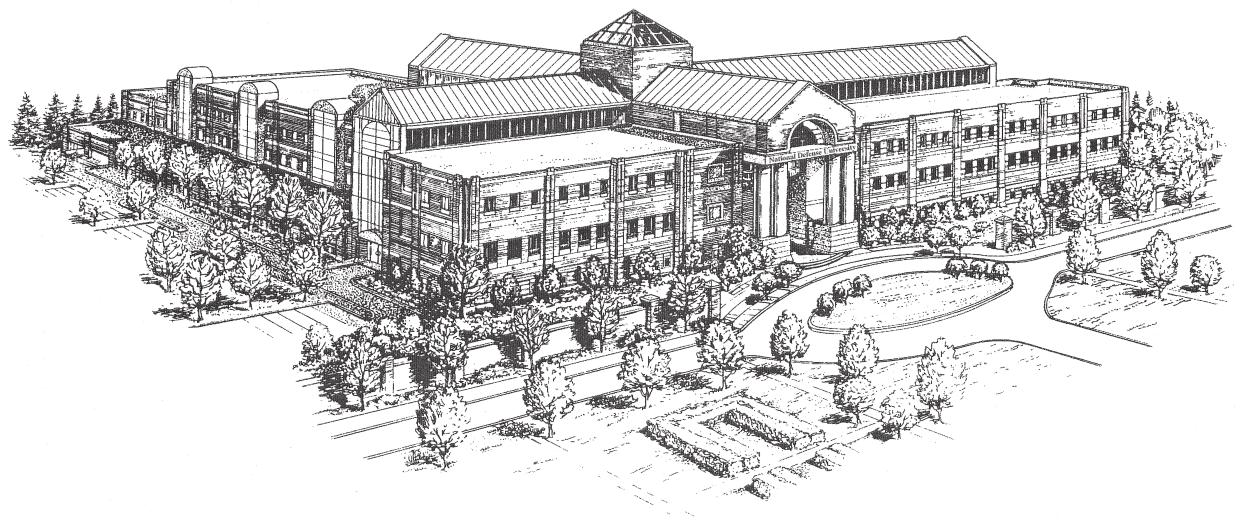
Report to the Congress

Information Technology Program



Center for Technology and National Security Policy
National Defense University

January 2006

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Report to the Congress. Information Technology Program	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,Fort Lesley J McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**122**	

Report to the Congress

Information Technology Program
Center for Technology and National Security Policy
National Defense University

January 2006

Preface

For the last three years, the Center for Technology and National Security Policy (CTNSP) at the National Defense University (NDU) has been pursuing a broad range of activities on ways to link advanced commercial information technologies (IT) to improved military capabilities. In the National Defense Authorization Act for Fiscal Year 2006, the House Armed Services Committee (HASC) included language that requests that a report be provided that documents "…the results of the program and plans for future efforts with the submission of the fiscal year 2007 budget request to Congress."

The first part of the report includes an Executive Summary and a detailed summary of the CTNSP IT program. The second part includes three appendices, including synopses of the many activities that CTNSP staff have performed in support of the IT program and short biographies of the authors and contributors to the reports. It should be noted that the findings and recommendations in the studies summarized in this report represent the work of individual researchers and do not necessarily represent the views of the National Defense University, the Center for Technology and National Security Policy, or the Department of Defense.

Contents

Executive Summary

In the National Defense Authorization Act for Fiscal Year 2002, the Report of the Committee on Armed Services, House of Representatives, stated that the "Department of Defense can no longer depend on a dedicated defense industrial base, but will need to find ways to link advanced commercial technologies to improved military capabilities." Congress asked the Center for Technology and National Security Policy (CTNSP) to implement a program "to find practical ways in which the defense information technology (IT) community can gain a mutual understanding of defense needs and industry capabilities and identify opportunities to integrate technology innovation in the U. S. military strategy."

Subsequently, in the Report of the Committee on Armed Services for the National Defense Authorization Act for Fiscal Year 2006, the Committee requested that a report be provided that documents "…the results of the program and plans for future efforts with the submission of the fiscal year 2007 budget request to Congress."

This report summarizes the major findings and recommendations that CTNSP has developed through its IT program. These results were developed over three years through a structured set of nearly 40 coordinated activities, including studies and analyses, surveys, interviews, workshops, conferences, and prototypes. To the extent feasible, the program leveraged selected activities at CTNSP and related efforts at other centers at NDU. CTNSP also has taken steps to involve the most creative members of government, industry, academia, and think tanks in these activities.

Setting the Stage

To establish a foundation for the effort, CTNSP undertook activities to define the problem of using commercial technology in defense systems by understanding the perspectives of the various stakeholders, clarifying DoD's IT needs, and identifying relevant technology trends.

As an initial step, a series of fourteen assessments were performed to capture the perspectives of four key classes of stakeholders in the problem: commercial industry, DoD laboratories, key allies and partners, and key Asian nations. These studies provided the following insights:

- Small and medium-size innovative commercial IT firms are frustrated in their dealings with DoD. They believe that they have much to contribute to DoD but find the DoD market to be bureaucratic, opaque, and difficult to navigate.
- The DoD laboratories tend to be a useful catalyst in identifying and leveraging commercial IT, but they are perceived as parochial, focusing on single-Service issues.
- Our NATO allies are generally not allocating sufficient resources to applied defense science and technology (S&T), and there is concern that a gap may be

emerging that may limit our ability to conduct effective operations with them in the future.

- An interesting commercial-military model is emerging in Sweden that may provide useful insights for DoD. However, this initiative is still in its infancy, and there is concern that it might not scale effectively to meet DoD needs.
- We are witnessing dynamic growth of commercial IT initiatives in Asia, with the possibility that they may "leap frog" the U.S. and adversely affect our economic and military status. This is particularly true of China, which announced in its December 2004 White Paper on National Defense that it is undertaking an "informationalization" strategy. Consistent with this strategy, China has declared its intention of "building an informationalized force" and is "aiming at … winning an informationalized war."

As a second step, CTNSP performed a series of five studies to clarify the technology trends that are affecting the issue. At the physics level, it was observed that Moore's Law (which predicted the doubling of transistor density about every eighteen months) may overstate the future rate of growth in chip capabilities, reflecting the technological challenge of scaling ever-smaller components. This slowdown is likely to adversely affect the performance of IT systems. Several additional studies highlighted the growing vulnerability of IT-based systems to attacks by adversaries. These vulnerabilities include the threats of computer network attack, electromagnetic pulse attacks, and cascading effects if critical infrastructures are targeted.

To further set the stage, CTNSP staff conducted a series of workshops and assessments to characterize DoD's IT needs. These assessments revealed that DoD is aggressively pushing the limits of IT and will require ambitious breakthroughs in, inter alia, mobile, ad hoc communications, robotics, and information assurance. Furthermore, interoperability remains a pervasive problem if DoD is to function effectively across Service lines and with interagency and multinational partners. Substantial efforts should be made at the strategic, policy, institutional, systems, training, and technology levels to deal with these problems.

Recommended Actions to Enhance the Injection of Commercial IT into DoD Systems

Based on this understanding of the nature of the problem, CTNSP conducted several initiatives to enhance DoD's ability to exploit commercial IT. In view of the inability of DoD to communicate effectively with small and medium-size commercial IT companies, CTNSP undertook a prototype effort to create an interactive website for Joint Forces Command (JFCOM). The approach taken in this initiative, EMISARS ("Early Military Involvement Speeds Acceptance and Results"), would be of mutual value to DoD, which will be positioned to influence the development of IT products by early engagement, and to the commercial IT sector, which will gain important market input for development and build military contacts.

Second, DoD and the Intelligence Community (IC) are conducting a variety of venture capital-related prototype activities (e.g., the CIA's In-Q-Tel and OSD's Defense Venture Catalyst Initiative) to enhance the rapid injection of innovative commercial IT products into DoD and IC systems. A study of these efforts reveals that there are broker, equity, and portfolio models for employing venture capital techniques, but no single right way for DoD to employ these techniques. These efforts are in their infancy and should be monitored closely to derive best practices that can be disseminated among this emerging community of interest.

CTNSP performed two studies to explore the use of commercial-off-the-shelf (COTS) products in more traditional DoD acquisitions. These studies concluded that successful endeavors employed open architectures and spiral development processes. However, myths about the use of COTS need to be recognized and dispelled. For example, experience reveals an intelligent practitioner will factor in both COTS-based system sustainability costs as well as acquisition costs. Furthermore, COTS products should be modified as a last resort; when modified they cease to be COTS, and modifications create sustainment and evolvability issues.

Finally, several studies explored the role of lead system integrators (LSIs) in acquiring complex, IT-intensive, systems of systems. Those studies emphasized that the use of an LSI, although appropriate for highly complex acquisitions, does not absolve the Government from assuming final accountability.

CTNSP activities related to the use of commercial IT in DoD systems culminated in a report, entitled "Actions to Enhance the Use of Commercial IT in DoD Systems." That study sought to address the major obstacles that the earlier CTNSP studies had identified: non-attractiveness; non-transparency; non-agility; non-dominance; an isolating market; and the attitudes of prime contractors/LSIs. To overcome these obstacles, a balanced mix of initiatives was recommended by the study:

1. **Enhance communications/organization**. To enhance communications, "technology prospectors" should be created to conduct more focused searches and facilitate the injection of COTS into DoD systems. Web portals should be created to coordinate use of commercial IT and "acquisition guides" should be provided to smaller companies to help them navigate the DoD acquisition process. A new organization should be created at JFCOM to coordinate the use of commercial IT and support these activities.
2. **Increase resource flexibility**. Provide Combatant Commands (COCOMs) the ability to generate procurements using a joint task force for COCOMs (perhaps led by JFCOM), building on the limited acquisition authority model provided to JFCOM by USD(AT&L). The Defense Security Cooperation Agency (DSCA) model for procurement should be emulated vice the creation of a new major acquisition group. A bridging fund should be created to support the acquisition of key commercial IT products.
3. **Reduce acquisition barriers**. Meaningful measures could include changing DoD rules on Intellectual Property Rights (IPR) and increasing thresholds for applying a simplified acquisition process. In addition, other transaction authority (OTA) should

be adopted as the approach for commercial IT R&D and procurement.

4. **Promote cultural change**. This is a difficult task that might begin with increasing DoD education and training for commercial IT development and procurement, providing incentives for program managers and LSIs to use COTS, and adapting GAO-recommended best practices to acquire commercial-component business systems.
5. **Review testing**. Evaluate expanding Underwriter Laboratory-style testbeds and expanding operational testbeds to evaluate the impact of the technology on mission effectiveness.
6. **Adopt requirements for specific missions**. Explore opportunities for commercial IT to support specific missions such as stabilization and reconstruction (S&R) operations, homeland security, and information operations.

The findings and recommendations of this study have been briefed widely within DoD to some of the senior-most decisionmakers in DoD (e.g., Chairman, Joint Chiefs of Staff (CJCS); Commander, JFCOM; Service Chiefs of Staff).

At the conclusion of a briefing in the "Tank," then-VCJCS GEN Pace directed that LTG Shea, Director, J6, Joint Staff, pursue options for rationalizing the CTNSP recommendations with on-going initiatives in the Joint Staff. Subsequently, meetings were held with members of the Joint Staff and the Institute for Defense Analyses (IDA) to rationalize the recommendations. Follow-on discussions were conducted to explore options to modify three of the key recommendations: enhance communication/organization, increase flexibility, and review testing.

Based on those discussions with the Joint Staff, CTNSP has implemented the following modifications to the recommendations:

- Create an organization for rapid capability delivery that could perform the roles of tech-prospector, acquisition guide, and champion of industry-DoD communication interface. This role could be played by JFCOM, perhaps in concert with STRATCOM and the Defense Information Systems Agency (DISA).
- Create a Systems Engineering and Integration (SE&I) organization that would deal with system of systems issues. This might be resident at DISA with strong COCOM participation.
- With respect to increased resource flexibility, it is recommended that COCOMs be provided with limited acquisition authority. However, it would be inappropriate to create a new major acquisition group. Rather, a model like the DSCA should be adopted, which directs acquisition, using the Title 10 authorities to do so. Also, a Joint Task Force (JTF) procurement group should be established. This group could be under the Joint Staff with major roles for JFCOM and STRATCOM.
- With respect to testing, it is recommended that testbeds be expanded for product evaluation. Variants of these testbeds should be used to explore the impact of technology on mission effectiveness. This capability should be undertaken by the proposed SE&I organization.

Recently, CTNSP staff members have met with GEN Pace, CJCS, to discuss these rationalized recommendations.

JFCOM has recently undertaken a number of initiatives that are broadly consistent with the spirit of these recommendations. These include the receipt of national laboratory-like authority, the creation of the Office of Research and Technology Applications (ORTA), and the use of limited acquisition authority.

Critical Areas to Address

During the course of the IT program activities, CTNSP staff identified several additional critical IT issues that warrant immediate, in-depth assessment.

First, it is important to follow through on the recommendations that CTNSP staff formulated on the timely injection of innovative commercial IT from small and medium-size companies into DoD. CTNSP can play a major role in supporting the initiatives of JFCOM, ASD(NII), and the Joint Staff to ensure that follow-on activities are implemented effectively and efficiently.

Second, DoD is depending heavily on the concept of Net Centric Operations to achieve substantial advantage over future adversaries. Building on that concept, CTNSP has begun to examine the "next edge" of networked warfare. A forthcoming CTNSP book, *Battle-Wise: Gaining Cognitive Advantage in Networked Warfare,* calls for improving the cognitive abilities of warfighters, reforming command and control, and enhancing collective intelligence. This is an extremely fertile subject for follow-on research and analysis.

Third, CTNSP has begun to explore opportunities to employ commercial IT to enhance S&R operations. To shed light on this major challenge, CTNSP is in the process of generating two key products. First, it has produced a policy paper entitled "I-Power: Using the Information Revolution to Succeed in Stabilization & Reconstruction Operations." This paper includes a discussion of an information and communications technology (ICT) business model to guide the coordinated activities of the many participants in an S&R operation. Versions of this paper have been presented to several COCOMs, and it is serving to provide the framework for a serious dialogue on the issue. Second, working in partnership with the staff of the ASD(NII), an initial version of "A Primer on ICT Support for Civil-Military Coordination in S&R and Disaster Relief Operations" has been completed. It characterizes the existing ICT architecture, formulates options to ameliorate ICT shortfalls, and captures community best practices. Both products are living documents that must be expanded and evolved to guide the changes in this critical area.

Fourth, CTNSP is conducting a study of cyberpower to help understand the consequences of developments in cyber infrastructure, content, and institutions on the balance of power with potential adversaries of the U.S. In the absence of such a framework, the U.S. potentially will pursue fragmented, ill-coordinated cyber initiatives in the technical,

operational, legal, governance, and policy domains. The results of this study will serve to provide the intellectual underpinnings for coherent actions in this vital area.

Finally, CTNSP staff members have begun to focus on the challenges that the U.S. faces in the evolution of the Internet. From technical and operational perspectives, these involve the actions that the U.S. must undertake to reduce the vulnerabilities of the Internet to adversary actions. From a governance perspective, new mechanisms are required to ensure that the Internet needs of other nations are addressed without compromising the national interests of the U.S. These are timely, critical issues, which will require immediate, in-depth analyses.

The IT Program at CTNSP

Introduction

This paper documents the activities that have been performed in the Information Technology (IT) Program at the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU).

The report is organized as follows. A brief introduction presents the Congressional language that gave rise to the IT program and discusses the goals and objectives of the report. This is followed by a section that describes the nature of the IT problem. This section reports on several assessments, workshops, and conferences that were convened by CTNSP to capture the perspectives of key stakeholders—commercial industry, DoD laboratories, allies and partners, and key Asian nations—to explore important technology trends and to identify DoD needs for IT. Based on that understanding, staff members at CTNSP undertook several analyses, workshops, and prototypes to identify and explore possible solutions to injecting innovative commercial IT into DoD systems, including a prototype of a web portal, assessments of venture capital-related initiatives, lessons learned on the use of COTS IT in DoD systems, and assessment of the value of employing lead system integrators (LSIs) in acquiring complex system of systems. These efforts culminated in the CTNSP study "Actions to Enhance the Use of Commercial IT in DoD Systems." The study formulated six major recommendations that this report discusses in detail.

These initial activities have led to the identification of five critical IT issues that remain to be addressed: implementing CTNSP's major recommendations on the timely injection of innovative commercial IT from small and medium-size companies into DoD systems; evolving the concept of Net Centric Operations to gain cognitive advantage; employing commercial IT to enable stabilization and reconstruction (S&R) operations; developing a framework to address issues associated with cyberpower; and addressing challenges that the U.S. faces in evolving the Internet. The main report concludes with a brief summary of the key features of CTNSP's IT program and is followed with three appendixes. Appendix A contains synopses of the CTNSP activities discussed in this main report. Appendix B provides brief biographies of contributors to CTNSP studies and Appendix C provides a glossary of abbreviations and acronyms employed in this report.

Background

In the National Defense Authorization Act for Fiscal Year 2002, the Report of the Committee on Armed Services, House of Representatives, stated that the "Department of Defense can no longer depend on a dedicated defense industrial base, but will need to find ways to link advanced commercial technologies to improved military capabilities."

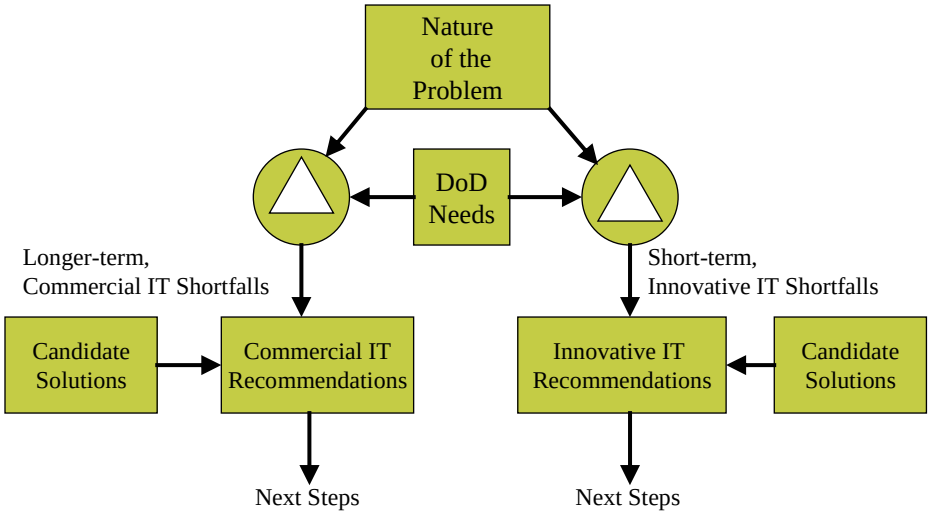
To respond to this circumstance, Congress asked CTNSP to develop a program "to find practical ways in which the defense information technology community can gain a mutual understanding of defense needs and industry capabilities and identify opportunities to integrate information technology innovations in the U.S. military strategy."

In the Report of the House Committee on Armed Services for the National Defense Authorization Act for Fiscal Year 2006, the Committee requested that a report be provided that documents "…the results of the program and plans for future efforts with the submission of the fiscal year 2007 budget request to Congress."

To achieve the IT program's objectives, CTNSP staff members led and participated in approximately 40 different activities over a 3-year period. These activities included studies and analyses, surveys, interviews, workshops, conferences, and prototypes. To elicit the best ideas, these activities involved the leading thinkers from the technology and policy communities in government, industry, academia, and think tanks. To derive the maximum benefit from the resources allocated to this effort, steps were taken to leverage other activities at the National Defense University—other studies at CTNSP and collaborative efforts with other Centers, such as the Institute for National Strategic Studies and other colleges, such as the Information Resources Management College.

The program adhered to the general roadmap depicted in figure 1.

Figure 1. Roadmap for the Report



To initiate the program, considerable effort was spent on understanding the true nature of the problem. This included understanding the perspectives of the various stakeholders and clarifying relevant technology trends. That was complemented by an effort to characterize DoD's IT needs. By comparing the nature of the problem to DoD's IT needs, two pictures emerged. First, an understanding was developed of DoD's need to inject commercial IT into DoD systems in the short-term, i.e., within a 6- to 18-month window. Second, commercial IT needs were identified to support the more traditional acquisition process, which takes place over several years. In support of the former issue, several studies were conducted to identify innovative options, such as the development of web portals and the use of venture capital-related mechanisms. Based upon these activities, a major presentation was developed, entitled "Actions to Enhance the Use of Commercial IT in DoD Systems," which has been briefed to the CJCS; VCJCS; Chiefs of Staff of the Services; Combatant Commander, JFCOM; and ASD(NII). Similarly, several studies were undertaken to explore options to inject commercial IT into more traditional DoD acquisitions. The studies included lessons learned from prior experiences and the use of lead system integrators (LSIs). Based on insights gained from that analysis, additional studies have explored innovative ways for DoD to exploit commercial IT over the long-term. This paper briefly identifies and discusses the activities that were undertaken to implement this roadmap.

Appendix A of this report provides more extensive synopses of these activities. The synopses describe the nature of each project, provide a project summary, identify major findings and recommendations, and discuss the project impact. It is important to note that, because the individual recommendations in these supporting activities have not been coordinated with DoD, they remain the personal recommendations of study authors.

