranage	Sharon Marie	SCI	CIA	Personnel at CIA, agents for CIA in Ghana
1985	Walker	John Anthony Jr.	Top Secret	USN	Cryptography, submarine, communications, intelligence
1985	Walker	Arthur James	Top Secret	USN	Repair manual, C3 fleet ships, reports on amphibian craft
1985	Walker	Michael Lance	Secret	USN	Naval C3 weapons plans
1985	Whitworth	Jerry Alfred	Top Secret	USN	Cryptography, intelligence
1988	Conrad	Clyde Lee	Top Secret	USA	NATO and U.S. plans for defense of Europe
1988	Dolce	Thomas Joseph	Secret	USA	Weapons systems R&D data
1988	Richardson	Daniel Walter	Secret	USA	Unclass info on M1 tank: wiring diag, circuit board
1989	Kunkle	Craig Dee	Secret	USN	Anti-sub warfare
1990	Ramsey	Roderick James	Top Secret	USA	Army/NATO defense secrets, incl tactical nuclear plans
1991	Sombolay	Albert T.	Unknown	USA	Troop deployments, veh ID documents, CW protective gear
1992	Gregory	Jeffery Eugene	Unknown	USA	Defense plans for C. Eur., U.S. & NATO mil secrets
1992	Rondeau	Jeffrey Stephen	Unknown	USA	Army/NATO defense secrets, incl tactical nuclear plans
1994	Ames	Aldrich Hazen	Top Secret	CIA	Identities CIA assets in Soviet Union, Russia
1995	Charlton	John Douglas	Secret	Lockheed	U.S. defense information
1996	Lessenthien	Kurt G.	Secret	USN	Nuclear submarine technology
1996	Nicholson	Harold James	SCI	CIA	Info re national defense + bio Info on CIA officers + CI Info
1996	Pitts	Earl Edwin	Top Secret	FBI	Class FBI documents
1997	Squillacote	Therese Marie	Secret	ODUSD	Class DoD and CIA documents
1997	Warren	Kelly Therese	Unknown	USA	U.S. and NATO secrets

Annex IX

Briefings Received by the Defense Science Board Task Force on Globalization and Security

Title	Briefer	Organization
October 8, 1998		
Hart Scott Rodino / Exon Florio Review Processes	Mr. Victor Ciardello	*Director, Financial & Economic Analysis, USD(A&T)*
Defense Security Service Zero Based FOCI Review	Mr. Joe Cashin	*Defense Security Service*
Foreign Ownership, Control Mitigation	Mr. Chris Griner	*Kaye, Scholer, Fierman, Hays & Handler*
Counter Intelligence Acquisition Board	Mr. Bob Reynolds	*CIA*
Conversation with	Dr. John Deutch	*MIT*
Conversation with	Dr. Craig Fields	*Chairman, Defense Science Board*
October 27, 1998		
Global Technical Talent Pool	Dr. Ron Lehman	*Lawrence Livermore National Laboratory*
Defense Threat Reduction Agency	Mr. George Singley	*Hicks & Associates, Inc.*
Secretary of Defense, Strategic Studies Group Effort	Col Ron Reichelderfer CAPT Bob Maslowsky	*Secretary of Defense, Strategic Studies Group*
Army's Commercial Satellite and Airlift Solutions	Dr. Joseph Braddock	*The Potomac Foundation*
Conversation with	Dr. Lin Wells, II	*OASD(C^3I)*
November 18, 1998		
Mobile Subscriber Equipment for the U.S. Army	MG Robert Morgan, USA (Ret)	*Private Consultant*
Changing Nature of the International Arms Market	Mr. Andrew W. Hull Mr. David R. Markov	*Institute for Defense Analyses*
Disclosure, Security & Globalization	Ms. Susan Ludlow-MacMurray	*OSD Security Policy*
History and Perceptions on Security for International Programs	Mr. Chuck Wilson	*Consultant*
Some Financial Industry Perspectives	Mr. Wolfgang Demisch	*Wasserstein Perella*
November 19, 1998		
Implications of COTS Software Vulnerabilities	Dr. Robert H. Anderson	*RAND Corporation*
Measures to Make the Possible Improbable	Dr. Joe Markowitz	*IOTC*
U.S. Export Controls in High Technology – Computers vs. Cryptography	Dr. Ken Flamm	*LBJ School, Univ. of Texas*
International Defense Consolidation Implications	Mr. Joe Schneider	*JSA Partners*
December 17, 1998		
DSB Task Force on Coalition Warfare	Dr. Ted Gold	*IDA*
Conversation with	Hon. Jacques Gansler	*Under Secretary of Defense, Acquisition and Technology*