Contextual Studies

The contextual efforts can be divided into two major categories. The first set of activities sought to characterize the nature of the problem. This consisted of two sub-categories: an understanding of the perspectives of the major stakeholders in the process, and an appreciation of key technology trends, particularly in the area of emerging IT vulnerabilities. The second category deals with DoD's requirements for IT. The latter effort subsumes several workshops and analyses that resulted in the generation of a monograph on the subject.

Alternative Stakeholder Perspectives

To capture the views of stakeholders, assessments were performed for four key classes: commercial industry (addressing the views of small, medium, and large commercial IT firms); DoD laboratories (considering the activities in each of the Services); allies and partners (focusing on the views of NATO allies and Sweden, a member of the Partnership for Peace); and key Asian nations (focusing on the activities in China and, to some extent, India). The following discussion identifies the major insights that emerged from these assessments.

***Commercial IT Perspectives*.** To capture the perspective of primarily small and medium-size commercial IT companies, a survey of IT industry was conducted by the University of Baltimore, under contract from CTNSP. The primary objective of this survey was to identify key obstacles to the injection of commercial IT into DoD systems by these IT companies.

The survey yielded a number of insights. The small and medium-size IT companies stated that they lacked visibility into DoD IT needs. They observed that doing business with the DoD involved excessive "red tape." As examples, they noted that the process is extremely slow and personnel-intensive (e.g., the need to perform additional record keeping). On a more fundamental basis, they viewed the DoD market as "exclusionary," and opined that they had a sense of "no opportunities." They cited several significant barriers to working with DoD, including the lack of information about how to contract with DoD and the challenge of coping with security requirements. With respect to the latter, many of these firms lack personnel with proper security clearances or facilities in which classified activities could be performed.

To focus the CTNSP efforts, a study was conducted on "Commercial IT Possibilities—Future Role in Military Operations." The primary purpose of this study was a proof of concept to identify that there were areas of commercial IT that held promise for DoD applications. Even though the study was not comprehensive, it did provide the proof of concept and identified three areas of commercial IT that appeared to be good matches for DoD needs: assured Information Assurance (IA) availability, information collection and retrieval, and information visualization and knowledge creation. The report went on to discuss two key issues. First, it emphasized the importance of identifying IT products early in their life-cycle. Early identification is important for two reasons: it provides the opportunity to influence the features of the product (e.g., allowing attributes important to the military to be added at reasonable cost while the product is still malleable) and it enables the commercial firm to address issues associated with competition or potential threats. Second, the report concluded that personal contacts matter. Entrepreneurs typically work outside traditional defense networks and find that they encounter high barriers to entry in the DoD market.

To elicit broad community perspectives on the use of COTS products to support DoD transformation, CTNSP convened a conference on "Commercial IT for Defense Transformation—Common Technology." The conference revealed that there will be a continuing need to require MILSPEC products for a variety of applications (e.g., weapons, sensors, and force protection), even though there is enormous promise for the enhanced use of COTS by the military.

With respect to the use of COTS products, both positive and negative dimensions were identified. On the positive side, it was concluded that the use of COTS products could serve to save time in acquiring systems, has the potential to save resources, and could ultimately enhance joint and multinational interoperability.

Several negative aspects of COTS also were cited. First, COTS products will be available to all buyers, including adversaries; equality of access might undermine the military strategy of achieving information and decision superiority. Second, COTS products will generally not include defense-specific features and technologically leading-edge capabilities. Furthermore, since the use of COTS applications can constrain the degrees of freedom available to the acquirer of systems, it may lead to sub-optimized DoD processes. The participants stressed that when a COTS product is modified, it generally ceases to be a COTS product (i.e., it is generally not covered by warranties and may not be compatible with future versions of the commercial product). Hence, adding MILSPEC modifications to COTS products should be resisted strongly.

The conference served to highlight two key residual issues. First, it observed that the DoD policy on Intellectual Property Rights (IPR) poses major problems for small and medium-size commercial IT firms. Thus, a new model might be desirable to ameliorate this barrier. Second, it was observed that Congressional constraints tend to adversely affect the use of COTS. Those constraints include issues of contracting flexibility and oversight.

The final CTNSP product on commercial IT corporate perspectives focused on one of the giants in the field as an example of how to deal with the larger IT companies: Microsoft. CTNSP staff convened several meetings with senior representatives of Microsoft to elicit their views on the role that Microsoft might play in support of DoD IT needs. On the positive side, Microsoft spends enormous resources on R&D (on the order of $40B over six years). Furthermore, Microsoft's corporate strategy is to seek closer ties with DoD, and Microsoft is embarking on activities that are important to DoD, including the creation of products that are more reliable and secure and the development of more user-friendly human-machine interfaces. On the negative side is the significant concern that Microsoft could overwhelm and dominate any smaller commercial IT companies that sought to provide innovative products to DoD.

Defense Laboratory Perspectives. To elicit the perspectives of the Defense Laboratories on IT, CTNSP conducted two complementary assessments. First, CTNSP conducted a Section 913 Report on Information Science and Technology and the DoD laboratories. The report sought to rate the relevance of work performed by the DoD laboratories and to gain a better understanding of them. The review was limited to laboratory work associated with sensors, IT, and weapons. One representative organization was selected from each Service: SPAWAR (USN), CECOM (USA), and AFRL (USAF). The review concluded that the work of the laboratories is indeed relevant to DoD. However, two important issues were raised. First, it was observed that the laboratories are placing too heavy an emphasis on short-term, quick-fix activities. Second, it was noted that each laboratory focuses almost exclusively on the needs of its own Service.

The second CTNSP study of defense laboratory perspectives explored the connectivity between the defense laboratories, industry, and academia in the area of IT. This study enumerated many of the opportunities for the defense labs to interact with these entities, such as Cooperative Research and Development Agreements (CRDAs) and Service-

sponsored institutes in academia. The assessment concluded that the levels and types of interaction are strong and healthy and that the scale and quality of collaboration is adequate.

NATO and Allied Perspectives. CTNSP conducted five studies to explore the IT perspectives of NATO nations and Sweden. As a point of departure, an assessment was performed of the extent and impact of the widening technology gap between the United States and NATO. The study observed that the United States invests over $13B annually in defense S&T. That sum exceeds the total annual defense spending of each of our NATO allies, with the exception of the UK, France, Germany, and Italy. It was concluded that the order-of-magnitude difference in defense funding between the United States and other NATO members, if sustained, will eventually cause such a wide gap in technical capabilities that divergence will occur. This divergence could be limited with a small, but consistently sustained increase in investment in allied S&T.

A second study on NATO, entitled "Bridging the Gap: European C4ISR Capabilities and Transatlantic Interoperability," developed insights that are at some variance with the prior study. It concluded that the gap is overstated. The authors noted that Europe possesses considerable C4ISR technology and capabilities in the defense and commercial sectors and that it can compete and cooperate with the United States and work through interoperability issues. At the time of the study, European nations did not take a network-centric approach to military planning. However, in the interim, many of our NATO allies have embraced network-enabled capabilities (NEC). From that vantage point, "plug and play" may be a good option for linking into U.S. systems.

A third NATO study addressed "The NATO Response Force (NRF): Facilitating Coalition Warfare Through Technology Transfer and Information Sharing." The authors examined the issues associated with the transfer of U.S. technology and information to stand up the NRF. The authors concluded that there is a tenuous link between the goals and operations of the NRF due to three factors: there is no specific plan or roadmap as to how the NRF will catalyze the acquisition of new capabilities; there is no clear plan to facilitate NRF interoperability; and there is no clarity concerning the extent to which the U.S. will contribute its advanced net centric "enablers" during NRF Phase II. They note that critical NRF technology transfer is needed to enhance interoperability and long term capability acquisition. However, current U.S. policy and processes would likely result in an expeditionary force with less potency due to limited interoperability and connectivity to advanced U.S. net-centric warfare enablers.

The final CTNSP study on NATO perspectives addressed "Transforming NATO Command and Control for Future Missions." The study looks at how NATO is integrating its networks to facilitate rapid political-military decisionmaking with capital cities and creating a mobile, net-enabled response force to implement collective decisions. The study concluded that the political decisions on mission transformation, although slow and deliberative, are largely complete. However, the acquisition of military capabilities to perform new missions remains hampered by resource constraints. Furthermore, adoption of emerging operational communications and information systems

(CIS) has progressed faster because experimental systems can be procured by the responsible NATO agency. However, the NATO system of standards setting remains archaic and is far too slow for the pace of CIS coming into military use by networked forces.

CTNSP staff complemented their assessments of NATO perspectives by undertaking an assessment of the role of commercial IT in Sweden's military systems. This study, entitled "Sweden's Approach to the Utilization of Commercial Information Technology for Military Applications," focuses on the policies and processes that enable the Swedish military to use high technology systems successfully to compensate for a small standing force. The authors observed that the Swedes are pursuing a military transformation strategy that is not unlike that of the U.S. At its foundation, they are exploiting sophisticated technology, mobility, and adaptability to counter unforeseen threats. Sweden's acquisition policy requires that commercial technology be used in military systems wherever possible. Although this policy is bearing fruit, the authors caution that the Swedish approach to the military use of commercial IT is still unproven and cannot simply be transplanted to the U.S. Among the reasons for exercising caution are differences between Sweden and the U.S. in three key dimensions. First, Sweden's economy and armed forces are miniscule in comparison to the U.S. Second, the Swedish acquisition community is extremely small and centralized. Finally, the fact that Sweden deals with fewer, smaller programs, dramatically simplifies such important functions as monitoring commercial IT for applicability and performing tradeoff studies to ascertain acceptability.

Asian Perspectives. CTNSP staff have conducted three studies aimed at exploring the IT perspectives of select Asian nations, with emphasis on China. As a point of departure, an initial study, "Beyond the Mainland: Chinese Telecommunications Expansion," explored the international security implications of Chinese telecommunications expansion. The study noted that China has developed one of the most advanced telecommunications infrastructures in the world. This capability has been achieved partially through China's purchase of several large telecommunications networks in Asia. As a consequence of China's emergence in this area, much of American telecommunications manufacturing capacity has moved to China. Due to this transition, China has significantly enhanced its engineering and network operations, management and executive capability, and information technology.

As a second perspective, CTNSP staff assessed "Global Networks: Emerging Constraints on Strategy." This paper assesses the changing geopolitical structure of the international telecommunications system and the consequences for the U.S. The paper observes that four major centers of telecommunications influence and innovation are emerging: the U.S., Europe, India, and China. In assessing this trend, three key aspects of the international telecommunications infrastructure are appearing. First, basic units of networks are domestic networks connected by international hubs. Second, national governmental funding for R&D is being replaced by funding from multinational corporations. Third, technological sharing and imitation is occurring. The consequence of this trend is two-fold. First, the technology gap in telecommunications between the U.S.

and other countries is closing. Second, the result of this closure of the technology gap may provide other nations with the opportunity to match America's power in selected areas.

The most recent CTNSP assessment in this area, "The New Reality of International Telecommunications Strategy," explores the relative decline of U.S. telecommunications leadership and assesses the consequences. Four significant insights emerged from this assessment. First, U.S. network operators in the international telecommunications market have often been replaced by Chinese and Indian companies. Second, the trend is for leading American companies to be the assemblers and sales distribution channels of Chinese manufacturers. Third, much of the key telecommunications equipment is based on open systems that are broadly available to potential adversaries. Finally, China is moving aggressively to advanced IT. As one manifestation, they are "leap frogging" to implement Internet Protocol version 6 (IPv6). It is hypothesized that this may prove advantageous to them in the military sphere.

Major Trends in Technology

As the second dimension of the nature of the problem, it is important to understand the major trends in IT. These trends were captured by CTNSP in two types of technology assessments. The first of these assessments explored developments that have fueled the exponential growth in IT capability and some that may slow it. The remaining assessments focused on the vulnerabilities that we foresee for IT. These vulnerabilities are a consequence of both technological developments and the emergence of adversaries who are more skilled in employing IT to exploit and degrade our systems.

As a foundation, the CTNSP staff undertook a study, entitled "Moore's Law: A DoD Perspective," to examine the prognosis for silicon integrated circuit (IC) technology from a DoD perspective. The study concluded that DoD has counted on rapid advances in electronics of all types to maintain technological superiority and is not prepared for a slowing rate of advance. However, solid-state microelectronics will enter a new regime over the next seven to ten years, when the current scaling paradigm will no longer hold. That is, the familiar "Moore's Law" doubling of IC density every 18-24 months will slow down. The report concludes that DoD should search aggressively for alternate paradigms beyond those on which Moore's Law is based to ensure new technology capabilities and that DoD should invest in long term research that focuses on new materials and new electronic phenomena in order to maintain information superiority and total situational awareness in the future.

In the area of IT vulnerabilities, CTNSP has undertaken two significant initiatives. First, a book was published entitled *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*. The objective of this project was to gain insight into DoD's transformation risks in four areas: trends in information system threats and vulnerabilities; vulnerabilities introduced by the complexity of the new digitized battlefield; the impact of degraded information systems on battlefield operations; and trends in information assurance technologies and system design. After exploring these

areas, three classes of threats and vulnerabilities were identified as being of particular concern: physical attack on critical information nodes, electromagnetic attacks against ground, airborne, or space-based information assets, and cyber attacks against information systems. It was observed that attacks and system failures are facilitated by the increased level of complexity inherent in the multiplicity of advanced systems.

Next, CTNSP convened a workshop on "Complexities and Critical Infrastructure Vulnerabilities" to identify issues related to critical infrastructure protection and cyber defense that require further study. As secondary objectives, the workshop was designed to promote social networking in the community and to educate the participants about the nature of the problem. As a result of the deliberations, it was concluded that our cyber infrastructure is fundamentally vulnerable and that the vulnerabilities are poorly understood. It was hypothesized that our knowledge of biology and biochemistry, if applied creatively, could prove to be useful in protecting critical infrastructure. The group stated that the U.S. Government needs to be doing much more than it is currently doing in the areas of offensive or defensive proactive infrastructure defense.

DoD Requirements

Multiple CTNSP studies on the nature of the IT problem have served to characterize the existing and projected capabilities of the key stakeholders and the associated technologies. To complement these studies, CTNSP undertook three initiatives to characterize DoD needs for IT. By comparing these IT needs against perceived IT trends, CTNSP was able to identify key shortfalls that needed to be addressed.

To establish a foundation for DoD needs, several workshops were convened, entitled "Connecting Service Requirements and Commercial Technology." These workshops sought to identify Service IT requirements and commercial IT that might be useful to the Services. The workshops revealed that industry is very interested in working with DoD to identify areas where it can provide DoD with state-of-the-art technologies. Through working with industry, DoD can better identify the best IT solutions possible.

One of DoD's flagship transformation activities is the Army's Future Combat Systems (FCS), which seeks to develop a "system of systems" subsuming eighteen systems plus an integrating network/command and control capability. In view of the criticality of this program, CTNSP performed a study entitled "Relevancy and Risk: The U.S. Army and FCS." This study explored the challenges facing the development of six critical FCS technologies. It was concluded that the least mature of these technologies is the network, which must be capable of supporting wideband, ad hoc networking in complex terrain. In addition, the performance of three of the technologies—the network, munitions, and robotics—is critical if the FCS concept is to be fully enabled. CTNSP staff observed that it is exceedingly difficult to predict when the sensor, robotics, and network technologies will exhibit the nonlinear advancement needed to satisfy FCS requirements.

Recently, CTNSP issued "Making IT Happen: Transforming Military Information Technology," which summarizes the IT thrusts of the Services, characterizes the nature of

the interoperability problem, and discusses the problem of sharing information with NATO allies. The monograph concludes that the Army's greatest unmet needs include the development of mobile, ad hoc networking protocols and architectures, collaborative Battle Command applications that can be executed over a distributed network, the fusion of data, interoperability, and computationally efficient modeling & simulation (M&S) of large scale communications and sensor networks. The study concluded that the Air Force has a serious imbalance between long-term and short-term information science research, with more emphasis needed on long-term research. One of the more contentious issues lies in the quest to enhance interoperability at the joint, interagency, and multinational levels, which requires a careful balancing of benefits and costs and coordinated initiatives at strategic, policy, management, operations, training, systems, and technical levels. Based on a series of case studies, the authors observed that a key to interoperability lies in the creation of testbeds to address many of these issues. Finally, it is noted that NATO is in the process of modernizing IT systems in three broad areas: optimizing management information systems, creating network-enabled military capabilities, and military information operations.

Recommended Actions

Preliminary Commercial IT Studies

This section of the report builds on our understanding of the problem to formulate recommended actions to enhance the rapid injection of commercial IT into DoD systems.

Based on our understanding of the nature of the problem and U.S. military requirements, several analyses, workshops, and prototypes were undertaken to identify and explore possible solutions to using commercial IT. Two perspectives were considered. In order to address the short-term problem of rapidly injecting commercial IT into DoD systems, initiatives were undertaken to develop the prototype of a web portal and an assessment was made of venture capital-related initiatives. Second, to address the issue of incorporating commercial IT in longer-term acquisition programs, two assessments were performed. Case studies were performed to identify lessons learned on the use of commercial IT in DoD systems and to explore the value of employing LSIs in acquiring complex systems of systems.

Short-Term Issues. CTNSP undertook a prototype effort to create an interactive website for JFCOM. The purpose of the website is to allow information exchange between government acquisition experts and the commercial sector. It is envisioned that such a capability would constitute a significant win for both DoD and the commercial sector. DoD would influence development of IT products by early engagement, gain early access to cutting-edge products, and review products without spinning up the acquisition process. IT companies would gain important market input for development, demonstrate market value to funding sources, build military contacts, and gain a foothold in the military market.

CTNSP subsequently undertook a study entitled "An Assessment of the Ability of Venture Capital-Related Initiatives to Support National Security Objectives." The study identifies issues associated with venture capital-related initiatives and formulates recommendations to enhance their utility to DoD. Currently, there are multiple models for employing venture capital-techniques in DoD. The study concluded that there is no single right way for DoD to employ these techniques. At this early stage in the life of these initiatives in OSD, the Services, CIA, and the National Geospatial-Intelligence Agency (NGA), it is difficult to characterize their success. However, early efforts to create and sustain a "community of practice" have been fruitful. They have stimulated the sharing of insights and resources and have begun to promote the systematic use of measures of merit for these initiatives. The major challenge for these initiatives is to inject identified product solutions into government systems. Problems include dealing with mismatches in technology (e.g., the proposed commercial IT that is to be injected and the DoD's IT infrastructure) and sustaining the product, including support of training and updating.

Longer-Term Issues. CTNSP performed several case studies of Army and Navy programs to generate lessons learned on using COTS in DoD systems. The study report, "Lessons Learned on Commercial IT in DoD Systems," concludes that the keys to successful COTS injection include use of an open system architecture and a spiral development process. The case studies reveal that there are many myths about the use of COTS that have to be recognized in order to take advantage of the benefits of COTS while avoiding potential pitfalls. For example, in certain circumstances, COTS-based system sustainability issues overwhelm acquisition costs. In addition, under some conditions, the costs to maintain a COTS-based system equal or exceed that of custom software. As a general rule, military IT systems involving the integration of multiple COTS components should avoid the modification of COTS products. Finally, demonstrations, pilots, and test beds are key tools for the acquisition and maintenance of a COTS-intensive IT system.

CTNSP also performed several studies of LSIs. These studies explore the issues associated with using an LSI to support the acquisition of complex systems of systems. The studies served to identify a set of best practices for the use of an LSI. These include the following:

- the LSI should augment the System Program Office (SPO) to lower overall risks;
- the Government's expectations of the LSI need to be articulated clearly;
- the Government must be resourced to maintain its accountability;
- the program must remain "right sized" in order to address risks adequately; and
- conflicts of interest must be recognized and addressed promptly.

Rapid Injection of Commercial IT into DoD Systems

Based on the supporting studies discussed above, several key dimensions of the problem have emerged. First, the successful injection of IT is critical if DoD is to accomplish the broad spectrum of missions that it must perform and maintain the technological lead that

it enjoys against its current adversaries. However, it is becoming apparent that much IT technological innovation is occurring outside the traditional DoD acquisition process. Consequently, DoD is missing major opportunities to capitalize on those technological innovations. This is particularly troublesome because potential adversaries—for example, transnational terrorists and potential near-peer nation-states such as China—have full access to the IT technological innovations that are emerging from commercial industry. This poses the concern that DoD's technological lead in the area of IT could erode substantially in the coming decades. This concern is exacerbated by the observation that DoD cooperation with the commercial IT industry is hamstrung in a variety of ways. These findings have led CTNSP to address the following key issue: How can DoD capture IT capabilities that have been developed outside the traditional processes?

Baseline. DoD has recognized the problem and sought to take steps to address it. A decade ago, Secretary of Defense William Perry issued a well-publicized white paper that stressed that DoD "…must increase access to commercial state-of-the-art technology."[1] More recently, in 2003, Deputy Secretary of Defense Paul Wolfowitz signed a revised DoD Instruction 5000.2 that mandated that the DoD acquisition process "…make maximum use of commercial off-the-shelf (COTS) technology."[2]

To comply with this guidance, DoD employs a broad spectrum of methods to capture commercial technology. However, the bulk of its resources are allocated to "business as usual" activities. This includes such processes as issuing requests for proposals (RFPs), supporting independent research and development (IR&D) activities by industry, conducting pilot activities, and promoting initiatives by program executive officers (PEOs). In general, these activities deliver systems to the user that are often characterized by timescales in excess of a decade, although expedited delivery of core capabilities and system increments is being sought through the adaptation of evolutionary acquisition strategies.

In an effort to be more consistent with the characteristic timescales of commercial IT products, DoD is turning to a variety of other techniques. These include the use of websites and bulletin boards to advertise DoD needs to commercial industry, the use of integrated process teams (IPTs) to facilitate communication among all the participants in the acquisition process, and the adoption of special initiatives. As an example of the latter, ASD(NII) has promoted the Rapid Acquisition Initiative-NetCentric (RAI-NC) to accelerate the acquisition of commercial IT products, but resource limitations have severely restricted the scope of this initiative.

Congress has consistently supported the Small Business Innovation Research (SBIR) program along with the related Small Business Technology Transfer (STTR) and Fast Track programs. As a benchmark, the annual DoD share of these activities is on the order

[1] Secretary of Defense William Perry, Memorandum on "Specifications & Standards – A New Way of Doing Business," June 29, 1994.
[2] Deputy Secretary of Defense Paul Wolfowitz, DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003.

of $1B. However, relatively few of these initiatives get to the third phase of the program, commercialization, which would facilitate their fielding to the force.

More recently, DoD and the Intelligence Community have sponsored venture capital-related initiatives to harness the knowledge and insights of venture capitalists and facilitate the identification and fielding of commercial products. These initiatives include the CIA's In-Q-Tel, NGA's Rosettex, OSD's Defense Venture Catalyst Initiative (DeVenCI), the Army's OnPoint, the Navy's Commercial Technology Transition Office (CTTO), and SOCOM's Arrowhead. Although many of these efforts are promising, most are currently in the pilot stage and are supported by relatively limited resources (less than $50M per year).[3]

Furthermore, DoD is using a variety of tools to facilitate the flow and expedited fielding of commercial technology. Specific examples include cooperative research and development agreements (CRDAs), advanced concept technology demonstrations (ACTDs), and Service-sponsored institutes. As an example of the latter, the Army has sponsored the establishment of the Institute for Creative Technologies (ICT) at the University of Southern California (USC) to tap the technological skills of the entertainment industry in Southern California.

Finally, there is an interesting array of COCOMs and Agency initiatives to capture commercial technology. One continuing effort is the Coalition Warrior Information Demonstration (CWID) (formerly the Joint Warrior Information Demonstration) in which the COCOMs, in concert with the Defense Information Systems Agency (DISA), sponsor a yearly event to identify promising new technologies. Other useful activities include the Enterprise Software Initiative (which promotes the joint acquisition of software), the Enterprise Integration Toolkit (to support the acquisition and management of COTS business systems), the DTIC web site and associated resources, and the resources of the Defense Acquisition University (DAU) (which provides acquisition courses to the DoD community along with a community of practice website) and the Information Resources Management College (IRMC).

Extensive as these initiatives are, they have not overcome the obstacles that make it difficult for DoD to identify and acquire commercial IT in a timely fashion. The next section of this report identifies and discusses those obstacles.

Obstacles. Six broad classes of obstacles have been identified that impede DoD's ability to capture IT capabilities developed outside the traditional defense acquisition process. These obstacles revolve around the fact that DoD constitutes a market for commercial IT products that is non-attractive, non-transparent, non-agile, non-dominant, and isolating. Furthermore, DoD's ability to tap commercial IT is sometimes limited by the attitudes of the prime contractors and LSIs that acquire major defense systems. Each of these obstacles is identified and discussed below.

[3] Stuart Starr, "An Assessment of the Ability of Venture Capital-Related Initiatives to Support National Security Objectives," CTNSP, NDU (forthcoming 2006).

Non-Attractive. As noted above, CTNSP sponsored a survey of small and medium-size commercial IT firms that infrequently do business with DoD.[4] Firms that currently do not engage in business with DoD gave the following major reasons for their reluctance to enter the DoD market:

- "They do not know what they want."
- "The application/bid process takes too long."
- "DoD only deals with large companies."
- "Our products are not needed by DoD."
- "We do not want to work with DoD."
- "There are too many barriers to the bid process."

Similarly, DoD conducted a study of commercial IT firms to learn why they are reluctant to do business with DoD.[5] The study concluded that non-traditional defense firms are reluctant to enter the defense market because of IPR issues (for example, small and medium-size firms are extremely reluctant to cede IPR to the Government); the long development times associated with defense procurements; and the substantial cost accounting, auditing, and oversight requirements levied by the Government.

Non-Transparent. In the CTNSP-sponsored survey of IT firms, current DoD contractors explained why they perceive DoD policies, processes, and procedures to be opaque. They noted that the process is too difficult, slow, and confusing. They decried the limited information that is available to small and medium-size business and noted the lack of opportunity for firms that have not won prior contracts. They also observed that it is desirable to ease the security clearance process and stated that the current DoD acquisition process is exclusionary. Finally, they complained that they lacked clear information about Federal contracting.

Non-Agile. The planning, programming, budgeting, and execution (PPBE) system requires participants to predict technology transitions 18 to 24 months in advance. However, the program manager community cannot always predict the pace of innovation two years in advance, and funding may not be available for fast-moving projects that are ready for transition. Consequently, a desirable S&T project may stall for two years awaiting funding (the so-called "valley of death").

Non-Dominant. In the 1960s, DoD was the dominant player in the IT market. However, the situation has changed dramatically over the last decade. As noted in the "Manager's Guide to Technology Transfers in an Evolutionary Acquisition Environment," "DoD is unable to acquire intellectual property rights for commercially developed technology, as it has done for defense-funded technologies in the past, because DoD's financial involvement will be limited and its demand is not dominant compared with the worldwide commercial market."[6]

---

[4] "Survey of Information Technology Firms," Schaefer Center for Public Policy, October 31, 2003.
[5] Defense Procurement and Acquisition Policy, OUSD(AT&L), "Manager's Guide to Technology Transfers in an Evolutionary Acquisition Environment," January 31, 2003.
[6] Ibid.

Isolating Market. Historically, DoD requirements (which tend to be battlefield oriented) demand capabilities that are not found in the commercial sector. A good example of this gap is illustrated in table 1, which compares the communications and networking characteristics of the commercial sector with those of the tactical military.[7] This table was derived from information provided at the 2004 Information System Technology (IST) Technology Area Review and Assessment (TARA). It compares communications and networking for the commercial sector and the tactical military user for six factors: mobile subscriber infrastructure, networks, antenna towers, frequency spectrum availability, protection, and low probability of detection/jam resistance. It can be seen that the military faces the problem of working in an environment where little or no infrastructure exists. Thus, it needs mobile/transportable, flexible resources that are highly protected from potential adversary actions. Even though there appears to be a broad chasm between the two needs, the commercial sector is actually beginning to offer commercial products that are more responsive to military needs.[8]

Table 1. Communications and Networking Comparison (2004 IST TARA)

Factor	Commercial	Tactical Military
Mobile Subscriber Infrastructure	Fixed	Mobile
Networks	Preconfigured	Ad hoc, self-organizing
Antenna Towers	Tall, fixed	Small, easily deployed
Frequency Spectrum Availability	Greater	Restricted (geographically)
Protection	None-to-privacy	None-to-TS/SI
Low Probability of Detection; Anti-jam	Not an issue	Critical

Primes/LSIs. During the course of ancillary studies, the roles of primes and LSIs were assessed with respect to the adoption/adaptation of commercial IT.[9] Three specific issues were identified that suggest that primes and LSIs may be a significant obstacle in this area. First, prime contractors may have a natural tendency to prefer internal technology because they can see the design and make it work. Second, prime contractors may have

[7] Information System Technology (IST) Technology Area Review & Assessment (TARA), conducted at Naval Research Laboratory, MD, July 2004.
[8] Discussions with representatives from Ericcson (Stockholm, Sweden), at CTNSP, NDU, May 2004.
[9] Kenneth Jordan, "Lessons Learned on Injecting Commercial IT into DoD Systems," CTNSP, NDU (Forthcoming 2006).

conflicting objectives about adopting technology from an outside provider. This can range from something as intangible as the "not invented here" syndrome, to more tangible issues, such as displacing the prime contractor's revenue base. In addition, primes may also be concerned about complex issues, such as problems with the timeliness and compatibility of technologies built by outside organizations.

Recommendations

To deal with the obstacles that limit DoD's ability to capture IT capabilities developed outside the defense acquisition process, a six-step approach was recommended: enhancing DoD-commercial communications and implementing organizational change, increasing DoD's resource flexibility, removing a variety of barriers to commercial IT acquisition, stimulating cultural change in the defense community, reviewing the testing process, and adapting requirements for specific missions. It must be emphasized that there is no single change, in and of itself, that will serve to mitigate these problems adequately. Thus, a suitable set of recommendations will have to be crafted and orchestrated if substantive improvement is to be achieved.

Enhance Communications/Organization. One of the fundamental problems that DoD faces is lack of knowledge about the products that the commercial IT community is creating. In particular, it lacks visibility into these products early in their life cycle, when DoD-required features could be designed with a relatively small cost. To address this issue, it is recommended strongly that a cadre of "techfinders" be created to conduct focused searches that could benefit the DoD community. It might be more appropriate to label these individuals "tech-prospectors," because their role is analogous to the miners that had to sort through extensive slag to find a few precious nuggets. These tech-prospectors could be organized to specialize in commercial IT areas that are potentially of greatest interest to DoD. As an initial taxonomy, it might be useful to track the IST TARA structure and organize tech-prospectors into the categories of communications and networking, information security, modeling and simulation, knowledge and information management, and computing and software technology. This structure would provide logical connections to existing members of the DoD S&T community.

Second, although the DoD community has begun to use the Web to enhance communications with the commercial sector, its initial efforts have been fragmented and only partially successful. It is recommended that DoD adopt the metaphor of a "virtual mall" in which "individual boutiques" could be embedded to respond to tailored needs.

To implement the virtual mall, a web portal should be established and maintained to coordinate the use of commercial IT. The virtual mall would be characterized by the following features. It would provide information to industry employing multi-layered access to ensure appropriate levels of security. It would encourage DoD collaborative information-sharing in a variety of ways, such as testing data, system reliability, and virtual IPTs. At the outset it would support joint efforts but would evolve over time to support multi-agency and coalition efforts.

As a key "boutique" element of the virtual mall it is recommended that a prototype web site along the lines of EMISARS (Early Military Involvement Speeds Acceptance and Results) be populated and maintained.[10]

Third, to deal with the lack of transparency that many small and medium-size commercial IT firms have complained about, it is recommended that "acquisition guides" be created and empowered to assist such firms. It is envisioned that these guides would assist companies as they traverse DoD's technical, procedural, and cultural barriers. In view of the potential demands on these resources, it is recommended that they limit their services to producers of products that are of highest value to DoD.

If these three recommendations are to be implemented effectively, it is vital that a new organization be created to perform those functions. It was recommended that this new organization be located at JFCOM (which could utilize a Joint Task Force approach) to ensure that its actions are responsive to the needs of the COCOMs who have the primary need for commercial IT products that can be implemented expeditiously (within 6 to 18 months). It is envisioned that JFCOM would create an entity that would operate the Web Portal and EMISARS, provide tech-prospectors and acquisition guides, and enhance internal DoD communications on commercial IT.

An additional recommendation is that consideration be given to the creation of other new institutions to address DoD's commercial IT needs. One possible step would be to create a Center of Excellence for the injection of commercial IT into DoD systems. By analogy, it might be conceived as a new, joint "Bell Labs" for the injection of commercial IT, with distributed reach to industry and academia.

In addition, an evaluation should be performed to assess the value of establishing collocated laboratories and manufacturing facilities that would bring together users, R&D staff, and manufacturers. The core of this capability could be a "purple" laboratory to coordinate the IT S&T activities of the individual Service labs. This capability would address the concern cited in an earlier CTNSP study, which concluded that the Service laboratories were excessively focused on individual Service needs. This organization could serve as a "skunk works," leveraging commercial industry capabilities.

Increase Resource Flexibility. If DoD is to improve its ability to capture commercial IT outside the traditional defense acquisition process, it will require additional resources. It is strongly recommended that this be done by providing COCOMs with a capability to ensure that acquisitions are of greatest value to them. This could be done by building on the limited acquisition authority model provided to JFCOM in a recent USD(AT&L) memorandum.[11] To minimize bureaucracy and inefficiency, it is recommended strongly that a new major acquisition group *not* be created.

---

[10] Joseph N. Mait, "EMISARS – Early Military Involvement Speeds Acceptance and Results: Introducing Innovative Information Technology Vendors to the Military Market," Standard Advantage, March 2004.
[11] Mike Wynne, Acting USD(AT&L), "Assistance to Commander, U.S. Joint Forces Command for Development and Acquisition of Certain Equipment," June 4, 2004.

Organizationally, it is recommended that a JTF procurement group be established to play this role. It was originally envisioned that the JTF would be led by JFCOM, with representation from the other COCOM's to elicit their inputs. (After further analysis, as discussed below, the Joint Staff might be best positioned to lead the group. It should be noted that as a parallel effort, Northern Command (NORTHCOM) could be given analogous procurement authority for information systems that support homeland defense and homeland security operations.)

If those new organizations are to implement prompt procurement of commercial IT products, the procurement group will require a flexible fund. Although it is premature to estimate the precise size of that fund, it would be appropriate to begin with a fund of approximately $300M per annum and evolve it based on successful performance.

In addition, the procurement group should administer the fund to facilitate the transition of commercial IT products from R&D to procurement. This fund would help avoid the "valley of death" cited above. In addition, such an initiative should include sufficient resources to support such critical functions as test and evaluation (particularly to ensure interoperability) and sustainment (for example, personnel training and upgrading systems as technology evolves). Furthermore, greater reprogramming flexibility should be allowed when commercial IT is to be acquired.

Decrease Barriers. An earlier section of this paper highlighted the barriers that inhibit DoD's ability to exploit commercial IT products. Several steps are recommended to lower selected acquisition barriers. First, DoD's rules on IPR should be changed. Given the concerns of small and medium-size, commercial IT companies, it would make sense to utilize a licensing vice a rights model for IPR. Second, to facilitate the navigation of the acquisition process, thresholds should be increased for the application of a simplified acquisition process. This would entail modifications to the Federal Acquisition Regulations (FAR).

Third, other transaction authority (OTA) should be used as the norm in acquiring commercial IT. Note that OTA authorizes commercial-type arrangements, not FAR-type contracting. In addition, OTA should be made available in procurements. Currently, OTA is generally available only for R&D and prototyping activities (although it had been applied to the Army's FCS activity, until that contract was revised recently).

Promote Cultural Change. It is well known that there is nothing more challenging than stimulating cultural change in a well-entrenched organization. However, if DoD is to be more agile and flexible in acquiring commercial IT products, it is vital that such a cultural change be implemented.

To initiate that process of cultural change, the following three steps are regarded as essential. First, steps must be taken to increase DoD education and training for commercial IT development and procurement. The key organizations in this process are DAU and IRMC. Several years ago DAU taught a module on this subject, but with the stress on the curriculum (given the recent changes in DoD requirements and acquisition

processes), its role in the curriculum has waned. It is important that the DAU update the commercial IT material and provide adequate room in the curriculum for this vital subject. More recently, IRMC has been playing an increasingly prominent role in IT education, and it has the capability to do more.

Second, changes must be made to provide incentives for program managers (PMs) and LSIs to use commercial technology. Since "what gets measured gets accomplished," it is suggested that performance ratings be instituted for PMs to assess their ability to transition commercial IT into fielded DoD systems. Similarly, steps should be taken to incentivize LSIs to manage commercial IT, though it should be noted that commercial IT is used effectively in some LSI-led programs.

Finally, GAO recently recommended best practices to acquire commercial-component business systems.[12] It is suggested that those best practices be adapted, as appropriate, by DoD.

Review Testing. A key issue in DoD's use of commercial IT is the testing process. Many vendors make claims for their products but it is necessary to adhere to the Reagan admonition: trust but verify. It is particularly important that these products be tested in environments that are representative of DoD's information infrastructure.

It is recommended that an evaluation be conducted to assess expanding Underwriter Laboratory-style testbeds to test the performance of candidate commercial IT products. In addition, many small and medium-size, commercial IT firms lack the clearances and facilities to perform testing in classified environments. Steps should be taken to establish those classified testing environments, perhaps on a "hoteling" or shared basis. In this latter area, it should be possible to use DoD laboratories and National laboratories more effectively.

It is important that DoD go beyond performance testing to evaluating the impact of potential commercial IT products on mission effectiveness. To do so, consideration should be given to expanding existing operational testbeds. As one step, a review should be conducted on the value of expanding the Service battle labs to play this role. In addition, NORTHCOM has discussed the creation of a "cyber-range" in which candidate commercial IT products could be evaluated to assess their potential impact on homeland defense and homeland security effectiveness. Consistent with NORTHCOM's interest in a cyber-range, JFCOM is in the process of implementing an Information Operations (IO) Range. The initial version of this capability is to be achieved in the summer of 2006 by integrating ten existing ranges. The initial capability will emphasize the evaluation of computer network attack capabilities, although the final IO Range is projected to support the evaluation of all of the pillars of IO by FY11.

[12] Government Accountability Office, "Information Technology, DoD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls," July 2004.

Adapt Requirements for Specific Missions. Commercial IT products have the potential to play a significant role in support of key specific missions. During the course of CTNSP IT research, several applications were identified that warrant further study. These include support to stabilization and reconstruction (S&R) activities, support to homeland security, support to such key cross-cutting installations as commissaries and hospitals, and support to IO.

In the area of S&R activities, the participants generally include DoD, inter-agency organizations, multinational military partners, international organizations, non-governmental organizations (NGOs), host nation organizations, and businesses. The importance of achieving a minimal level of interoperability to exchanging requisite information among participants implies the need for a common package of commercial IT resources. To support the creation of this common package, CTNSP has generated a "primer" to characterize Information Exchange Requirements (IERs), the information and communications technology (ICT) needed to support those IERs, the data strategy needed to implement net-centric operations, and the education and training required of the participants.

In support of homeland security, it has been proposed that commercial IT be used with the National Guard to provide a "backbone" network. Consistent with this concept, commercial IT packages would be provided to state and local organizations. A study of this proposal is required to establish its feasibility and cost.

The DoD has common IT requirements for a variety of such cross-cutting installations as commissaries, and hospitals. A study is required to ascertain whether commercial IT can be used cost-effectively to support those functions.

Recently, DoD has generated a draft DoD Directive for Information Operations to guide the maturation of this increasingly vital activity.[13] It is important that a study be undertaken to understand the role that commercial IT has to play in this mission area. This study should consider commercial IT from the perspective of computer network defense (for example, vulnerabilities in commercial IT products that could be exploited by an adversary), computer network exploitation (features of commercial IT that could be exploited by U.S. forces during various phases of conflict), and other computer network operations.

Follow-on Actions

The findings and recommendations of this study have been briefed widely within DoD to the decisionmakers at the highest levels. On July 27, 2005, this material was briefed to senior DoD decisionmakers in the "Tank." The audience included the CJCS, VCJCS, Commander JFCOM, and the Chiefs of Staff of the Services. At the conclusion of the briefing, then-VCJCS GEN Pace directed that LTG Shea, Director, J6, Joint Staff, pursue

[13] Gordon England, Acting Deputy Secretary of Defense, Draft DoD Directive 3600.1, "Information Operations," (in coordination).

options for rationalizing the CTNSP recommendations with on-going initiatives in the Joint Staff.

Subsequently, meetings were held with members of the Joint Staff and the Institute for Defense Analyses (IDA) to rationalize the recommendations. Follow-on discussions were conducted to explore options to modify three of the key recommendations: enhance communication/organization, increase flexibility, and review testing. Based on discussions with the Joint Staff, CTNSP staff have implemented the following modifications to the recommendations to enhance communication and organization:

- Create an organization for rapid capability delivery that could perform the roles of tech-prospector, acquisition guide, and champion of industry-DoD communication interface. This role could be played by JFCOM, perhaps in concert with STRATCOM and DISA.
- Create a Systems Engineering and Integration (SE&I) organization that would deal with system of systems issues. This might be resident at DISA with strong COCOM participation.

Those discussions have led CTNSP staff to implement the following modifications to the recommendations on increasing resource flexibility and review testing:

- With respect to increased resource flexibility, it is recommended that COCOMs be provided with limited acquisition authority. However, it would be inappropriate to create a new major acquisition group. Rather, a model like the Defense Security Cooperation Agency (DSCA) should be adopted, which directs acquisition, using the Title 10 authorities to do so. Also, a JTF procurement group should be established. This group could be under the Joint Staff with major roles for JFCOM and STRATCOM.
- With respect to testing, it is recommended that testbeds be expanded for product evaluation. Variants of these testbeds should be used to explore the impact of technology on mission effectiveness. This capability should be undertaken by the proposed SE&I organization.

Recently, CTNSP staff members have met with GEN Pace, CJCS, to discuss these rationalized recommendations.

It should be noted that JFCOM has recently undertaken a number of initiatives that are broadly consistent with the spirit of these recommendations. These include the receipt of National laboratory-like authority, the creation of the Office of Research and Technology Applications (ORTA), and the use of limited acquisition authority.