December 18, 1998		
Information Operations Threat	Ms. Pam Alexander Mr. Steve Stigall	*CIA*
Conversation with	Hon. John Holum	*Acting Under Secretary of State for Arms Control and International Security Affairs*
January 21, 1999		
Global Defense Technology Availability	Mr. Russell Burns Mr. Chris Beck Mr. Tom Clemens	*DIA*
Global Technology Assessment	Mr. Steve Cohn	*Army Science and Technology Master Plan*
Critical Infrastructure Assurance Office Department of Commerce	Dr. Jeffrey Hunker	*Then-Director, CIAO*
National Infrastructure Protection Center Federal Bureau of Investigation	Mr. Douglas Perritt	*Deputy Chief, NIPC*
Joint Task Force, Computer Network Defense Department of Defense	MG John Campbell, USAF	*Commander, JTF-CND, Deputy Director, DISA*
Information Systems Security - National Security Agency	Mr. John Nagengast	*Assistant Deputy Director, Information Systems Security*
January 22, 1999		
Globalization's Effects on Federal Acquisition Regulations	Mrs. Eleanor Spector	*Director, Defense Procurement*
Personnel Security Issues	Mr. John Elliff Mr. Bill Leonard	*CIA/CMS* *OASD(C3I)*
Export Controls	Mr. John Barker	*Deputy Assistant Secretary of State*
Conversation with	Honorable John J. Hamre	*Deputy Secretary of Defense*
March 11, 1999		
Export Control Implementation Perspective	Mr. Chris Griner	*Kaye, Scholer, Fierman, Hays & Handler*
Globalization of Biotechnology Panel	Professor Charles Cooney Dr. Joshua Lederberg Mr. Don Mahley	*MIT* *Rockefeller University* *ACDA*
March 12, 1999		
Information Security	Dr. Joe Markowitz	*IOTC*
Personnel Security	Mr. John Elliff	*CIA/CMS*
April 6, 1999		
Vulnerability Assessment/Red Team Briefings and Discussion of DoD's current activity (C3I)	Mr. Mike Peters Mr. Randy Resnick Mr. Gary Guissanie	*National Security Agency* *C3I* *C3I*
April 28, 1999		
China Briefing	Dr. Dave Shaumbaugh Mr. John Culver	*George Washington University* *CIA*
May 13, 1999		
Strategic Planning, Saab Military Aircraft	Mr. Tommy Ivarson	*Senior VP, Strategic Planning, Saab Military Aircraft*
May 24, 1999		
FAR/DFARS	Mr. Frank Kendall	*Consultant*

Annex X

List of Acronyms

AECA	Arms Export Control Act
AESA	Active Electronically Scanned Array
ASATs	anti-satellite weapons
ASD	Assistant Secretary of Defense
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASIC	application-specific integrated circuit
C3I	Command, control, communications and intelligence
C3ISR	Command, control, communications, intelligence, surveillance, and reconnaissance
CAFÉ	corporate average fuel efficiency
CAS	Cost Accounting Standards
CFIUS	Committee on Foreign Investment in the United States
CIA	Central Intelligence Agency
CMI	classified military information
CMM	Capability Maturity Model
CoCom	Coordinating Committee on Export Controls
COMSEC	communications security
COTS	commercial-off-the-shelf
DARPA	Defense Advanced Research Projects Agency
DCI	Director, Central Intelligence
DDL	Designated Delegation of Authority Letter
DEA	Data Exchange Agreement
DFARS	Defense Federal Acquisition Regulations Supplement
DIAP	Defense Information Assurance Program
DIRNSA	Director of the National Security Agency
DoD	Department of Defense
DSB	Defense Science Board
DSMC	Defense Systems Management College
DSP-83	Non-Transfer and Use Certificate
DSCA	Defense Security and Cooperation Agency
DSS	Defense Security Service
DTC	State Department's Office of Defense Trade Controls, also ODTC
DTRA	Defense Threat Reduction Agency
DTRA/DTSA	DTRA/Defense Technology Security Administration
EELV	Evolved Expendable Launch Vehicle
EMP	electromagnetic pulse
ENDP	Exception to National Disclosure Policy
EU	European Union
FAR	Federal Acquisition Regulations, see also DFARS