Critical Areas to Address

This section of the report discusses critical issues that warrant more in-depth analyses in the future. Building on the base of effective injection of commercial IT into DoD systems, CTNSP is beginning to address four major areas: the evolution and extension of

the concept of Net Centric Operations to gain cognitive advantage, the employment of commercial IT to enhance S&R operations, a study of cyberpower, and the challenges in evolving the Internet. Each of these areas is discussed below.

Evolving the Concept of Net Centric Operations to Gain Cognitive Advantage. CTNSP has performed a number of assessments to explore how advances in IT can help realize the vision of Net Centric Operations. As an example, in response to a request from Congress, the staff of CTNSP recently developed an Alternative Fleet Architecture Design. This study explored options for the USN to acquire substantially more, smaller ships, taking advantage of the flexibility provided by network-enabled operations.

Furthermore, it is understood that the concept of Net Centric Operations raises issues that transcend the physical and informational domains. If the advantages of Net Centric Operations are to be realized, it is vital to achieve a deeper understanding of the cognitive dimension of the problem. This entails issues such as "sensemaking," where the operational staff needs to formulate a meaningful conceptual framework into which relevant data and information can be aggregated.

In support of these issues, CTNSP staff undertook a study, "Battle-Wise: Gaining Cognitive Advantage in Networked Warfare." The study concluded that a battle-wise lead for the armed forces can be cultivated in three key areas, which must go hand-in-hand. First, the cognitive abilities of individual warfighters must be improved by strengthening recruiting standards and strategies, including requiring relevant education and training and identifying, retaining, promoting, and utilizing those who excel. Second, command and control should be reformed by expanding the opportunity for battle-wise problem solving from "the few" senior officers to "the many" junior officers. Such changes would permit more effective horizontal collaboration by enabling warfighters, units, and whole forces to solve problems at the lowest appropriate level. Finally, collective intelligence can be achieved by forming coherent, if temporary, teams to tackle particular operational problems to deliver sound decisions and offer greater flexibility than vertical command and control. Additional study is needed to refine and extend these major findings.

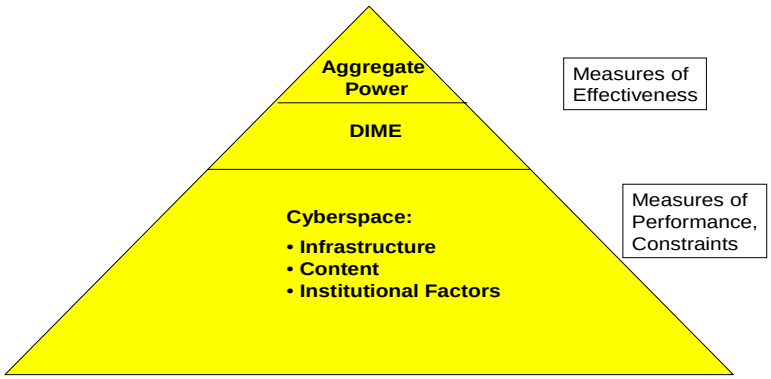
Employing Commercial IT to Enhance S&R Operations. To complement these studies, CTNSP staff have been working in partnership with ASD(NII) to explore the value of enhanced IT in support of S&R operations. As a tool for planners and operational staffs, CTNSP has produced a first version of a Primer on ICT for S&R. That Primer identifies the heterogeneous participants in civil-military coordination, describes their current ICT baseline, identifies significant shortfalls in that baseline, and formulates key initiatives to ameliorate those shortfalls. It also identifies a set of best practices based on experiences with recent S&R operations and disaster relief operations. It is envisioned that the Primer will be a "living document" that will help all members of the civil-military community acquire and employ ICT to enable them to work collaboratively in future S&R operations.

To support the policy community, CTNSP is refining a white paper entitled, "I-Power: Using the Information Revolution to Succeed in S&R Operations." This paper argues for the criticality of creating, sharing, and disseminating appropriate information to support S&R operations. Consistent with that observation, it maintains that senior civil-military leadership needs to recognize commercial ICT as a key enabler of the operation. Furthermore, an ICT Business Model is needed, inter alia, to facilitate coordination, cooperation, and information sharing with key partners. An ICT Business Plan is also needed for host nation capacity building. Early versions of this product have been briefed to selected COCOMs, and it is expected to evolve based on feedback from them.

In addition, an assessment was made of the value of using innovative IT to support net-capable operations in the context of S&R for Darfur, Sudan. That study, entitled "Learning from Darfur: Building a Net-Capable African Force to Stop Mass Killing," argues that IT has the potential to enhance dramatically the effectiveness of forces that could be forthcoming from the African Union.

Undertaking a Study of Cyberpower. The U.S. Government needs a framework for cyberpower to evaluate a broad range of policy issues that will have a profound effect upon the Nation's ability to exercise effective power against a broad range of potential adversaries. As a foundation for such a framework, CTNSP has developed a structure to facilitate the logical decomposition of the problem. At the base of the pyramid lies the infrastructure that subsumes the computers and communications that provide the foundation for cyberspace. This infrastructure can be viewed as layers that include component elements (e.g., integrated circuits), protocols and standards (e.g., Internet Protocol Version 6), applications (e.g., Voice Over IP), systems (e.g., routers, servers), and systems of systems (e.g., Internet Service Providers). All of the layers of this infrastructure are in the process of rapid change.

Figure 2. Decomposing Cyberspace



At the next level of the pyramid is the content that rides on the infrastructure. This includes the aggregate set of mass media as well as the information that is being disseminated on the Internet.

Furthermore, consideration has to be paid to the institutional factors that guide the use and limitations of cyberspace. This includes factors such as the institutions that control the Internet, the legal factors that limit the use of cyberspace, and the actions that are taken to defend cyberspace from attack.

At the next level of the pyramid are the classic pillars of power that are available to the Nation: Diplomacy, Informational, Military, and Economic (DIME). These pillars of power are strongly dependent on the underlying trends in the three lower layers of cyberspace. One of the major challenges is to understand the relationship between the evolution in cyberspace (characterized by measures of performance and constraints) and the aggregate power that the U.S. is able to achieve against potential adversaries such as nation states, terrorists, and transnational criminals (characterized by measures of effectiveness).

CTNSP is in the process of identifying, clarifying, and assessing the key policy issues associated with cyberpower. During the course of this effort, it is anticipated that the CTNSP team will explore the similarities among, and differences between, cyberspace and other global commons, such as the open seas and international air space. In addition, the effort will describe the law of cyberspace, both as it is and what it should be.

Ultimately, there is a need to develop cause-and-effect relationships between projected trends in cyberspace and the power that is achievable through DIME activities. This is an extremely challenging issue that will take the concerted efforts of the most capable interdisciplinary team that CTNSP can assemble. In view of the difficulty and importance of these issues, it will take several years of concerted effort to develop and refine the insights that the U.S. Government requires.

Addressing Challenges in Evolving the Internet. There are multiple issues associated with the Internet that require immediate attention. First, in recent years, the Internet has come under increasingly sophisticated attacks from a variety of sources (hackers, transnational criminals, agents of nation states). If the Internet is to evolve and prosper, it is vital that the U.S. identify and implement innovative actions to mitigate the effects of these evolving attacks. In particular, there is concern that the privately owned critical infrastructures of the United States might not be able to withstand a concerted attack by our adversaries. That raises the issue about the role of the Government in thwarting such threats.

Furthermore, the U.S. has controlled the Internet since its inception, but other institutions, for example, the United Nations and the European Union, are requesting a more

significant role.[14] This issue was raised at the recent World Summit on the Information Society (WSIS), but it is clear that additional in-depth analyses of the major issues will be needed.

Summary

It is widely recognized in the defense community that advances in IT are the key to transforming the military from an industrial age, platform-oriented force to an information age, net centric force. In support of that understanding, the IT program at CTNSP has created an extraordinary intellectual reservoir that can help DoD navigate that transformation effectively and efficiently. The cumulative value of the CTNSP work has been to support four objectives: clarify the nature of the IT problem that DoD faces; identify the needs of the users of this technology; identify and recommend actions to enhance the injection of commercial IT into DoD systems; and explore innovative ways of employing IT to enhance the effectiveness of future U.S. Government operations.

The IT program at CTNSP is notable for two key features. First, it has enlisted a multi-disciplinary set of the most knowledgeable and experienced members of the technology and national security policy communities. These complementary views have served to clarify the major technical issues and to explore the impact of those issues on national security. Second, it has resulted in the generation and dissemination of an exceptional set of peer-reviewed products that are characterized by their breadth and depth. It is particularly notable that, with extremely modest resources, CTNSP staff members have been able to produce nearly forty assessments, conferences, workshops, books, and prototypes that have shaped the discourse on this critical area in the defense community.

In view of the success of this pilot effort, CTNSP believes that the program should be continued on a formal, institutional basis. Building on the base that was established through the pilot effort, the staff at CTNSP are well-positioned to address critical issues where future commercial IT has the potential to affect U.S. Government capabilities and strategy. In particular, two broad areas require continuing assessment. First, with respect to short-term issues, there is a need to pursue opportunities to enhance the timely injection of innovative commercial IT from small and medium-size companies into DoD systems. Building on the results of CTNSP's work, JFCOM, ASD(NII), and the Joint Staff are pursuing this goal and are looking for continued support from CTNSP to implement key initiatives. Second, a host of long-term issues on commercial IT require serious, in-depth analyses. These include the evolution and extension of the concept of Net Centric Operations, the contribution of information and ICT to S&R operations, the formulation of a framework for cyberpower, and the evolution of the Internet. Given the extraordinary accomplishments of the CTNSP IT program and the significance of these future IT challenges, NDU believes that this pilot project should receive continued funding.

[14] Kenneth Neil Cukier, "Who Will Control the Internet?," *Foreign Affairs*, Vol. 8, No. 6, November/December 2005, pp. 7-13.

Appendix A

Synopses of Selected CTNSP Products

The views expressed in these summaries are those of the authors and do not necessarily reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government.

Overview

Key Stakeholder Perspectives

A. Commercial Industry

- Information Technology Industry Survey
- Commercial Information Technology Possibilities: Perspectives on its Future Role in Military Operations as Inspired by Visits to Selected Sites
- Common Technology 2002 Conference
- Microsoft Research and Development Program: An Overview

B. DoD Laboratories

- Information Science and Technology and the Department of Defense Laboratories
- A Study of the Connectivity between the Defense Laboratories, Industry, and Academia in the Area of Information Technology

C. NATO Allies and Partners

- NATO Technology: From Gap to Divergence?
- Bridging the Gap: European C4ISR Capabilities and Transatlantic Interoperability
- The NATO Response Force: Facilitating Coalition Warfare Through Technology Transfer and Information Sharing
- Transforming NATO Command and Control for Future Missions
- Sweden's Approach to the Utilization of Commercial Information Technology for Military Applications

D. Asian Nations

- Beyond the Mainland: Chinese Telecommunications Expansion
- Global Networks: Emerging Constraints on Strategy
- Constraints and Leap Frogs: The United States and the New Geopolitics of International Telecommunications

Trends in Information Technology

- Moore's Law: A Department of Defense Perspective
- Information Assurance: Trends in Vulnerabilities, Threats, and Technologies
- Complexity and Critical Infrastructure Vulnerabilities Workshop

DoD Requirements

- Connecting Service Requirements and Commercial Technology
- Relevancy and Risk: The U.S. Army and Future Combat Systems
- Making IT Happen: Transforming Military Information Technology

Possible Solutions to Utilizing Commercial IT

- Creating an Interactive Website for JFCOM

- An Assessment of the Ability of Venture Capital-Related Initiatives to Support National Security Objectives
- Lessons Learned on Commercial IT in DoD Systems
- An Assessment of Lead System Integrators/Transformation and the Defense Industrial Base: A New Model/ The Deepwater Program and the Role of Commercial Technology
- Actions to Enhance the Use of Commercial Information Technology in Department of Defense Systems

Extensions of Net Centric Operations

- Alternative Fleet Architecture Design
- Battle-Wise: Gaining Cognitive Advantage in Networked Warfare
- Extending the User's Reach: Responsive Networking for Integrated Military Operations

Information and Communications Technology (ICT) and Stabilization & Reconstruction (S&R)

- Stabilization & Reconstruction (S&R) Workshops
- Information Communications Technology (ICT) to Support Stabilization and Reconstruction (S&R) Operations
- Learning from Darfur: Building a Net-Capable African Force to Stop Mass Killing

Key Stakeholder Perspectives

A. Commercial Industry

Information Technology Industry Survey

Nature of Project
CTNSP commissioned a professional survey of primarily small and medium-size firms in the IT industry to gather statistically grounded information on commercial firms' attitudes toward doing business with DoD. The results would inform recommendations for regulatory or legislative improvement to the processes of DoD contracting. In particular, the interest was in speeding the contracting process to take early advantage of IT products that too often became obsolete before DoD could import them into its inventory.

Project Summary
In mid-2003, CTNSP retained University of Baltimore's Public Policy Research Center to survey the leaders of 4,600 IT firms across the United States. The purpose of the survey was to examine IT industry attitudes about doing business with DoD. Specifically, questions addressed why some businesses forego competing for DoD business and what companies that do contract with DoD think should be done to improve the contracting process. A report was produced in late 2003 that drew conclusions based on the responses of a statistically relevant industry sample. The respondents included firms that were currently doing business with DoD as well as firms that had had stopped doing business with DoD or had never ventured into the DoD market. Firms were divided into software and hardware firms as well as into business sectors (e.g., telecommunications, network integration, navigation, and intelligence).

Findings
- Many firms would like to do business with DoD but are unaware of what products are being sought due to a lack of visibility into DoD IT needs.
- Businesses that work with DoD were critical of red tape and additional record keeping.
- There is a sense of "no opportunities" among firms desiring to do business with DoD that have never won a DoD contract.
- There is a general lack of information about how to contract with DoD.
- There is a sense that DoD contracting is exclusionary and that some firms have an inside track to selection based on prior contract awards.
- The process of contractor selection and project award is too slow.
- Profit margins for DoD business are not a concern for most companies surveyed.
- Security requirements pose an obstacle that may be difficult to overcome for small and medium-size firms with limited resources.

- Firms not doing business with DoD want more accurate and detailed information about DoD requirements as well as a contact office or person where more information is available.
- The majority of firms not doing business with DoD would welcome being contacted by DoD.
- Most firms not doing business with DoD indicated the current bid and proposal process was too time and personnel intensive and had too little chance of success to warrant their doing business with DoD on their own.
- There is significant interest in a DoD "matchmaker" web portal where potential IT vendors could find project specifications and guidelines and as much detail about requirements as possible.
- Small and medium-size firms in particular would like to see DoD venture capital-like initiatives expand and reach out to smaller incubator enterprises.
- Most firms surveyed would compete for contracts if DoD made the process easier and faster.

Recommendations

- DoD should make information about its contracting processes more readily available, particularly to small and medium-size businesses, which may feel excluded or overwhelmed by current processes and security requirements.
- DoD should make its current and future IT requirements more readily known through an unclassified interactive website where IT firms could get information on DoD contacts and defense IT trends and requirements.
- Streamline the DoD contracting process to reduce red tape.
- Make contract announcements via multiple media, including list serves, websites, and fax lists.
- Expand DoD venture capital initiatives.

Project Impact

The survey report was published on-line. Copies of the survey were sent to members of Congress, relevant primary offices within DoD, policymakers and industry leaders. Results of the questionnaire were discussed with the Joint Chiefs. It has been used as a reference on IT industry attitudes on doing business with DoD as well as a benchmark for identifying areas where both regulatory and legislative changes might make the prospect of doing business with government more inviting, especially to small and medium-size enterprises. Many of the suggestions for change from this survey were incorporated into a separate report and briefing, entitled "Actions to Enhance the Use of Commercial IT in DoD Systems."

Commercial Information Technology Possibilities: Perspectives on its Future Role in Military Operations as Inspired by Visits to Selected Sites

Desmond Saunders-Newton, December 2003

Nature of Project

"Commercial Information Technology Possibilities" is a report on relevant emerging technologies available from selected companies.

Project Summary

This report describes CTNSP efforts to assess the availability of IT to support current and future military operations. It identifies technological products that are currently available and that can easily be adapted by users and institutions within DoD to effectively support future operations. The report describes a number of IT R&D efforts initiated and funded by private-sector firms. Eight firms were visited for this report. Included in this report are detailed case studies of relevant firms and the results of their R&D efforts, as well as reflections on the process of identifying relevant technologies in the commercial sector. It identifies a number of firms producing technologies associated with three categories important to current and future operations: assured information infrastructure availability; information retrieval and collection; and information visualization and knowledge creation.

Findings

- Based on the case studies derived from this study's sample, currently available technological products can be easily adopted by users and institutions within DoD.
- These technologies will be able to support future operations effectively.
- Personal and credible contacts matter:
    - Many entrepreneurs work outside traditional defense acquisition networks.
    - DoD is typically viewed as a market with high barriers to entry.
- Identifying technologies in their completed form often results in a decreased ability to influence the utility of the products in emerging defense systems.
- The ability to act earlier in the R&D cycle affords DoD an increased ability to deal with competition or potential threats.

Recommendations

While the products described in the report do not arise from DoD investments, they, and variants of the underlying technology, are capable of supporting future military operational concepts and addressing anticipated national security challenges.

Project Impact

This was a proof-of-concept study, confirming the central thesis of the entire project: that DoD is not acquiring emerging commercial technologies that could be useful to its operations. This report was published on-line as a CTNSP paper and has been distributed to the Services. It has been included in briefing packages to Rep. Adam Smith (WA) and his staff.

Common Technology 2002 Conference

Nature of Project
This project was a two-day workshop on IT attended by U.S. and European government and industry professionals and experts. The goal was to explore the potential and limitations of COTS, particularly as applied to command and control (C2) and information resource management activities. Participants and presenters engaged in discussions on possible solutions to DoD IT requirements over the next 20 years and shared ideas on IT applications for defense transformation.

Project Summary
Defense transformation is a single, DoD-wide enterprise composed of two distinct endeavors being pursued simultaneously. One is DoD corporate transformation, a major public-sector organization moving from old bureaucratic methods into best business practices, many already proven in the private sector. The other is DoD force transformation, aimed at transforming military doctrine, concepts, structures, and systems to achieve force-wide, network-centric capabilities. Both transformations are made essential by information age technologies, new threats, and the ubiquity of information. There is broad advocacy by industry and wide acceptance among DoD professionals, both civilian and military, that COTS systems provide the baseline for acquisition for defense transformation—least costly, most standardized, and easiest to upgrade to latest technologies.

Findings
- The largest industry players determine COTS standards. If DoD wants to influence COTS design standards, it must participate in industry project teams and standards-setting groups during the R&D phase of emerging technologies.
- The downside to COTS includes: it is available to everyone, including adversaries; it will not include defense-specific features; and leading edge capabilities are not included. COTS also can invert the idea that IT should support business processes; DoD processes may have to sub-optimize to conform to COTS applications.
- DoD access to pre-COTS will be limited and primarily through larger companies that have the ability to bring new technologies to market. Industry cautions that pre-COTS, often first invented in micro-enterprises, are unknowns. Direct adoption could stick DoD with costly, non-standard, non-upgradeable systems.
- Industry consolidation has given a new role to the remaining prime contractors. They have become the integrators of a multitude of critical second- and third-tier contractors increasingly involved in large and complex programs.
- If a single contractor in a critical supply area wins two or more consecutive major DoD contracts, it may be advisable to offer one or two competitor firms R&D contracts to maintain competition in the area.
- DoD can speed development of pre-COTS technologies by keeping industry informed of DoD interests in new technologies.

- DoD can work with venture capital firms to identify innovations; however, this method will usually not obviate the need to team with a larger industry player to develop and standardize the technology.
- DoD is increasing its investment in business software products and innovative management concepts to improve all its management processes.
- In spite of the emphasis on COTS for IT, DoD will continue to require MILSPEC technologies, most notably for weaponry, sensors, and force protection.
- At their boundaries, ERPs must interface with legacy systems—sub-systems, external systems, and inter-functional systems. Often the advantages of the investment are diluted until related systems can be upgraded.
- Network-centric warfighting means interoperable forces, which is difficult, expensive, and time consuming to achieve, both across the Services and with allies. Interoperability will require continuous, top-down emphasis.
- Networking of forces creates robust, real-time, information flows and moves "power to the edge" where information is most needed. The hierarchical command structure remains, but the flow of information does not parallel it as before. Rather, information flows both peer-to-peer and through the command chain.
- Brakes on transforming the DoD acquisition of IT from commercial developers include issues such as intellectual property rights (IPR), the burdensome government procurement system, and the potential reluctance of Congress to allow greater contracting flexibility and reduced Congressional oversight.

Recommendations

- When procuring systems, opt for COTS wherever possible and resist temptations to add MILSPEC modifications to requirements.
- Accept the notion of adjusting defense processes to COTS wherever commercial products can meet core operational requirements. This is particularly applicable to DoD "corporate transformation" processes such as planning, logistics, and human resources processes. These processes have parallels in the private sector for which COTS systems often feature "best practice" solutions.
- Military add-on features and "packaging" are acceptable, but the core should continue to be COTS.

Project Impact

This conference set the tone for the overall CTNSP IT project by 1) gathering information quickly about the nature of the project and the problem; 2) developing a network of individuals used throughout the project; 3) building connections between the commercial IT industry and DoD; and 4) creating ideas for future research in the IT program at CTNSP.

The conference was widely attended by the Services and joint military communities as well as industry representatives and several congressional staff members. The conference report was made available to the Assistant Secretary of Defense (Networking and Information Infrastructure) and the Chairman of the Joint Chiefs of Staff.

Microsoft Research and Development Program: An Overview

Nancy Palma, Summer 2004

Nature of Project

This report provides an overview of Microsoft's research and development (R&D) program in contributing to the general advancement of the IT industry.

Project Summary

With a budget of $6.8 billion in 2004 and proposed expenditures of $40 billion over the next six years, Microsoft takes the lead over all other companies in terms of R&D spending. Its large expenditures and high levels of innovation have allowed Microsoft to compete in an increasingly global, interconnected environment.

Findings

- Microsoft has been eager to develop closer ties to DoD and has created a special office headed by a retired two-star general.
- Concern exists that Microsoft would overwhelm and dominate smaller companies also trying to develop ties with DoD.
- Microsoft strives to make software more reliable and secure. Microsoft working groups do this by focusing on prevention and early detection of defects, creating more simplified systems, developing specialized algorithms to ensure the secure exchange of data across systems, and closing the gap between the time when vulnerability is discovered and when a patch is applied.
- Microsoft is overseeing efforts to enhance interaction between humans and computers by concentrating on programs that will analyze, understand, and generate languages, and by finding solutions to elements that hinder human-to-computer dialogue. Developments underway include a product that will abbreviate email messages so that they can be displayed on a cell phone. The Personalized Language Model seeks to enable a computer to learn the voice characteristics of individuals to translate and understand what is being said more accurately.
- To maximize communications and networking, Microsoft has led research in three areas: communications and collaboration, wireless and networking, and systems and networking. Some of the projects in these areas include: intelligent people-tracking, which automatically detects specific speakers in a meeting or lecture environment by using audio-visual data, XML compression and bandwidth sharing, and face recognition technologies that provide accurate face detection under variations of lighting, pose, and expression.

Recommendations

DoD should seek to take full advantage of the large Microsoft R&D program.

Project Impact

This overview provided the background for a briefing on commercial information technology.

B. DoD Laboratories

Information Science and Technology and the Department of Defense Laboratories

Don J. DeYoung, July 2002

Nature of Project

Section 913 of the National Defense Authorization Act for Fiscal Year 2000 required that the Secretary of Defense develop a performance review process for rating the relevance of the work performed by DoD laboratories. NDU was selected to design and implement this process. The objective of the NDU effort was twofold. Its primary purpose was to assess whether the S&T programs of the DoD laboratories were relevant to meeting the national security threats likely to arise over the next decade. The secondary purpose was to use the reviews as an opportunity to gain a better understanding of the laboratories. Three technology areas were chosen for analysis: sensors, IT, and weapons. These were selected because they best captured the range of capabilities that U.S. forces will need to achieve the full spectrum dominance called for in Joint Vision 2020.

Project Summary

CTNSP examined the DoD laboratories' most forward-looking work, which is in the S&T spectrum of the DoD research, development, test, and evaluation program. S&T includes the budget categories for Research (6.1), Applied Research (6.2), and Advanced Technology Development (6.3), which together provide the source of future military capabilities. While predicting the impact of S&T on future military requirements[15] may range from the feasible to the impossible, informed judgments about the relevance of individual projects to broad defense mission areas are possible. To reach these informed judgments, CTNSP relied on a study team of nine experts composed of four retired four-star Flag/General officers (one to represent each Service); three senior technical experts selected for both their expertise in scientific and technical matters and their experience in high-level defense (and non-defense) R&D management; and two members of a George Washington University (GWU) study team. The job of the GWU team was to provide a connection with a parallel study on the historical relevance of DoD laboratories. The study team made three site visits to major performers of Information S&T; Space and Naval Warfare (SPAWAR) Systems Center (SSC) in San Diego, California; Communications—Electronics Command (CECOM) Research, Development and Engineering Center (RDEC) in Ft. Monmouth, New Jersey; Air Force Research Laboratory (AFRL) in Rome, New York.

Findings

- The laboratories are performing relevant work; all understand their mission and are very knowledgeable of their respective Service's warfighting requirements.
- While there are high-quality S&T programs at each of the laboratories that have the potential to make a significant impact on the warfighting capabilities of the armed

[15] In this report, the term "requirement" is generally used in the colloquial sense pertaining to future warfighting concepts, capabilities, and needs.

services, there were very significant differences in quality between the best and "the rest" of the programs presented.
- The team found a much heavier emphasis on command R&D (i.e., problems of a short-term, "quick-fix" nature). This is understandable, given that these are more engineering centers than laboratories.
- Operating environments affect laboratory performance.
- Surveys show that the customers are involved and largely satisfied, but that there are also significant indications of concern.
- The laboratories are more stove-piped than they should be, with an almost exclusive focus on their own Services.

Recommendations
- Two of the three sites visited spent only about $1-2 million annually on research; most of them focus on applied research and advanced technology development. The study team concluded that this amount is not enough to conduct significant research explorations of a long-term, high-risk nature with a potential of revolutionary payoff.
- The study team strongly endorses a viewpoint expressed in a long line of studies beginning with the 1962 "Bell Report." That report, written by President Kennedy's Commission on Government R&D Contracting after the contracting abuses of the 1950s, affirmed the importance of maintaining in-house technical competence.
- Much more needs to be done to create a "purple" or "virtual joint" laboratory, especially in the IT/C4 area.

Project Impact
This report has been briefed and given to its sponsor, the Director, Defense Research and Engineering (DDR&E), Office of the Secretary of Defense. CTNSP used the findings in this report to suggest that the Information Science and Technology Laboratories are the most viable to become an integrated "joint" laboratory.

A Study of the Connectivity between the Defense Laboratories, Industry, and Academia in the Area of Information Technology

Dr. Alan Berman, July 2003 (revised April 2004)

Nature of Project

This report was commissioned to assess the current status of the DoD Laboratories' work in IT and the status of their relationship with the IT industry. The scope was later expanded to include their relationship with academia and other DoD laboratories. The impetus for the study was the Congressional mandate in FY02 for CTNSP to develop a pilot program "to find practical ways in which the defense information technology community can gain a mutual understanding of defense needs and industry capabilities and identify opportunities to integrate information technology innovations into the U.S. military strategy."

The defense laboratories, given their size and focus, are the best places to create an ongoing interface with research in the commercial IT industry. These defense laboratories are not taking the lead, because the commercial sector is so far ahead. The people working at the branch level in the laboratories need to be in constant contact with their counterparts in the private sector. The project was designed to find out to what degree this is occurring.

Project Summary

There are many ways that a DoD IT laboratory can interact with commercial organizations, academia, Federally Funded Research and Development Centers (FFRDCs) and other DoD and Government organizations that sponsor IT R&D. The modes of interaction considered by the CTNSP study team included:

- Cooperative research and development agreements (CRDAs)
- Sponsor-directed joint activities with industry or academia
- Service as contracting officer's technical representative (COTR) for IT R&D contracts with industry and academia
- Contractual relationship (industry or academic organization works for DoD IT laboratory under contract)
- DoD IT laboratory serving as contract monitor or agent for the Office of Naval Research or the Defense Advanced Research Projects Agency to oversee/manage R&D activity with industrial or academic performing organization
- 10 U.S.C.2563 "Sales of Articles or Services" agreements with industrial funding of DoD IT laboratories by industrial sponsors
- Faculty sabbaticals or summer employment
- Licensing and royalty agreements
- Joint authorship of papers submitted to refereed journals
- Direct support of graduate student research (salary and facility support)
- NRC/NAS/NAE post-doctoral programs
- Specialized local area partnerships (e.g. Center for Commercialization of Advance Technology)

- Membership in state or university sponsored consortia (e.g. California Institute for Telecommunications and Information Technologies)
- Ad hoc professional relationships between laboratory staff members and their peers in industry and academia

All of the organizations reviewed by the team could claim that, to some degree, they used all of these modes of interaction.

In response to its tasking, the team visited the following DoD IT laboratories:

- The SPAWAR Systems Center San Diego (SSC-SD)
- The Naval Research Laboratory (NRL), Washington, DC
- The Air Force Research Laboratory Information Directorate (AFRL/IF) or (AFRL-RRS) Rome, NY
- The Communications-Electronics Command (CECOM) Research, Development and Engineering Center (RDEC), Fort Monmouth, NJ
- The Marine Corps Warfighting Laboratory (MCWL), Quantico, VA

A typical visit involved an initial informal interview with the senior technical official and members of the senior management staff. The objectives of the visit were explained and the reactions of local management to the issues of laboratory interactions with industry, academia, FFRDCs, and sponsoring organizations were elicited. The informal interview was typically followed by a formal brief that presented the organization's overview of the situation. The overview brief was followed by briefings presented by 8 to 12 mid-level managers (typically branch heads) who discussed their programs, constraints, branch culture, and interactions with external organizations. Time was left for interactive discussions between the study team and the presenters. At the end of the day, a wrap-up discussion was held with senior laboratory management to discuss the sub-group's impressions.

Findings

- The level and types of interactions between DoD laboratories, IT industry, and IT developments in academia are generally strong and healthy.
- The scale and quality of collaborations between the DoD IT laboratories and the IT industry appear to be adequate, with mechanisms available to implement such interactions. Some technical and legal impediments exist, but management has always been able to find work-around solutions.
- Laboratory interaction with the IT industry is a function of the nature of the work of each laboratory, its perception of its mission, and its sources of funding. Laboratories use the same techniques to foster interactions with industry and academia.
- For a majority of the laboratories visited, management was proud of the professional interactions and the positions of influence that staff members hold in the worldwide IT community.
- It is important that Service laboratories have internal expertise to link to their external collaborators to advise senior leadership on acquisition decisions.

Recommendations

- DoD should submit an annual report to Congress that summarizes the extensive nature of the entire range of interactions of DoD IT laboratories with industry and academia. The report should be given broad dissemination and should be highlighted as one of the significant contributions of these organizations to the continuing development of the Nation's information technology infrastructure.
- The ad hoc nature of the numerous interactions that were discussed in this report should be institutionalized by a system of rewards and incentives. Among the rewards and incentives that should be considered are:
    - Financial awards or other recognition for DoD employees who serve as co-authors of publications with colleagues affiliated with industrial or academic organizations.
    - The establishment of a designated overhead account to pay for the activities of DoD IT laboratory personnel in support of national professional IT societies and standards-setting panels.
    - Annual performance evaluation factors of senior DoD IT laboratory managers should include activities that have resulted in demonstrable improvements in the interactions between their organizations and IT organizations in industry and academia.
    - Agencies that sponsor IT S&T activities in DoD laboratories should be directed to designate a small, fixed percentage of the funds that they transfer to the DoD IT laboratories for exclusive use as seed money for the development and support of new interactions with industrial and academic IT organizations.
- When setting up external centers of excellence for collaboration, the defense laboratories should:
    - Select the topical areas through a careful assessment of internal strengths and weaknesses.
    - Build external capability through consortia of academia and industry rather than individual firms or schools.
    - Make certain internal matching strengths are well supported.
    - Require agreement as to the movement of staff to and from centers.

Project Impact

The results of this study were included in briefing packages to Rep. Adam Smith (WA) and his staff. This report is publicly available on the CTNSP website but has not been formally published.

C. NATO Allies and Partners

NATO Technology: From Gap to Divergence?

Donald C. Daniel, July 2004

Nature of Project

The key premise of this report is to bring attention to the widening technology gap between the United States and NATO that, if left unchanged, could challenge the ability of NATO to function as a cohesive, multinational force in the future.

Project Summary

Over several decades, great disparities in the funding of defense research and technology by NATO members has produced a widening technological gap that threatens to become a divergence. The technology gap, in turn, is creating a capabilities gap that undercuts the operational effectiveness of NATO forces. But this divergence can be stopped. With slight modifications to current total defense expenditures, and using funds that will be available as they restructure their forces, European members could not only double their current investment, but take significant strides to ensure that they are not left behind in a world dominated by technology.

In addition, and of equal importance, the United States must share more of its fundamental basic and applied research with NATO partners, take a greater role in NATO's Research and Technology Organization (RTO), and increase participation across all technical areas in the RTO.

Findings

- The widening NATO capabilities gap is driven by many elements, the most important of which is defense spending.
- Small, but consistently sustained, investments in research and technology could make a significant difference in the technology gap.
- The United States invests over $13 billion annually in defense science and technology, exceeding the total annual defense investments of each of its NATO allies, except the UK, France, Germany, and Italy.
- The United States is the only nation in the world investing significantly in longer-term technologies, such as hypersonics.
- The order-of-magnitude differences in defense funding between the United States and other NATO members, if sustained, eventually will cause such a wide gap in technical capabilities that a divergence will occur.

Recommendations

- Every NATO member should commit to invest 3 percent of its military budget in defense research and technology programs.
- The United States should take a much more active role in sharing basic and applied research with NATO partners.

- Three key technologies should receive priority consideration for funding because of their importance to the mission of the NRF: information technology, distributed mission training, and sensor fusion.
- The RTO should seek more involvement and participation with defense industries from both sides of the Atlantic.
- The RTO should request the NATO Industrial Advisory Group (NIAG) to investigate the possible role of defense industries, with specific emphasis on the magnitude and technical excellence of non-government-sponsored, defense-relevant, industrial research.

Project Impact

This report was written by the Chairman of NATO's Research and Technology Board, who sought to implement many of the recommendations directly. The report has been briefed many times to a wide variety of audiences and has enjoyed a large audience in the NATO defense community in Europe. The paper was briefed in March 2005 in Paris, France, to the Federation for Strategic Research (FRS)/Royal United Services Institute for Defence and Security Studies (RUSI) Seminar on "Science and Technology for a Transforming Alliance," and to the NATO Army, Navy and Air Force Armament Group Chairs, as well as the NIAG Chair. It has also been briefed approximately four times at the NATO Staff Officers Orientation Course at NDU.

Bridging the Gap: European C4ISR Capabilities and Transatlantic Interoperability

Gordon Adams, Guy Ben-Ari, John Logsdon, Ray Williamson, November 2004

Nature of Project

The study analyzes the deployed and planned command, control, communications, computers, intelligence, reconnaissance, and surveillance (C4ISR) capabilities of seven European countries: France, the United Kingdom, Germany, Italy, the Netherlands, Spain, and Sweden. Capabilities discussions are divided into command and control (C2), communications and computers, and intelligence, surveillance, and reconnaissance (ISR). The study examines the extent to which advanced C4ISR and network doctrines figure in the defense planning of these nations and explores the extent of interoperability within and between these national forces and between the European forces and those of the United States. The study also examines the C4ISR doctrines and capabilities of the NATO alliances and C4ISR related work being done under the aegis of the European Union.

Project Summary

This study is the result of a two-year examination of the presumed defense technology gap between the United States and Europe. Its focus is information and communications technologies and their integration into military systems in what has come to be called network-centric warfare. These C4ISR technologies are at the heart of modern warfighting. They act not only as force multipliers for the military platforms into which they are integrated, but also as the means to better link air, sea, and land forces. Moreover, they can connect forces of different nationalities, enabling interoperability and the efficient use of military resources.

Findings

- The "gap" is overstated: Europe possesses considerable C4ISR technology and capabilities in defense and commercial sectors, can compete and cooperate with the United States, and can work interoperability issues.
- No European country takes a network-centric approach; "plug and play" is a good option for linking into U.S. systems.

Recommendations

- The EU needs to make intra-European and transatlantic interoperability in C4ISR within EU and NATO defense planning concept a priority. The study suggests that this commitment is not strong at the trans-European level and is uneven at the transatlantic level.
- Europeans need to have a clearer focus on C4ISR and inter-European as well as transatlantic interoperability, within NATO and within EU defense planning contexts.
- U.S. policy needs to understand European strategic perspectives, take European C4ISR technology and intentions seriously, work through NATO for greater connectivity, and reform the U.S. export control and technology transfer regime.

Project Impact

The study was published as CTNSP *Defense & Technology Paper* 5, which is distributed broadly to technologists, scientists, and policymakers. This study has been widely cited in the press. The article can be accessed on the CTNSP website at: http://www.ndu.edu/ctnsp/Def_Tech/C4ISR%20Gap_5.pdf.

The NATO Response Force: Facilitating Coalition Warfare Through Technology Transfer and Information Sharing

Jeffrey P. Bialos and Stuart H. Koehl, September 2005

Nature of Project

The report examines the issues associated with transferring U.S. technology and information to stand up the NATO Response Force (NRF) for early entry into high intensity conflicts.

Project Summary

At the Prague Summit in 2002, NATO Heads of State announced the creation of the NRF, a relatively small expeditionary force for "spearhead operations" in out-of-area conflicts. The central concept was to create, over time, an advanced, primarily European force for high-intensity conflicts that would catalyze force transformation and capability acquisition in Europe, promote transatlantic force interoperability, and provide Europe with out-of-area capabilities to match its new strategic direction. The hope was that this type of operational force would help revitalize the NATO alliance and improve transatlantic security relations.

A six-month rotational force, the NRF will have three phases of development: the stand-up of an initial "spearhead" force in 2004-6; full operational capability in 2006 (using European ground elements together with U.S. "enablers" in areas such as intelligence and surveillance and reconnaissance; and, in 2013 and beyond, the integration of European or NATO "enablers" as Europe and/or NATO acquire advanced capabilities.

Undoubtedly, the sharing of U.S. technology and technical information would facilitate, and in some cases be essential to, the development and fielding of a highly capable and interoperable NRF. Unfortunately, however, the history of recent transatlantic armaments initiatives suggests that the complex problems associated with such technology and information sharing with the United States could be a significant limiting factor in standing up the NRF. Hence, this study is primarily an examination of the issues associated with transferring U.S. technology and information needed for standing up such an advanced force for early entry into high intensity conflicts.

Section I of the analysis includes an understanding of the purposes, operational realities and developmental path of the NRF. Section II identifies and prioritizes the technology transfer and information sharing needs associated with standing up the NRF, including those related to force operation and doctrine, interoperability, and the incentives in the acquisition of enhanced capabilities. The research is based upon projections about the force's likely trajectory. Section III assesses the specific technology transfer issues, concerns and impediments likely to arise with respect to the releasability of needed technologies, and information sharing under applicable U.S. laws, rules and policies. This section also provides recommendations on specific and realistic steps needed to address these concerns so that the NRF can achieve its stated purposes.

Findings

- The NRF—a tenuous link between goals and operations.
  - There is no specific plan or roadmap regarding how the NRF will catalyze the acquisition of new capabilities.
  - There also is no clear plan to facilitate NRF interoperability.
  - There is no clarity concerning the extent to which the United States will contribute its advanced net-centric "enablers" during NRF Phase II.
- Critical NRF technology transfer needs relate to interoperability and long-term capability acquisition.
  - Interoperability concerns, technology transfers, and information sharing are necessary for full situational awareness.
  - Acquisition issues must be addressed to meet the long-term goal of European *capability* acquisition for NRF phase III.
- Current U.S. policy and processes would likely result in a constrained NRF with limited interoperability, limited connectivity to advanced U.S. net centric warfare enablers and, hence, less potency as an expeditionary force.
  - The cumulative thrust of current U.S. policies and programs undermines rather than facilitates allied force interoperability.
  - U.S. national disclosure policy and technology transfer rules are at odds with a changing security paradigm with an emphasis on coalition warfighting.
  - Interoperability initiatives have not been successful.
  - The "interoperability gap" will worsen, not improve, due to divergences in transatlantic spending patterns.

Recommendations

- Develop overall C4 architecture for use with potential coalition partners.
- The United States and its NATO partners should adopt a range of other necessary steps to improve interoperability.
- The United States should adopt new "top down" approaches to technology transfer and information sharing— including considering "one stop shopping" modalities and other more flexible mechanisms that recognize the necessities of sharing information on a sustained basis during the planning, training, and actual operations necessary for successful coalition operations.
- The United States should adopt a more flexible approach to information sharing that gives more priority to coalition warfare.
- The United States should tackle the "enabling" issues of technology transfer reform, exert leadership, and develop meaningful and comprehensive modalities to this end.

Project Impact

The research was published as a CTNSP *Defense & Technology Paper* 18 with a distribution of 1,500. The report can be found on the CTNSP website at: http://www.ndu.edu/ctnsp/Def_Tech/DTP%2018%20NATO%20Response%20Force.pdf.

Transforming NATO Command and Control for Future Missions

Charles L. Barry, June 2003

Nature of Project

This report analyzes NATO's transforming C3 systems as well as its Communications and Information Systems (CIS) architecture. It is the result of a year-long study of emergent decisions to make alliance decisionmaking, planning, and implementation of forces more responsive to new missions. In particular, it looks at how NATO is integrating its networks to facilitate rapid political-military decisionmaking with capital cities and to create a mobile, net-enabled response force to implement collective decisions.

Project Summary

NATO C3 and CIS are examined in depth, and the report concludes that the blueprint for transformed alliance command and control are in place. The main factor impeding its realization is national investment in the systems necessary to network forces as prescribed by NATO's latest technical and operational architectures, including C3 for forces deployed well beyond NATO frontiers. Nations are also slow to agree to increase NATO spending on CIS. Notwithstanding, the analysis concludes that almost all legacy systems are programmed for replacement by newer systems largely based on COTS systems that are less costly and more readily upgradeable. While the command structure is more streamlined and newer systems are slowly coming on line, some basic references have not been changed, such as interoperability levels and command relationships. These, too, will have to come under scrutiny by Allied Command Transformation as NATO gains operational experience in extended range C3. This report should be re-examined in 2006 due to the rapid pace of change toward networked forces and continuing mission evolution, including the growth in NATO stability operations.