FBI	Federal Bureau of Investigation
FDI	Foreign Direct Investment
FFRDC	Federally-funded Research and Development Center
FMS	Foreign Military Sales
FOCI	foreign ownership, control, or influence
FYDP	Future Years Defense Program
GCCS	Global Command and Control System
GLONASS	**GLO**bal **NA**vigation **S**atellite **S**ystem
GPS	Global Positioning System
GSOMIA	General Security of Military Information Agreements
GTO	geosynchronous transfer orbit
HPCs	high-performance computers
INFOSEC	information security
IO	Information Operations
IOC	initial operational capability
IR&D	Independent (or internal)Research and Development
ISR	intelligence, surveillance and reconnaissance
ITAR	International Traffic in Arms Regulations
KPP	Key Performance Parameter
LEO	low earth orbit
LOA	Letter of Offer and Acceptance
LRPS	long-range precision strike
MEMS	microelectromechanical systems
MEO	medium earth orbit
MLA	Manufacturing License Agreement
MOU	Memorandum of Understanding
MTOPS	millions of theoretical operations per second
NATO	North Atlantic Treaty Organization
NDAs	Non-disclosure agreeements
NDP	National Disclosure Policy
NDPC	National Disclosure Policy Committee
NIAP	National Infrastructure Assurance Partnership
NID	National Interest Determination
NIPRNet	**U**nclassified-but-sensitive **I**nternet **P**rotocol **R**outing **NET**work
NIS	networked information systems
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
non-SME	non-Significant Military Equipment
NRO	National Reconnaissance Office
NSA	National Security Agency
OUSD(A&T)	Office of the Under Secretary of Defense for Acquisition and Technology
R&D	research and development
RD	Restricted Data
RDT&E	research, development, test and evaluation
RFP	Request for Proposal

RMA	revolution in military affairs
ROE	rules of engagement
ROK	Republic of Korea (South Korea)
SAP	Special Access Program
SCI	Special Compartmented Information
SDI	Strategic Defense Initiative
SIPRNet	Secret Internet Protocol Routing NETwork
SME	Significant Military Equipment
SPOT	French remote sensing satellite
SSA	Special Security Agreement
SSTO	Single Stage to Orbit
TAA	Technology Assistance Agreement
TRANSCOM	U.S. Transportation Command
TSCM	Technical Surveillance Counter Measures
TSTO	Two Stage to Orbit
UK	United Kingdom
UN	United Nations
USA	United States Army
USAF	United States Air Force
USD	Under Secretary of Defense
USD(A&T)	Under Secretary of Defense for Acquisition and Technology
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USMC	United States Marine Corps
USML	U.S. Munitions List
USN	United States Navy
WMD	weapons of mass destruction
Y2K	Year 2000

Annex XI

Bibliography

Globalization

Bedi, Rahul, "Cost Hikes in Russian Aircraft Spares Forces India Into Local Action," *Jane's Defence Weekly*, December 2, 1998.

"DASA Chief Urges Fast Track on European Consolidation," *Aviation Week and Space Technology*, June 1, 1998.

Donnelly, John, "New Chip to Make Satellites Nuke-Proof," *Defense Week*, December 7, 1998.

Erwin, Sandra I., "Need for Global Mobility Spurs Demand for Airlift: Aerospace giants Boeing, Lockheed, poised to corner world military air transport market," *National Defense*, December 1998.

"Finally, Commanders Get Clout on Weapons Requirements," *Aviation Week & Space Technology*, December 7, 1998, p. 110.

"4 French Companies In Missile Contract Pact," *New York Times*, December 10, 1998.

Fleming, Charles, "Turbine Makers Are Caught in Innovation Trap," *Wall Street Journal*, February 13, 1998.

Gertz, Bill, "Chinese Army Is Building Anti-Satellite Laser Weapons," *Washington Times*, November 3, 1998.

"Global Defence Industry," *The Economist*, June 14, 1997.

Greider, William, *Fortress America: The American Military and Consequences of Peace* (New York: Public Affairs), 1998.