Findings

- NATO has been transforming its forces since the end of the Cold War from a focus on territorial defense to a focus on crisis response in protection of collective allied interests far beyond Europe. The political decisions on mission transformation, though slow and deliberative, are largely complete.
- The acquisition of military capabilities to perform new missions remains hampered by resource constraints, especially at the national level among European NATO members.
- Alliance adoption of emerging operational CIS has progressed faster because experimental systems can be procured by the responsible NATO agency when funded by NATO commanders with limited resources, both for exercises and actual NATO operations in Bosnia, Afghanistan, and elsewhere.
- However, deployed NATO forces require new doctrine for logistical support and sustainment cost sharing that recognizes that few nations can sustain their own forces over long distances independently—nor should NATO want multiple independent logistics communications, information, and transportation systems.
- The NATO system of standards setting remains archaic and is far too slow for the pace of CIS coming into military use by networked forces. Before a standard is

agreed by all NATO nations, the technology under consideration is often already obsolete.

Recommendations

- NATO should expedite the acquisition of systems its members have already agreed are essential to transform NATO forces for future missions.
- NATO members should increase their national investment in CIS so that they do not become disconnected as NATO transitions to deployable network enabled operations.
- As a priority, NATO should concentrate on transformation of the necessary C3 systems and CIS to support the NATO Response Force and a deployable Coalition JTF HQ and Logistic Center.
- ACT should invest in the necessary exercises, experimentation, and joint multinational doctrine to establish optimum alliance network enabled forces and supporting command and control architectures.

Project Impact

This analysis has been widely hailed for its thoroughness and comprehensive analysis of all aspects of NATO command and control. It is valued in particular for grounding NATO CIS in the context of the full breadth of command and control transformation, including command relationships, levels of interoperability, various response force structures, and major systems architectures. The paper has been widely distributed, including overseas, in print and electronic formats. It has been selected as a reference at the NATO library in Brussels. Due to the pace of systems and mission evolution, there have been calls to reexamine NATO's command and control transformation in 2006. By then, with the NRF fully operational, the contribution to future missions, including stability operations, will need to be better understood from a U.S. perspective. The paper can be found on the CTNSP website at:
http://www.ndu.edu/inss/DefHor/DH28/DH28.pdf .

Sweden's Approach to the Utilization of Commercial Information Technology for Military Applications

Franklin D. Kramer and John C. Cittadino, October 2005

Nature of Project

This paper focuses on the policies and processes that enable the Swedish military's successful use of high-technology military capabilities to compensate for a small standing force. Sweden was picked as a case study to examine government-industry relations to determine ways to improve DoD's ability to capitalize on the use of commercial information technology (CIT) in military systems.

Project Summary

This case study found more similarities than differences in Swedish and American policies and processes for acquiring CIT for military systems. The most significant difference is that in Sweden, the policy for maximum utilization of CIT has been embraced by government and industry participants in the acquisition process, whereas Americans still debate whether CIT can do the job in warfighter or other DoD applications. Furthermore, Sweden has initiated an acquisition process that *routinely* examines all requirements to determine the potential to do the job with CIT and then performs tradeoff analyses to determine acceptance.

Findings

- Swedish acquisition policy requires that commercial technology be used in military systems wherever possible.
- A 1999 parliamentary decision put the Swedish armed forces on a path of modernization to counter lack of manpower with sophisticated technology, mobility, and adaptability to meet new and unforeseen threats. This in not unlike the American approach to military transformation.
- The Swedish approach to military use of CIT cannot simply be transplanted to the United States since Swedish policies in this area are new and the government does not yet have much experience with the results.
- Sweden enjoys many advantages over the United States in innovating in procurement:
    - The nation and its armed forces are small; fewer and smaller programs simplify monitoring for CIT applicability and performing tradeoff studies to ascertain acceptability.
    - Acquisition is centralized, and a small (20-person) headquarters staff can ensure that the policy of employing CIT is being followed to the highest degree practical.
    - Many of Sweden's military systems are procured internationally.

Recommendations

- Establish a center of excellence to monitor the status of CIT and publish information online for all DoD developers. Such a center could be established at JFCOM in conjunction with its C4ISR testbed capability.

- Establish a methodology to be used by all DoD acquisition centers to review new developments and major upgrades for applicability of CIT to meet requirements. Such a methodology could be developed at the Defense Acquisition University.
- Include in the Defense Acquisition Board process a requirement to present tradeoff analysis on CIT considered to meet program requirements.
- Rather than develop a new system (primarily software) to meet the way the organization "has always done business," encourage the user to consider changing the way of doing business when a CIT product implements a more efficient/effective way.
- Introduce more flexibility in acquisition by providing a statement in all RFPs that use of CIT is encouraged and that tradeoffs, including the opportunity to challenge specifications, are invited.
- Explore methods of motivating defense contractors, especially the major system integrators, to use more CIT vice tailored development.
- Take a more proactive role participating in international standards organizations to influence and stay abreast of commercial standards that drive new technology.

Project Impact

The report was published as *Defense Horizons* 50 and distributed to over 4,000 people. The report can be found on the CTNSP website at: http://www.ndu.edu/ctnsp/defense_horizons/DH_50.pdf .

D. Asian Nations

Beyond the Mainland: Chinese Telecommunications Expansion

Robert C. Fonow, July 2003

Nature of Project

Commercial Information Technology (CIT) is now available globally—it is no longer a technology the United States or DoD has proprietary rights over. CIT is growing not only with our European allies but with potential adversaries as well. This article examines the international security implications of Chinese telecommunications expansion.

Project Summary

Telecommunications development, a major component of IT, is a function of national capabilities. In the last 10 years, China has developed one of the most advanced telecommunications infrastructures in the world, partly through the purchase of several large telecommunications networks in Asia that were previously owned by U.S. investors. The result is that the American telecommunications manufacturing industry has predominately moved to China. Through its growing telecommunications industry, China has experienced improvements in engineering and network operations, as well as an enhanced management and executive capability at the expense of U.S. technological and commercial hegemony. This in turn has facilitated the general expansion of IT in China. Notable is the impact that information technology will have on the advancement of Chinese warfare. The growth and development of China's telecommunications assets pose a national security threat to the United States. Without stronger U.S. trade diplomacy, China will eventually usurp the advantages held by the United States in controlling the telecommunications environment in Asia and between the United States and Asia.

Findings

- Several features are notable in China's technical policy, including import substitution to protect domestic industries by subsidizing local firms, financial support for indigenous technology products, and increasingly open policies designed to attract foreign investment and technology flows.
- China's reliance on an external market will mean an increasing emphasis on the importation and replication of configuration technologies rather than a reliance on complete systems, which include proprietary knowledge, which is more difficult to engineer. This poses a threat to the preservation of U.S. technology and research and development.
- China's expansion into international telecommunications will make it more difficult for U.S. diplomats and trade negotiators to mold economic policies in Asia.
- Recent advances in Chinese commercial technology development indicate a capability for similar military advances, particularly information warfare. China's accumulation of wealth from its telecommunications industry could also be used to purchase weapons.

Recommendations

- A favorable competitive climate should be ensured within the United States to accelerate technical innovation. The Federal Communications Commission must begin to recognize that it is now an instrument of national security.
- Policymakers, specifically the Committee on Foreign Investments in the United States, must become more aware of the complexities and interlocking ownership of the international telecommunications infrastructure.
- It is important to keep a close watch on the contribution that American allies make to Chinese technology.

Project Impact

Published as *Defense Horizons* 29 and distributed to 4000 people. The report can be found on the CTSNP website at: http://www.ndu.edu/inss/DefHor/DH29/DH29.pdf.

Global Networks: Emerging Constraints on Strategy

Robert Fonow, July 2004

Nature of Project

This article assesses the changing geopolitical structure of the international telecommunications system and analyzes the problems for the United States in a vastly expanding information technology environment.

Project Summary

The international communications system is rebalancing into new centers of influence and innovation—Europe, India, and China are emerging as centers of IT development. If the current trend of regionalization of communications technologies persists, the United States will be hard pressed to keep a strategic advantage in network capability. There is also a trend of an emerging unitary global telecommunications system outside the complete control of any one political sovereign. Three aspects of the international telecommunications infrastructure are factors in the rebalancing of the system: the basic units of networks are still domestic networks that are connected by international hubs; national government funding for research and development is being replaced by funding from multinational corporations; and technology sharing and imitation is occurring. The result is the closing of the technology gap between the United States and other countries. At the very least, American technical power, and by extension its military power—especially aspects that are based on international communications networks—may be severely constrained in the future.

Findings

- The emergence of communications clusters will lead to the extension and solidification of regional culture (i.e. the extension of Chinese culture throughout East and Southeast Asia).
- In India, the economic development initiated by homegrown entrepreneurs may give India a long-term advantage over China. India has spawned a number of indigenous companies that compete internationally with the best American and European companies.
- Chinese companies are likely to replace Western companies as vendors of choice for infrastructure expansion in developing countries based on China's low-cost equipment and expanding research and development spending.
- China is joining India and the Philippines as a destination for outsourced service jobs.
- While Europe as a whole seems reluctant to use telecommunications and IT to operate more efficiently and to exploit market opportunities, specific countries are finding unique niches in telecommunications. Finland is the most "wired" country in the world and home to Nokia, and Russia has critical technical ties with China and India.
- Since telecommunications facilitates information warfare and network warfare as much as it facilitates trade, political control of military technologies is becoming increasingly difficult. China and India will be able to develop offensive information warfare capability.

- Ultimately, the security of the United States, in a strategic environment dominated by information and network warfare, depends more than ever on the education of its population. More specifically, enlisted recruitment and retention, key factors in maintaining service-level information warfare capabilities, will increasingly depend on educational and promotional opportunities.

Recommendations

- From a public policy perspective, it will become increasingly important to fund American postgraduates for programs abroad to understand the international telecommunications system in depth.
- Scholarships are needed to send both civilians and junior military officers to technical and management programs in countries such as China, Russia, India, Romania, Brazil, and Indonesia.
- The human resource and training functions of the military must also change to ensure a very high degree of information warfare capability. The military should send more junior officers abroad on Master's degree and Ph.D. programs—and to civilian universities, not just military academies.
- DoD should support accelerated degree programs at an undergraduate college for enlisted and junior noncommissioned officer staff. Prototypes of this program could be developed by the National Defense University. The objective would be to produce trained cadres of information warfare specialists in the mid- and senior enlisted ranks.

Project Impact

Published as *Defense Horizons* 43 and distributed to 4,000 people. The report can be found on the CTSNP website at: http://www.ndu.edu/ctnsp/defense_horizons/DH43.pdf.

The New Reality of International Telecommunications Strategy

Robert Fonow, January 2006

Nature of Project

This paper traces the relative decline of U.S. telecommunications leadership from both geopolitical and technical perspectives, as well as discusses the problems that this decline produces in the area of U.S. network-centric military operations.

Project Summary

As unlikely as it seems, the United States is rapidly losing primacy in international telecommunications. Within five to ten years, the United States will be one of several regional telecommunications centers, and not necessarily the most powerful and influential. This is a consequence of greater intra-regional telecommunication links between Asian and European networks, accelerating technical expertise and changing education demographics within these regions, the capability of competitive nations to develop leap frog technologies in IT, and technology transfer of commercial IT and outsourcing of their manufacture to competitive countries outside of the United States These telecommunications trends have profound effects on U.S. national security. The telecommunications network system that the battle space relies on is not only experiencing competition, but is more than ever depending on a fragile telecommunications network infrastructure that is increasingly international and ceasing to be controlled by U.S. military authorities. This represents a threat to future U.S. military operations in the area of network-centric warfare.

Findings

- The United States owns only a very small share of the international telecommunications network; U.S. network operators in the international telecommunications market have been replaced by Chinese and Indian companies.
- Increasingly, network-centric warfare will depend on foreign manufactured equipment at the end of foreign-managed circuits, and run by foreign contract engineers. The leading American companies producing and selling net-centric operations (NCO) equipment and services are, more and more, the assemblers and sales distribution channels of Chinese manufacturers.
- Most DoD traffic crosses other national networks, including those of potential adversaries, thus foreign nationals control U.S. military information once it leaves the United States Though U.S. critical military traffic is encrypted, other countries control much of the routing infrastructure.
- Much of the equipment and software that supports NCO is based on open systems. All potential adversaries have the same equipment and operating systems. It will become increasingly difficult to develop unique applications that cannot be replicated.
- NCO rests on a very fragile infrastructure that can be crashed by anyone with a serious intention to do so. The vulnerability points are easy to locate and easily destroyed by any reasonably informed terrorist organization, and certainly any state adversary with its own telecommunications infrastructure. Particularly, U.S. leadership is threatened in the telecommunications technologies that make up the

underlying routing and protocol fabric of the Internet. Internet Protocol version 6 is of particular importance because it will be the primary Internet connection protocol for both military and security applications worldwide.

- Chinese R&D is sufficiently robust now to enable China to develop its own communications systems and the software to run them. R&D activity includes integrating foreign technology with local systems or making foreign technology compatible with Chinese technical standards. This latter form of knowledge transfer (systems and standards integration capabilities), in particular, could be useful to China's defense modernization goals, especially in developing low-cost asymmetric capabilities. The growth of the low-cost base software and semiconductor industry in China, which provides the underlying technologies for all equipment and applications, permits experimentation in product design and development.

Recommendations

- There is a need for a more highly developed awareness of the technical power, particularly in telecommunications, of U.S. economic competitors and potential adversaries. The United States must reexamine its current defense policies in regard to telecommunications so that U.S. national security is not threatened by a decline in telecommunications leadership.

Project Impact

Published as *Defense & Technology Paper* 23, January 2006.

Trends in Information Technology

Moore's Law: A Department of Defense Perspective

Gerald M. Borsuk and Timothy Coffey, July 2003

Nature of Project

The purpose of this study is to examine the prognosis for silicon integrated circuit technology from a DoD perspective.

Project Summary

The past 50 years have seen enormous advances in electronics and the systems that depend on or exploit them. DoD has been an important driver in, and a profound beneficiary of, these advances, which have come so regularly that many observers expect them to continue indefinitely. However, as Jean de la Fontaine said, "In all matters one must consider the end." A substantial literature debates the ultimate limits to progress in solid-state electronics as they apply to the current paradigm for silicon integrated circuit (IC) technology. The outcome of this debate will have a profound societal impact because of the key role that silicon ICs play in computing, information, and sensor technologies.

The consequences for DoD are profound. For example, DoD planning assumptions regarding total situational awareness have been keyed to Moore's Law, which predicts the doubling of transistor density about every 18 months. While this prediction proved to be accurate for more than 30 years, we are entering a period when industry will have increasing difficulty in sustaining this pace. Under the current device and manufacturing paradigm, progress in areas such as total situational awareness will slow or stagnate. If DoD planning assumptions are to be met, the DoD science and technology program would be well advised to search aggressively for alternate paradigms beyond those on which Moore's Law is based to ensure new technology capabilities.

Findings

- DoD has depended on rapid advances in electronics of all types to maintain technological superiority and expects these advances to continue indefinitely. DoD is not prepared for a slowdown in these advances.
- Solid-state microelectronics will enter a new regime over the next 7 to 10 years in which the current scaling paradigm will no longer hold.

Recommendations

- DoD should search aggressively for alternate paradigms beyond those on which Moore's Law is based to ensure new technology capabilities.
- DoD needs to invest in long-term research that focuses on new materials and new electronic phenomena to maintain information superiority and total situational awareness in the future.
- DoD should nurture long-term research within the United States in the private sector, universities, and Government laboratories.

Project Impact
Findings published by NDU as *Defense Horizons* 30 and distributed to an audience of about 4,000. The report is also available on the CTNSP webpage at: http://www.ndu.edu/inss/DefHor/DH30/DH30.pdf.

Information Assurance: Trends in Vulnerabilities, Threats, and Technologies

Edited by Jacques S. Gansler and Hans Binnendijk, 2004

Nature of Project

This book documents the proceedings of a workshop sponsored jointly by NDU and the University of Maryland, and includes the eight papers presented. The workshop's objective was to:

- Gain insight into DoD's transformation risks in the following areas: trends in information system threats and vulnerabilities; vulnerabilities introduced by the complexity of the new digitized battlefield; impact of degraded information systems on battlefield operations; and trends in information assurance technologies and system design.
- Develop specific recommendations to help assure the integrity, confidentiality, and availability of the necessary networks and systems.

Project Summary

The eight papers presented at the workshop, plus two others, comprise the body of the book. The chapters are:

- "Trends in Vulnerabilities, Threats, and Technologies," by Dr. J.S. Gansler and W. Lucyshyn. This chapter outlines the scope of information technology systems and services now being used in network-centric military architectures.
- "Physical Vulnerabilities of Critical U.S. Information Systems," by Dr. R.H. Anderson. This chapter extends the scope of the workshop to include homeland defense and critical infrastructure.
- "Physical Vulnerabilities Exposed at the National Training Center," by COL J. Rosenberger. This chapter provides an example of the challenges and vulnerabilities of advanced technology warfare when they are the main defense in rugged terrain environment against a knowledgeable adversary.
- "Dealing with Physical Vulnerabilities," by Mr. B. MacDonald. This chapter reiterates the recurring theme of the workshop: that as network-centric designs expand, vulnerabilities must be mitigated to ensure that our ability to understand the battlefield is intact.
- "Vulnerabilities to Electromagnetic Attack of Defense Information Systems," by Dr. J.M. Borky. This chapter focuses on warfare susceptibility of "friendly information systems and networks" that use high power radio frequency (HPRF) or microwave (HPM), and their potential for disruption or damage from electromagnetic (EM) weapons.
- "Vulnerabilities to Electromagnetic Attack of the Civil Infrastructure," by Mr. D.C. Latham. This chapter focuses on the vulnerabilities to EM attack of the civil infrastructure, which collects, manipulates, and delivers information products and services in support of both weapons and military operations.
- "Trends in Cyber Vulnerabilities, Threats and Countermeasures," by Mr. M. A. Vatis. This chapter explores the threat to U.S. critical infrastructure posed by cyber attacks, identifies the scope of cyber attacks on military and civilian

infrastructure, and points out the lack of a nation-wide strategic approach to defending against cyber attacks.

- "Enhancing Cyber-Security for the Warfighter," by Mr. S.R. Finnegan. This chapter discusses the need to implement current best practices, but points out that for some vulnerabilities no fixes can be found, while other vulnerabilities have not yet been identified.
- "Complexity of Network-centric Warfare," by Dr. S.B. Alterman. This chapter addresses the complexity of modern IT-based networks used in the design of a networked, Information-Age battlefield.
- "Difficulties with Network-Centric Warfare," by Dr. C. Perrow. This chapter discusses the complexity of NCW and warns of two main problems that demand an innovative approach to strategy and tactics: stove piping and micromanagement.

Findings

- The following threats and vulnerabilities are especially important:
  - Physical attacks on critical information nodes.
  - Electromagnetic attacks against ground, airborne, or space-based information assets.
  - Cyber attacks against information systems.
- Attacks and system failures are facilitated by the increased level of complexity inherent in the multiplicity of advanced systems.

Recommendations

- Protect critical infrastructures. Private sector infrastructure, in many cases, directly supports military operations (e.g., communications, logistics).
- Develop a system architecture. Design for graceful degradation, robustness, rapid reconstitution, and security up front.
- Increase "red teaming." Identify vulnerabilities of systems, which can then be fixed before they can be exploited.
- Develop secure wireless technologies. Introduce laptops and other portable/wireless technologies slowly into the battlefield to mitigate potential vulnerabilities.
- Develop security metrics. Apply a simple, consistent, easy to use metric to implement accountability.
- Monitor the threat. Improve the intelligence on potential adversaries; anticipating an attack will allow U.S. forces to preempt vulnerabilities.
- Use an evolutionary approach. Introduce changes in an evolutionary manner (so-called "spiral" development and deployment).
- Improve security training. Implement a program to promote the understanding of security best practices, policies, and controls, and of the risks that prompted their adoption.

Project Impact

- The workshop brought together senior decisionmakers working on a broad spectrum of information assurance issues and fostered discussion on some of the most critical questions in this area.
- Over 3,500 copies of the book were provided to the public and to subject matter experts and senior officials.

Complexity and Critical Infrastructure Vulnerabilities Workshop

Sponsored by the Cyber Conflict Studies Association and CTNSP, December 2003

Nature of Project

The goal of this workshop was to network, educate, and identify issues related to critical infrastructure protection and cyber defense that require further study. Issues discussed included:

- What is the definition for cyber conflict, and does the description change with the adversary?
- Does cyber conflict constitute a significant form of coercive power?
- What large-scale effects can be achieved through cyber attacks?
- How should national policy and military doctrine be changed to reflect cyber conflict concerns?
- What international agreements are needed to ensure protection against interdiction and punishment of cyber attacks, while respecting the sovereignty of nation-states?
- How can states and organizations establish the most effective defenses, and how will those defenses interact with other coercive means, particularly economic and military power?

This was the first in a series of five workshops cosponsored by NDU and the National Security Council (NSC), all relating to elements of cyber conflict. Other workshops included discussions on the organization of Government to deal with cyber attacks. The other four workshops were classified.

Project Summary

Presentations included:

- *Implication of Complexity for Shared Infrastructure*, Dr. Harold Morowitz, Robinson Professor in Biology and Natural Philosophy at George Mason University. Dr. Morowitz discussed whether our knowledge of biology and biochemistry was useful in protecting the critical infrastructure.
- *Power Grid Interconnectivity, Failures, and Regulatory Interaction*, Dr. Rejan Sobajic, Director of Grid Reliability and Power Markets, Electric Power Research Institute. According to Sobajic, vulnerabilities are designed into the power grid. The behavior of transmission networks, categorized as large, non-linear, uncertain, and time dependent, is not fully understood. Most new power grid systems receive upgrades through modem dial up, and the systems, especially those used for monitoring and control, rely heavily on the Internet. These dial-up and Internet connections introduce vulnerability into the system and present a target for attacks. The speed at which network attacks occur makes this a very high risk.
- *Impact of Sound Security Practices on Mitigating Risks from Cyber Attacks*, Mr. Allan Paller, Director of Research, SANS Institute. Mr. Paller addressed the following questions: What are the elements of the problem in cyber security? Where does heterogeneity fit? To help participants in addressing those questions,

Paller talked about the current status of worms, viruses, and other attacks against the Internet and IT systems.

- *A Machine Dominated Future?*, Mr. Richard Clarke, President of Good Harbor Consulting and former Presidential Advisor on Cyberspace Security. Mr. Clarke posited a future wherein machines are at best a ubiquitous necessity and at worst, control mankind. He posed the question, "Where are we in the march towards a machine world?"
- *Cascading Effects and Ubiquitous Use of Common Platforms and Protocols*, Dr. Daniel Geer, Principal, Geer Risk Services. Mr. Geer addressed the risks and vulnerabilities of our cyber infrastructure, which permeates all aspects of society.
- *Challenges for Security Shared Infrastructure Against Large Scale Cyber Attack*, Col (S) Gregory Rattray, Ph.D., Director for Cyberspace Security, Office of Defense Policy and Arms Control, NSC. Col Rattray said that securing Government and private sector shared infrastructure against a large-scale cyber campaign will prove extremely challenging. Rattray called for a much-needed change in the cyber defense mindset. Network operators and the senior management of most organizations that rely on information and communications infrastructures must understand the fundamental vulnerability of these technologies systems. It must be assumed that sophisticated adversaries can infiltrate and create the capacity for disruption of most systems and networks given motivation and time. Therefore, we need to be capable of "functioning while under attack."

Findings

- Our cyber infrastructure is fundamentally vulnerable; these vulnerabilities are poorly understood.
- Our knowledge of biology and biochemistry is useful in protecting critical infrastructure.
- Vendors increase risk to the Internet by delivering bad software.
- The U.S. Government needs to be doing much more than it is vis-à-vis offensive or defensive proactive infrastructure defense.

Recommendations

Government decision-makers must focus on developing and implementing actions in the following areas:

- Policy: must be resolved as a national mandate requiring action from senior leaders in the following areas:
    - Strategy, which affects national planning, protection, or oversight activities.
    - Tactics, which affect operation and management of infrastructure.
    - Research, which requires further study and funding.
    - Education, as a better understanding of complexity and critical infrastructure protection is required.

Project Impact

- The workshop brought together senior cyber defense colleagues representing the U.S. Government, industry, and academia to share ideas on pressing security issues. By identifying issues related to critical infrastructure protection and cyber defense that require further study, the workshop laid the groundwork for an on-going exchange of ideas between some of the field's leaders.
- The workshop was the first of five such sessions.

DoD Requirements

Connecting Service Requirements and Commercial Technology

Nature of Project
From November 2001 to November 2002, CTNSP conducted three workshops to identify Service requirements for information technology and possible commercial information technology that might be useful to the Services.

Project Summary
The first workshop, "Information Technology Solutions for Challenges Facing the 21st Century Army," was held on November 13-14, 2001, and looked at challenges facing the Army in equipping forces with state of the art information technology. Senior technology program leaders spoke on four key areas: wireless communications, intelligent agent technology, adaptive and reconfigurable networks, and quantum information.

The second workshop, "Objective Force Network and Communications Challenges," was held on February 13, 2002 and focused on the specific communications challenges facing the Future Combat Systems and the Objective Force. The goals of the general discussion part of the workshop were threefold: (1) to suggest architectures for the communications, and command and control networks; (2) to identify critical issues necessary to achieve interoperability; and (3) to identify opportunities for industry participation.

The third workshop was held on November 19, 2002. It focused on enhancing military and industrial communications between the commercial IT industry and the Air Force and Navy. The presentations and discussions looked at Air Force and Navy information technology visions and strategies from S&T, acquisition, and operations perspectives.

Findings
- Industry is very interested in working with DoD to identify areas where it can provide DoD with state of the art technologies.
- Through working with industry, DoD can better identify the best IT technology solutions possible.

Recommendations
- DoD and the IT industry need to enhance existing methods of communication.
- DoD needs to undertake a program of study to analyze how to better inject commercial IT into DoD systems.

Project Impact
The three workshops hosted and run by CTNP were the beginning stages of the Center's current work in IT. These workshops allowed the Center to identify Service requirements in IT and to identify and make contacts in both the industry and DoD IT communities.

Relevancy and Risk: The U.S. Army and Future Combat Systems

Joseph N. Mait and Jon G. Grossman, May 2002

Nature of Project

This *Defense Horizons* paper addresses the main focus of U.S. Army force transformation plans, the Future Combat Systems (FCS). Open literature sources are used to examine some of the challenges facing the development of six critical FCS technologies and assess when each technology may become viable. Information technology for the networks is a key variable in this equation and is the least mature of the technologies discussed.

Project Summary

The Army aims for an agile, versatile, lethal, survivable, responsive, deployable, and sustainable force that is strategically responsive and dominant across the spectrum of military operations. The FCS plan is the cornerstone of the Army's transformation initiative. The FCS are designed to integrate the best information technologies from the ongoing revolution in military affairs and to provide the requisite rapid deployment to distant and austere theaters to meet the challenges of 21st-century expeditionary requirements.

This paper identifies six basic technologies that contribute to meeting core FCS operating requirements: sensors, networking, robotics, armor, munitions, and hybrid power. The authors chose these six because of their importance to enabling FCS capabilities. The first three are enabling technologies that cut across FCS capabilities while contributing directly to situation awareness. The latter three address directly FCS survivability, lethality, and deployability. The paper discusses the needs of FCS in each area and analyzes the current state of the art.

The paper attempts to answer five questions:

- Is the Army making the key decisions for its future at the right time? Are 2003 and 2006 too soon to make key technological decisions?
- Does the transformation of the Objective Force rely too heavily upon new technology for the survivability of the FCS?
- Given uncertainties in survivability and future threats, are the costs for the FCS worth the investment?
- Is the Army accepting too much strategic risk in the near term? Has it built in strategic hedges to account for mistakes in judgment?
- Is the Army changing too quickly to handle the transformation?

Findings

- Relatively speaking, the most mature technologies include hybrid power, munitions, and armor, which are essentially products of the industrial revolution. Although advances in these areas will occur (in some instances via integration with electronic technology), their capabilities will increase at relatively slow and linear rates.

- Sensors and robotics are the most recent technologies growing out of the development of electronics in the late industrial period and early computer age. Their capabilities will grow exponentially due to their foundation in electronics and the impact of Moore's Law.
- The least mature technology is networks (a product of the Information Age). Exponential growth in this area should occur around 2010.
- The performance of three technologies—the network, munitions, and robotics—is critical to fully enabling the FCS concept. Without the network, the theoretical advantages of network-centric warfare cannot be achieved; with present technology, it may be possible to network a single FCS unit cell, but not an FCS unit of action or unit of employment. Similarly, present technology in munitions provides an effective line-of-sight fire; however, FCS is dependent upon Netfires to ensure its capability for beyond-line-of-sight fire. Finally, in terms of robotics, unmanned aerial vehicle (UAV) technology is mature, and UAVs are expected to be a significant constituent of the FCS initial operational capabilities. Unmanned ground vehicle technology is less mature and may have only limited utilization in the initial operating capabilities.
- Predicting when the sensor, robotics, and networks technology will exhibit the nonlinear advancement to meet FCS requirements is at best an educated guess and the primary difficulty in managing the risk inherent in a high-technology program.

Recommendations

- In light of the uncertainty about when critical technologies will become available, and because the FCS seems unlikely to meet the development milestones set by the Army, it is best to consider a graduated application of the FCS to its missions. The Army should develop initial versions of FCS for low-intensity conflicts and, as technologies mature, new versions for higher-intensity conflict. This approach would address strategic concerns along with technological ones.
    - Specifically, a decision on a version of the FCS capable of effective involvement in a small-scale conflict could be made by 2010, and the decision on a Major Combat Operation (MCO)-capable FCS version by 2014. Thus, even if the FCS is unable to compete in a MCO within the next decade, the investment in FCS technology will have provided enhanced capabilities for an expeditionary force; with block upgrades, it may realize its fullest potential in its second decade of development.

Project Impact

Over 3,500 copies of the paper were provided to the public, subject matter experts, and senior officials. Results of the study were briefed widely within the Army. The paper was published as *Defense Horizons* 13 and available online at: http://www.ndu.edu/inss/DefHor/DH13/DH13.pdf.

Making IT Happen: Transforming Military Information Technology

Charles Barry, Dr. Richard Chait, Dr. Donald Daniel, Dr. Stuart Johnson, Dr. Joseph Mait, Dr. Paul Phister Jr., Albert Sciarretta, Dr. Stuart Starr and Dr. Elihu Zimet, September 2005

Nature of Project

"Making IT Happen" is a primer for commercial IT providers to gain some understanding of the military's thinking about military information technology and the programs it foresees for the future.

Project Summary

Information has always been critical to successful warfighting, as important as rapid maneuver, overwhelming firepower, and dependable logistics. Yet the ever-increasing ease with which information can be accessed and transmitted has made IT a cornerstone of military transformation. Common to each Service is a de-emphasis on platforms, on the concentration of mass to provide overwhelming force, and an increased emphasis on networking to enhance warfighting capabilities.

The intent of the report is to introduce those not presently involved in the development of military IT to some of the thinking and programs being developed by DoD for deployment in the next five to ten years. The report is organized into five chapters, primarily along Service, joint, and coalition operations, providing slightly different perspectives on information technology.

Chapters 1, 2, and 3 summarize the thrusts of the Army, Navy, and Air Force programs in IT. Although they share common themes, the programs reflect specific needs dictated by the operational environment of their Service. The Army's program, in particular, is heavily influenced by its emphasis on FCS. The discussion in chapter 2 emphasizes the technical objectives of the Navy's FORCEnet to meet its operational capabilities, characterized broadly as sea strike, sea shield, and sea basing. The chapter focuses on the functionalities that FORCEnet requires and the technologies to produce these functions. Further, the impact of systems and platforms on implementing FORCEnet are also discussed.

Chapter 3 provides a broad perspective of the Air Force program. The chapter discusses activities in the Air Force Research Laboratory and the Air Force Battle Labs that support the Joint Battlespace Infosphere. This includes the operational capabilities Global Awareness, Global Information Enterprise, and Dynamic Planning and Execution, and some of the technologies required to realize these capabilities. The chapter further discusses how the Air Force integrates and tests these new capabilities in its battle labs.

Chapter 4 provides a detailed and complete overview of the issues and requirements necessary to insure networking and information sharing occurs across the services. The chapter characterizes the nature of the interoperability problem, describes recent initiatives to ameliorate interoperability shortfalls, and identifies interoperability challenges. In particular, the chapter emphasizes interoperability among systems in the

context of joint, interagency, and multinational operations, including international organizations such the United Nations, nongovernmental organizations, and contractors.

The unique problem of sharing information with allies and changing coalitions is addressed in chapter 5 in the context of NATO operations. The chapter describes NATO's efforts to move into an age of information-intensive military operations with particular attention on political decision-making, and the command and control of distant multinational operations.

Findings

- Currently, the Army's greatest unmet needs are in the development of mobile ad-hoc networking protocols and architectures; collaborative Battle Command applications that can be executed over a distributed network; the fusion of data from self-configuring, networked sensors; interoperability; and computationally efficient models and simulations of large scale, realistic communications and sensor networks.
- One of the most serious improvements required in Air Force information S&T is a better balance between long-term and short-term research with more emphasis on long-term research.
- One of the key findings in regard to interoperability is the need to create test beds and use them in an innovative fashion to deal with all the dimensions of the problem.
- NATO is modernizing its IT systems by measured, regular investments in three broad areas: optimizing management information systems, creating network-enabled military capabilities, and the conduct of military information operations.

Recommendations

- The Army must invest not only in individual technologies such as low power software-based radios, but also in the integration of many diverse information technologies (sensors, antennas, computers, and protocols).
- This primer recommends a package of actions to address all of the dimensions of interoperability, e.g., institutional, programmatic, technical, standards, and architectures.
- This primer should be used as an adjunct to other IT outreach activities.

Project Impact

The Primer was published as *Defense and Technology Paper* 20 in October 2005. The main impact of this primer will be on industry's understanding of the requirements of military networks and communication systems. This understanding will allow industry to provide better solutions to the unique needs of the military. The Primer is available on the CTNSP website at: http://www.ndu.edu/ctnsp/Def_Tech/DTP%2020%20Making%20IT%20Happen.pdf.

Possible Solutions to Utilizing Commercial IT

Creating an Interactive Website for JFCOM

Nature of Project
This project was undertaken to provide JFCOM with an interactive website to allow information exchange between acquisition experts at JFCOM and the commercial arena. Working closely with JFCOM and the results of a survey of the IT industry, CTNSP has created a website that will match Service requirements with opportunities presented in the commercial sector. What was designed as a demonstration project has worked well enough that it is now being transitioned to JFCOM for incorporation into their broader network. CTNSP has created a website that:

- Presents a low-barrier, always-available platform for forming pre-sales relationships between DoD and new IT vendors seeking input for pre-release products.
- Attracts new vendors by presenting the DoD as a penetrable market for innovative IT products.
- Matches vendors and interested DoD product reviewers.
- Involves military with vendors during product definition, Beta testing, and as a first buyer.
- Builds a pipeline of IT products influenced by military requirements and familiar to military experts.

Project Summary
The purpose of the website is to match innovative IT vendors with military personnel interested in providing input and product testing. The beginnings of a goal-oriented relationship start on the site, where vendors submit information about their pre-release products, and military personnel receive submissions based on product categories they have selected.

This website contributes to expanding military and IT contacts by:

- Publishing areas of military interests in general categories, not specific to a project, to promote feasible searches and an easy-to-maintain database.
- Allowing DoD personnel to sign up via the website to receive vendor submissions in each interest category they select.
- Allowing vendors to submit information about their products. In the submission form, vendors select categories from the list of military interests, which are used to match the submissions to military reviewers.
- Emailing vendor submissions to all DoD personnel whose selected interests match the category in the submission; DoD personnel decide if they want to move forward and when they want to reveal their identity.
- Creating relationships that are linked to product development phases and have specific goals.

Findings
IT companies seek potential customers at the early stages of product development to validate marketability before the product is released. There are several points of entry in product development (requirements-gathering and design stage, Beta testing, piloting first releases), but earlier involvement achieves more influence at very low cost. This project focuses on the product development stage rather than company funding or sales because this critical phase of product development is underserved and contributes to goals of both DoD and IT companies.

- Win for company: gain important market input for development; demonstrate market value to funding sources; build military contacts; gain foothold in military market.
- Win for DoD: influence development by engaging early; get early access to cutting-edge products; review products without spinning up the acquisition process.

Recommendations
An earlier CTNSP survey of IT industry attitudes suggested that industry could be receptive to using their own technology (i.e., website) in a way that would allow them to find out what Service requirements are and to offer DoD specific ideas on the technologies they are developing. As an incentive, the report recommends Beta testing for technologies that they are offering up for military value.

Project Impact
The project was undertaken in March 2004 by CTNSP and resulted in the creation of an interactive website. This project was also incorporated into a briefing to the Joint Experimentation Directorate (J9) JFCOM. CTNSP is working to transition the website to JFCOM for their use in matching service requirements with opportunities presented in the commercial sector.

An Assessment of the Ability of Venture Capital-Related Initiatives to Support National Security Objectives

Stuart Starr, December 30, 2004

Nature of Project

The paper evaluates venture capital-related initiatives as a mechanism to support national security objectives. The project assesses how well these initiatives can exploit commercial information technology products efficiently and effectively so that the DoD is not operating from a position of information inferiority. The primary objective of this paper is to identify issues associated with venture capital-related models and to formulate recommendations to enhance their utility to DoD and to the Intelligence Community (IC). The paper is supported by an appendix that summarizes interviews that have been conducted with senior representatives from the various venture capital-related activities.

Project Summary

One of the major challenges confronting DoD is keeping up with innovative commercial IT products and practices in national security systems. In recent years, there has been considerable interest on the part of DoD and the IC to exploit venture capital-related methods to address the issue of bringing commercial IT, specifically commercial off-the-shelf (COTS) products, into DoD systems. Three alternative macro-models represent different initiatives to integrate commercial IT into DoD systems: the Broker Model, the Equity Investor, and the Portfolio Model. In order to contrast these models, in-depth interviews were conducted with senior representatives of the major DoD and IC venture capital-related initiatives.

Findings

- A single "right way" for the DoD to employ venture capital-related initiatives does not exist.
- At this early stage, it is difficult to characterize the success of on-going initiatives.
- It is very useful to create and sustain a Community of Practice for venture capital-related efforts.
- It is valuable to pursue the purposeful evaluation of these venture capital-related efforts.
- A substantial number of more specific venture capital-related issues have been identified:
    - Employing venture capital-related activities to acquire commercial IT is counter-cultural to many participants in the national security community (e.g., Program Executive Officers, program manager, Congress). This raises barriers to the acceptance and utilization of these mechanisms.
    - Small and medium-size commercial IT companies do not know the DoD processes and regulations. Furthermore, they generally lack the security clearances that are needed to gain access to critical national security data.
    - Nearly every activity analyzed highlighted resource constraints as a major issue.
    - It appears that the most difficult part of the process is to take identified product solutions and to inject them into Government systems. Problems

include mismatches in technology, difficulties in training personnel, and updating the product. It will generally be more feasible to inject COTS products that are associated with the low end of the conflict spectrum (e.g., S&R operations versus warfighting operations) and deployed in offices vice the battlefield.

Recommendations

- If DoD is to use commercial IT products, it must be willing to relax its requirements and use the IT products flexibly.
- Cultural change is required in order to employ venture capital-related initiatives. Incentives must be modified to encourage program executive officers (PEOs) and program managers (PMs) to take prudent risks. One possibility is to reward PEOs or PMs who use these initiatives judiciously through the provision of additional program resources, special recognition, or promotions.
    - Organizational changes: A Commercial Information Technology Innovation and Integration Center (CITIC) is envisioned that would serve as an "Innovation Manager" to orchestrate these venture capital-related activities. Meetings should be encouraged to establish boundary lines of responsibility and to facilitate the hand-over/transition of technology from venture capital-related activities to the Service System Commands.
    - Address the people issues: It is important to educate and train stakeholders on the capabilities and limitations of venture capital-related activities. For example, the curriculum of NDU's Capstone course should be augmented to educate senior decisionmakers, the Defense Acquisition University should feature this material in courses for PEOs and PMs, and venture capital-related associations should offer short courses to venture capitalists who wish to participate in these activities. Steps should be taken to increase the number of venture capitalists involved in these activities.
    - Revise policy: Steps must be taken to make the FAR less opaque so that commercial companies are better able to comprehend and adhere to its regulations. Consideration should be given to extending Other Transactional Authority (Article 845) to enable organizations to use these mechanisms to go beyond prototypes to fielded systems.
- Re-engineer key processes to enhance the ability to inject commercial IT into DoD systems. On a case-by-case basis, provide appropriate levels of security clearances to participating venture capitalists and to small and medium-size, innovative commercial firms. It would be useful if the Government could go beyond briefings on individual user needs to generate a synoptic, integrated set of needs for key issue areas.

Project Impact

Results of this study were incorporated into the briefing, "Actions to Enhance the Use of Commercial IT in DoD Systems."

Lessons Learned on Commercial IT in DoD Systems

Dr. Kenneth L. Jordan, November 2004, working paper

Nature of Project

This report reviews previous studies, conferences, and articles that have addressed how DoD can place increased emphasis on using the commercial IT base. The report also reviews several case studies of past or ongoing programs that have used commercial off-the-shelf (COTS) systems.

Project Summary

Reviews of past studies and conferences:

- Air Force Science Advisory Board (AFSAB) Report on Ensuring Successful Implementation of Commercial Items in Air force Systems, April 2000 (a report of 34 programs that had used or were attempting to use commercial items that tended to be integrated).
- COTS-Based Systems Top 10 List (hypotheses for examining COTS-based product decisions).
- International Workshops on Commercial IT for Military Operations (informal initiative to explore opportunities for the military to make use of commercial technologies, systems, and services).
- International Conference on COTS-Based Software Systems (annual conference aimed at addressing the growing field of COTS-based system practice and research).
- Software Engineering Institute COTS-Based Systems Initiative (focused on principles, methods, and techniques for creating systems from COTS products).