Griner, G. Christopher, Christopher R. Brewster, and Farhad Jalinous, "The Exon-Florio Process – Review of Acquisitions and Investments in the United States by Foreign Investors," Kaye, Scholer, Fierman, Hays and Handler, LLP, January 1998.

Griner, G. Christopher, Christopher R. Brewster, and Farhad Jalinous, "The National Industrial Security Program Operating Manual: An Overview of Foreign Ownership, Control, or Influence Regulations," Kaye, Scholer, Fierman, Hays and Handler, LLP, January 1998.

Griner, G. Christopher, Christopher R. Brewster, and Farhad Jalinous, "U.S. Statutory Restrictions on Foreign Investment," Kaye, Scholer, Fierman, Hays and Handler, LLP, January 1998.

Hirsh, Michael, "The Great Technology Giveaway?: Trading With Potential Foes," *Foreign Affairs*, September/October 1998.

Honan, William, "More Foreign Students Attending U.S. Colleges," *New York Times*, December 7, 1998.

Hull, Andrew and David Markov, "A Changing Market in the Arms Bazaar," *Jane's Intelligence Review*, March 1997, pp. 140-142.

Hull, Andrew and David Markov, "Trends in the Arms Market – Part 1," *Jane's Intelligence Review*, April 1997, pp. 187-190.

Hull, Andrew and David Markov, "Trends in the Arms Market – Part 2," *Jane's Intelligence Review*, May 1997, pp. 232-238.

Hull, Andrew, Richard White, and David Markov, "Inserting Commercial Technologies into Military Systems: Lessons from British Experience," Institute for Defense Analysis, November 1997.

"Israel Will Help Display Improved MiG At Show," *Washington Times*, December 2, 1998.

Louscher, David J., Alethia H. Cook and Victoria D. Barto, "The Emerging Competitive Position of US Defense Firms in the International Market," *Defense Analysis*, Vol. 14, No. 2, 1998, pp. 115-134.

Markoff, John, "International Group Reaches Agreement on Data-Scrambling Software," *New York Times*, December 4, 1998.

Markusen, Ann, "The Rise of World Weapons," *Foreign Policy*, Spring 1999, pp. 40-51.

Marsh, Peter, "Cutting Out the Core," *Financial Times*, November 16, 1998.

Morrocco, John D., "U.S. Assesses Shifting Transatlantic Ties," *Aviation Week & Space Technology*, December 14, 1998, p. 59.

"NATO's mid-life crisis," *The Economist*, December 12, 1998.

"New Visions For NATO," *New York Times*, December 7, 1998.

"Platform Envy," *The Economist*, December 12, 1998.

"Privacy Rules Send U.S. Firms Scrambling. European Union Will Curb Transmissions to Nations Considered Lax," *Washington Post*, October 20, 1998.

Reed, Stanley, Gail Edmondson, Karen Lowry Miller, and Stan Crock, "Europe's Defense Industry: No More Flying Solo?" *Business Week* (International Edition), December 21, 1998.

Rees-Mogg, William, "Britain, a Nation of Subcontractors: Proposed Mergers that Place Key Defence Concerns in Foreign Hands are Politically Unacceptable," *London Times*, December 14, 1998.

Robbins, Carla Anne, "Out of the Box, Why Nuclear Threat Today Can Be Found at the Electronics Store: U.S. Can't Control the Spread of New High-Speed PCs, Raising Proliferation Risk, National Security for Sale?" *Wall Street Journal*, December 14, 1998.

Robbins, Carla Anne, and Andrew Higgins, "Fission For Cash: Money Hungry, Russia Finds a Foreign Market For Nuclear Knowledge: But Is It Selling More Than a Power Plant to Iran? U.S. Intelligence Says Yes; Days of Plutonium and Caviar," *Wall Street Journal*, December 15, 1998.

Robinson, Edward, "The Pentagon Finally Learns How to Shop: The military is changing the inane ways it has always bought hardware," *Fortune*, December 21, 1998.

"Russia Holds Talks on Su-30 Transfer Technology," *Flight International*, November 25-December 1, 1998.

Schlesinger, Jacob M. and Christine Duff, "No Jingo Jangle: As Foreigners Again Gobble Up U.S. Firms, Where's the Backlash? Unlike in Japan's '80s Spree, Americans Are Cockier, Less Fearful of Invasion. Just a Yawn in Washington," *Wall Street Journal*, December 15, 1998.

Schlesinger, James R., "Raise the Anchor or Lower the Ship – Defense Budgeting and Planning," *The National Interest*, Fall 1998, pp. 3-12.

Simons, John, "Senate Clears Way for Bill Increasing Visa for Foreign High-Tech Workers," *Wall Street Journal*, October 14, 1998.

Simons, John, "U.S. Prohibits Some Satellite Imaging of Israel," *Wall Street Journal*, July 24, 1998.

Steinberg, Jessica, "The Military-Technological Complex is Thriving in Israel," *New York Times*, December 6, 1998.

Swire, Peter P. and Robert E. Litan, *Avoiding a Showdown Over EU Privacy Laws*, Brookings Policy Brief #29, February 1998.

"Toyota Revamps Plants for Shift to Exports if Local Markets Fail," *Wall Street Journal*, October 7, 1998.

Wald, Matthew L., "Concerns About Jamming Surround New Air-Navigation System," *New York Times*, November 23, 1998.

Information/Infrastructure Security

Anderson, Robert H., Richard O. Hundley, "The Implications of COTS Vulnerabilities for the DoD and Critical U.S. Infrastructures: What Can/Should the DoD Do?" RAND Corporation, August 14, 1998.

Arquilla, John and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND), 1997.

Binkely, Christina, "Bad Luck: Glitches Can Make One-Armed Jackpots Evaporate," *Wall Street Journal*, August 10, 1998.

Cillaffo, Frank J., Task Force Director and Editor, *Cybercrime, Cyberterrorism, Cyberwarfare*, Report of the Center for Strategic and International Studies (CSIS) Global Organized Crime Project, November 1998.

"The Clinton Administration's Policy on Critical Infrastructure Protection: PDD 63," White Paper, May 22, 1998.

Crawley, James W., "Terror on the Web? Experts scoff at Pentagon purge of Internet sites," *San Diego Union-Tribune*, November 9, 1998.

Ewing, Jonathan and Sami Lais, "70 CPUs add up to big power: Los Alamos staff build one of the cheapest, fastest supercomputers in world," *Government Computer News*, September 7, 1998.

Ewing, Jonathan, "The Beowulf blazes the homemade supercomputer trail," *Government Computer News*, September 7, 1998.

Flamm, Kenneth, "Controlling the Uncontrollable—Reforming U.S. Export Controls on Computers," *Brookings Review*, Winter 1996, Vol. 14, No. 1, p. 22.

Flamm, Kenneth, *Deciphering the Cryptography Debate*, Brookings Policy Brief #21, July 1997.

Goetz, Thomas, "Corporate Highfliers Beware: Someone May Be on Your Tail," *Wall Street Journal*, October 29, 1998.

Graham, Bradley, "U.S. Studies New Threat: Cyber Attack, Hackers, Simulation Expose Vulnerability," *Washington Post*, May 24, 1998.

Ismael, Katie E., "4 Accused in High-Tech Gas Pump Scam," *Los Angeles Times*, October 9, 1998.

Kutner, Joshua, "Terrorist Threat Epidemic Prompts Pentagon Response," *National Defense*, September 1998.

Makulowich, John, "Computer Security Testing Scheme Springs Forward," *Washington Technology*, September 24, 1998.

Simons, John, "U.S. to Allow Coalition of Companies to Export New Encryption Technology," *Wall Street Journal*, October 19, 1998.

Wilson, William, "Despite Computer Security Advances, Hackers Appear to be Keeping Pace," *National Defense*, September 1998.

Defense Science Board Reports

DSB 1995 Summer Study on Investments for 21st Century Military Superiority, November 1995.

DSB 1996 Summer Study Task Force on Tactics and Technology for 21st Century Military Superiority, October 1996.

DSB 1997 Summer Study on DoD Responses to Transnational Threats (Volume 1), October 1997.

DSB Task Force on Defense Acquisition Reform (Phase I), July 1993.

DSB Task Force on Defense Acquisition Reform (Phase II), August 1994.

DSB Task Force on Defense Acquisition Reform (Phase III), May 1996.

DSB Task Force on Defense Acquisition Reform (Phase IV), through March 1999.

DSB Task Force on Information Warfare Defense (IW-D), November 1996.

DSB Task Force on International Armaments Cooperation, July 1996.

DSB Task Force on Outsourcing and Privatization, August 1996.