Case studies of past and ongoing programs using commercial IT:

- Cellular Communications for Baghdad: The existing telecommunication infrastructure was inadequate or non-existent, requiring the use of a wireless communication system by U.S. Government approved contractors and civilian personnel as part of the planning for post-war reconstruction efforts in Iraq.
- ArcSight: A technology security initiative project providing the integration, correlation, and display of the numerous alerts or logs from individual security applications such as virus detection and intrusion detection software.
- Brigade Subscriber Node (BSN): One of the communication elements that the Army would develop that provides integrated voice, video, and data services.
- Navy/Marine Corps Intranet: Initiative to provide a single, secure, enterprise-wide network to support establishment and to tie it to the forces at sea by interfacing with the at-sea network.

Findings

Over one hundred principal success factors and lessons learned were found. The following illustrates the nature of the problem:

- Open system architecture and spiral development processes are utilized in successful COTS insertions.
- COTS-based system sustainability issues overwhelm acquisition costs.

- Cost to maintain a COTS-Based System equals or exceeds that of custom software.
- COTS-Based Systems development and post deployment efforts can scale as high as the square of the number of independently developed COTS products targeted for integration.
- The evolutionary nature of COTS products has a profound impact on program cost, schedule and risks.
- The average COTS software product undergoes a new release every eight to nine months, with active vendor support for only its largest three releases.

Recommendations

- A military IT system that is anything but a short term, quick fix solution must have a total life cycle procurement and sustainment strategy.
- As a general rule, for military IT systems involving the integration of multiple COTS components, modification of COTS should be avoided. There may be circumstances, however, in which modification makes good business sense for both the military customer and the commercial contractor. This step should be taken only after the long-term implications are thoroughly investigated and a business case is evaluated.
- Demonstrations, pilots, and testbeds are key tools for the acquisition and maintenance of a COTS intensive IT system.

Project Impact

Provided background for the briefing on “Actions to Enhance the Use of Commercial IT in DoD Systems.”

Transformation and the Defense Industrial Base: A New Model
Robbin F. Laird, May 2003

The Deepwater Program and the Role of Commercial Technology
Robbin F. Laird

Nature of Project
There is a recent trend towards creating lead system integrators (LSIs)—large commercial companies such as Lockheed Martin and Boeing—that are assigned the task of creating complex systems-of-systems (SOS). Examples of such complex projects are missile defense, FCS, and the Coast Guard's Deepwater Program.

Project Summary
There may be value in having a large aerospace company serve as an LSI in acquiring complex SOS. In several cases, the Government has turned over to these commercial companies many responsibilities that were traditionally the responsibility of the Federal Government, such as deciding what technologies should go into these systems. Part of transformation involves this shifting responsibility from the Government to the private sector, which may make sense in the case of large program development requiring sizeable resources. While it is efficient, it also means that DoD gives up control of the kinds of technologies used. This raises the question of how this shift affects the ability of DoD to take advantage of innovative technologies being developed if there are no incentives for these large corporations to take advantage of new technologies from small and medium-size, innovative companies. Many companies work with subcontractors for on-site development of required technologies. CTNSP conducted two studies on this topic.

Findings
- There may be value in using large commercial companies—lead system integrators—when acquiring complex SOS.
- In the process, the Government has lost a degree of control to the private sector in the acquisition of technology for these weapons systems.

Recommendations
New incentives need to be created to ensure that lead system integrators take advantage of new commercial technologies evolving from small and medium-size companies.

Project Impact
The results of these studies were taken into consideration in the development of the briefing, "Actions to Enhance the use of Commercial IT in DoD Systems."

Actions to Enhance the Use of Commercial Information Technology in Department of Defense Systems

Franklin Kramer, Stuart Starr, and Larry Wentz, July 2005

Nature of Project

In 2004, Congress directed CTNSP to study the problem of acquiring commercial IT for DoD systems.

Based on supporting studies previously performed on the subject, several key dimensions of the problem emerged. First, the successful injection of IT is critical if DoD is to accomplish the broad spectrum of missions that it must perform and to maintain the technological lead that it enjoys against current adversaries. However, it is becoming apparent that much IT technological innovation is occurring outside the traditional DoD acquisition process. Consequently, DoD is missing major opportunities to capitalize on those technological innovations. This is particularly troublesome because potential adversaries (e.g., transnational terrorists and potential near-peer nation states such as China) have full access to the IT innovations that are emerging from commercial industry. This poses the concern that DoD's technological lead in the area of IT could erode substantially in the coming decades. This concern is exacerbated by the observation that DoD cooperation with the IT industry is hamstrung in a variety of ways.

Project Summary

Current DoD guidance reveals that DoD has recognized the problem and sought to take steps to address it. A decade ago, Secretary of Defense William Perry issued a well-publicized white paper that stressed that DoD "…must increase access to commercial state-of-the-art technology." More recently, in 2003, Deputy Secretary of Defense Paul Wolfowitz signed a revised DoD Instruction 5000.2 that mandated that the DoD acquisition process "…make maximum use of commercial off-the-shelf (COTS) technology." These two examples are merely illustrative of DoD interest in the aggressive use of commercial technologies, in general, and commercial IT, in particular.

In order to comply with this guidance, DoD employs a broad spectrum of methods to capture commercial technology. However, the bulk of its resources are allocated to "business as usual" activities. This subsumes such processes as issuing requests for proposals (RFPs), supporting independent research and development (IR&D) activities by industry, conducting pilot activities, and promoting initiatives by program executive officers (PEOs). In general, these activities deliver systems to the user that are characterized by timescales in excess of a decade, although expedited delivery of core capabilities and system increments is being sought through the adaptation of evolutionary acquisition strategies.

In an effort to be more consistent with the characteristic timescales of commercial IT products, DoD is turning to a variety of other techniques. These include the use of multiple websites and bulletin boards to advertise DoD needs to commercial industry, the use of integrated process teams (IPTs) to facilitate communications among all the participants in the acquisition process, and the promotion of special initiatives. As an example of the latter, ASD(NII) has promoted the Rapid Acquisition Initiative-NetCentric (RAI-NC) in an effort to accelerate the acquisition of commercial IT

products, but resource limitations have severely restricted the scope of this initiative.

Congress has consistently supported the Small Business Innovation Research (SBIR) program along with the related Small Business Technology Transfer (STTR) and Fast Track programs. As a benchmark, the annual DoD share of these activities is on the order of $1B. However, relatively few of these initiatives get to the third phase (commercialization) which would facilitate their fielding to the force.

More recently, there have been a variety of venture capital-related initiatives sponsored by DoD and the Intelligence Community. These efforts have sought to harness the knowledge and insights of venture capitalists to facilitate the identification and fielding of commercial products. These include CIA's In-Q-Tel, NGA's Rosettex, OSD's Defense Venture Catalyst Initiative (DeVenCI), the Army's OnPoint, the Navy's Commercial Technology Transition Office (CTTO), and SOCOM's Arrowhead. Although many of these efforts are promising, most are currently in the pilot stage and are supported by relatively limited resources (e.g., less than $50M per year). An extensive analysis of these activities is provided in an associated study.

Furthermore, DoD is using a variety of tools to facilitate the flow and expedited fielding of commercial technology. Specific examples include cooperative research and development agreements (CRDAs), advanced concept technology demonstrations (ACTDs), and Service-sponsored institutes. As an example of the latter, the Army has sponsored the establishment of the Institute for Creative Technologies (ICT) at the University of Southern California (USC) to tap the technological skills of the entertainment industry in Southern California.

Finally, there is an interesting array of Combatant Command (COCOM) and Agency initiatives to capture commercial technology. One continuing effort is the Coalition Warrior Information Demonstration (CWID) (formerly the Joint Warrior Information Demonstration) in which COCOMs in concert with the Defense Information Systems Agency (DISA) sponsor a yearly event to identify promising new technologies. Other useful activities include the Enterprise Software Initiative (which promotes the joint acquisition of software), the Enterprise Integration Toolkit (to support the acquisition and management of COTS business systems), the DTIC web site and associated resources, and the resources of the Defense Acquisition University (DAU) (which provides acquisition courses to the DoD community along with a community of practice website).

Findings

Six broad classes of obstacles have been identified that impede DoD's ability to capture IT capabilities developed outside the traditional defense acquisition process. These obstacles revolve around the facts that DoD constitutes a market for commercial IT products that is non-attractive, non-transparent, non-agile, non-dominant, and isolating. Furthermore, DoD's ability to tap commercial IT is limited by the attitudes of the prime contractors and Lead System Integrators (LSIs) that acquire major defense systems. Each of these obstacles is identified and discussed below.

Non-Attractive

Recently, CTNSP sponsored a survey of commercial IT firms that infrequently do business with DoD. In that survey, the firms that currently do not business with DoD cited the following major reasons for their reluctance to enter the DoD market:

- "They do not know what they want"
- "The application/bid process takes too long"
- "DoD only deals with large companies"
- "Our products are not needed by DoD"
- "We do not want to work with DoD"
- "There are too many barriers to the bid process"

Similarly, DoD conducted a study to identify why commercial IT firms are reluctant to do business with DoD. That study concluded that non-traditional defense firms are reluctant to enter the defense market because of intellectual property rights (IPR)issues (e.g., small and medium-size firms are extremely reluctant to cede IPR rights to the Government); the long development times associated with defense procurements; and the onerous cost accounting, auditing, and oversight requirements levied by the Government.

Non-Transparent

In the CTNSP-sponsored survey cited above, current DoD contractors explained why they perceive the current DoD policies, processes, and procedures to be opaque.

- They noted that the process is too difficult, too slow, and too confusing.
- They decried the limited information that is available to small and medium-size business.
- They noted the lack of opportunity for firms that have not won prior contracts.
- They observed that it is desirable to ease the security clearance process.
- They stated that the current DoD acquisition process is an exclusionary one.
- They complained that they lacked clear information about Government contracting.

Non-Agile

The planning, programming, budgeting, execution (PPBE) system requires the participants to predict technology transitions 18 to 24 months in advance. However, the program manager community cannot always predict the pace of innovation two years in advance and funding may not be available for fast-moving projects that are ready for transition. Consequently, a desirable S&T project may stall for 18 to 24 months, waiting for funding. This gap is sometimes called the "valley of death".

Non-Dominant

In the 1960s, the DoD was the dominant player in the IT marketplace. However, that situation has changed dramatically over the last decade. As noted in the Manager's Guide to Technology Transfers in an Evolutionary Acquisition Environment, "DoD is unable to acquire intellectual property (IP) rights for commercially developed technology, as it has done for defense-funded technologies in the past, because DoD's financial involvement will be limited and its demand is not dominant compared with the worldwide commercial market."

Isolating Market

Historically, DoD requirements (which tend to be battlefield oriented) demand capabilities that are not found in the commercial sector. A good example of this gap is illustrated in table 1 which compares the communications and networking characteristics of the commercial sector with those of the tactical military. This table was derived from information provided at the 2004 Information System Technology (IST) Technology Area Review and Assessment (TARA). It compares communications and networking for the commercial sector and the tactical military user for six factors: mobile subscriber infrastructure, networks, antenna towers, frequency spectrum availability, protection, and low probability of detection/jam resistance. It can be seen that the military faces the problem of working in an environment where little or no infrastructure exists. Thus, it needs mobile/transportable, flexible resources which are highly protected from potential adversary actions. Even though there appears to be a broad chasm between the two needs, the commercial sector is actually beginning to offer commercial products that are more responsive to military needs.

Rhetorically, the DoD R&D community employs the mantra: "adopt, adapt, and develop" (i.e., first try to adopt commercial technology; if that is inadequate, try to adapt commercial technology to meet military needs; if that fails, develop military-unique solutions). Although that mantra is quite reasonable, there is a tendency to focus on the reasons why adopt or adapt are inappropriate and to jump to the development of military-unique solutions. In reality, the commercial sector is beginning to develop significant IT capabilities for the commercial sector that are more readily extensible to the military sector.

Primes/LSIs

During the course of ancillary studies, the roles of primes and LSIs were assessed with respect to the adoption/adaptation of commercial IT. Three specific issues were identified that suggest that primes and LSIs may be a significant obstacle in this area. First, prime contractors may have a natural tendency to prefer internal technology because they can see the design and make it work. Second, prime contractors may have conflicting objectives about adopting technology from an outside provider. This can range from something as intangible as the "not invented here" syndrome to more tangible issues,

such as displacing the prime contractor's revenue base. In addition, primes may also be concerned about complex issues, such as problems with the timeliness and compatibility of technologies built by outside organizations.

Recommendations

In order to deal with the obstacles that limit DoD's ability to capture IT capabilities developed outside the defense acquisition process, a six-step approach is recommended. This includes enhancing DoD-commercial communications and implementing organizational change, increasing DoD's resource flexibility, removing a variety of barriers to commercial IT acquisition, stimulating cultural change in the defense community, reviewing the testing process, and adapting requirements for specific missions. It must be emphasized that there are no "silver bullets" (i.e., there is no single change that will serve to mitigate the problem adequately). Thus, a suitable set of these recommendations will have to be crafted and orchestrated if substantive improvement is to be achieved.

- Enhance communications/organization (e.g., create a new organization at JFCOM to coordinate the use of commercial IT in DoD, including the operation of a Web Portal and EMISARS and the provision of tech-prospectors and acquisition guides).
- Increase resource flexibility (e.g., provide COCOMs Limited Acquisition Authority, on the order of $300M, with lead responsibility for JFCOM and NORTHCOM).
- Decrease barriers (e.g., change DoD rules on IP and use OTA as the norm in IT R&D).
- Stimulate cultural change (e.g., increase DoD education and training for commercial IT procurement; provide incentives for PMs, LSIs to use commercial technology; and adopt GAO-recommended best practices to acquire commercial component business systems).
- Review testing (e.g., evaluate expanding "underwriter lab" testbeds; consider expanding operational testbeds to evaluate the impact of the technology on mission effectiveness).
- Adapt requirements for specific missions (e.g., undertake studies on the use of commercial IT in S&R operations, homeland security, cross-cutting installations, and IO).

Project Impact

The findings and recommendations of this study have been briefed widely within DoD to the highest level decisionmakers (e.g., Chairman, Joint Chiefs of Staff (JCS); Commander, JFCOM; Service Chiefs of Staff). It is notable that JFCOM has recently undertaken a number of initiatives that are broadly consistent with the spirit of these recommendations. These include the granting of "National Laboratory"-like authority, the creation of the Office of Research and Technology Applications (ORTA), and the granting of limited acquisition authority to Combatant Commands.

Extensions of Net Centric Operations

Alternative Fleet Architecture Design

Office of the Secretary of Defense (OSD), Office of Force Transformation, March 2005, Project Director: Stuart Johnson, CTNSP

Nature of Project

Congress mandated a study on the impact of information technology networks on Alternative Future Naval Fleet Architectures. A team from CTNSP executed the study under the sponsorship of OSD's Office of Force Transformation and in co-operation with the Joint Staff, J-8. The report sets out to capture the spectrum of threats with which a future Navy must cope; establish design principles based on meeting those future challenges and on taking advantage of rapid advances in technology and organizational effectiveness; and propose an alternative to the programmed future fleet architecture. If sea-based battle platforms can be networked up front, what new capabilities does that provide?

Project Summary

The report addresses the need for the Navy to adapt to the changed security environment, becoming more relevant to asymmetric challenges, while still maintaining its dominance against any strategic competitor. The Navy must find a way to build a fleet that can meet both asymmetric and strategic challenges, and it must do so despite the fact that it may not receive the resources to complete its current long-range shipbuilding plan.

After analyzing the capabilities needed by a future fleet and considering the budgetary challenges, the report offers three examples of future fleet architectures. These alternatives were chosen for analytical purposes and executability, not because any particular component is necessary for the viability of the example architecture. Existing hull designs were used and configured in well-established ways to constitute alternative fleet architectures. The alternative fleet architectures were constructed at an equal cost to the programmed fleet architecture in terms of procurement costs and 30 years of operating and support costs.

The alternative fleet architectures were based on the following four design principles:

- Complexity: The alternative architecture has been designed to complicate both an adversary's force planning and operations planning. It does this through:
    - Large numbers of platforms that the enemy must track and target;
    - Great variety of forces with which the enemy must contend;
    - Fast, agile, low-signature platforms;
    - Distribution of forces across large areas for the enemy to search and cover.
- Smaller ships and improved payload fraction: Advances in shipbuilding are making it possible for ever smaller ships to be seaworthy in the spectrum of conditions that combat fleets encounter. Moreover, R&D on smaller weapons with high precision and enhanced terminal effects is making it possible to package

capabilities onto small ships. Ships can be made faster and more maneuverable while payload fraction can increase substantially.

- Network-centric warfare: Advances in information technologies make it possible to network dispersed components of a fleet so that the total power of the fleet greatly exceeds the sum of the capabilities of its individual components.
- Modularity: The alternative fleet platform architecture incorporates a generous mix of ship capabilities. The ships make extensive use of modularity to maintain the ability to adapt to changing strategic or operational challenges. Separating the sensor and weapon suites from the hull permits the Navy to incorporate new technology into the module without taking the ship out of service to do so. The alternative architecture also leverages the growing capabilities of unmanned vehicles.

Findings

- A future fleet characterized by large numbers of relatively small, fast, stealthy ships can operate against an asymmetric threat in the littorals and still confront a challenge to the U.S. Navy's strategic dominance of the ocean commons. Analysis showed that such a fleet can perform as well as or better than the programmed future fleet in scenarios against both asymmetric and strategic enemies.
- A design based on low unit cost ships yields a larger fleet. This puts the future fleet platform architecture on the right side of trends in technology. First, advances in technology allow our steadily increasing strike capability to be packaged onto smaller platforms. Second, advances in information technologies open up the power of networking to the fleet.
- Modularity gives the fleet operational agility. By designing ship hulls with common system interfaces, different combat modules can be swapped on and off ships. This allows the fleet to adapt rapidly to a dynamic operational environment. Moreover, it permits the Navy to incorporate advances in technology into the fleet more quickly and at less expense.
- Such a fleet, based on existing hull designs, can be procured and maintained at the same cost as the programmed future fleet. If funding levels do not meet the Navy's projections, and there is reason to think that they will not, the proposed architecture is more scalable than the programmed fleet, which is designed around large, high unit cost ships.

Recommendations

- The Navy should adopt a future fleet architecture based on the above design principles, using large numbers of relatively small, fast, stealthy ships with low unit cost and modular capabilities.

Project Impact

- The report was circulated to the House and Senate Armed Services committees and briefed to members of the House ASC Research and Development panel.
- The report was briefed to senior Navy leadership, including the Chief of Naval Operations.

- The report formed the basis of Congressional Research Service options presented to Congress for review of the Navy program.
- The report was briefed to the Director, J-8, Joint Staff.
- CTNSP published a version of the report for wide release in August 2005 as *Defense and Technology Paper* 19. The report is available on the CTSNP website at: http://www.ndu.edu/ctnsp/Def_Tech/DTP%2019%20Alternative%20Fleet%20Architecture%20Design.pdf.

Battle-Wise: Gaining Cognitive Advantage in Networked Warfare

David C. Gompert, Irving Lachow, and Justin Perkins

Nature of Project

The scope of this project is to examine the "next edge" of networked warfare. As advances are made with communication, intelligence, and network technologies by the United States, its allies and its adversaries, new thinking is needed on how to exploit the cognitive advantage of the warfighter; i.e. the soldier's ability to maximize anticipation, decision speed, opportunism, rapid adaptation to become "battle-wise." The research project drew upon open source materials and interviews with experts to produce the report. The battle-wise research relates to the use of IT in S&R operations, new uses for IT, and transformation issues.

Project Summary

As adversaries exploit networks, the United States must seek new leverage by improving its fighters' ability to use information in war's confusing, critical, and violent conditions. Blessed with more, better, and timelier information, yet vexed by increasingly murky circumstances, the cognitive faculties of military decisionmakers are more crucial then ever. In order to make key recommendations, the report establishes the geo-strategic context, draws from the experience of non-military sectors, frames policy issues, offers preliminary advice, and indicates where future research is needed.

Findings

A battle-wise lead for the armed forces can be cultivated in three key areas. These three efforts must go hand-in-hand:

- Improving the cognitive abilities of individual warfighters by:
  - strengthening recruiting standards and strategies
  - investing more in early, demanding, and relevant education and training
  - identifying, retaining, promoting, and utilizing those who excel
- Command and control reform should encompass
  - expanding the opportunity for battle-wise problem solving from "the few" senior officers to "the many" junior officers
  - permitting more effective horizontal collaboration
  - enabling warfighters, units and whole forces to solve problems at the lowest appropriate level
- Collective intelligence can be achieved by
  - forming coherent, if temporary teams to tackle particular operational problems to deliver sound decisions and offer greater flexibility than vertical command and control

Recommendations

- Recruit people with exceptional battle-wise aptitude.
- Educate and train early, competitively, and well.
- Sort and select as education, training, and operational experience permit.
- Rethink retention in light of battle-wise needs and flatter organization.
- Accelerate command and control research and reform.

- Foster collective intelligence.
- Conduct further research and analysis, for example:
    - What are the prerequisites that adversaries must meet to be able to exploit networking militarily, and how can the United States meet this challenge?
    - What profile of warfighting cognitive aptitude and qualities should be reflected in recruiting standards and strategies?
    - How should command and control networks, structures, and procedures be designed and developed to improve the distribution of authority and the efficacy of peer-to-peer collaboration?

Project Impact

- The research findings were presented at the 10th International Command and Control Research and Technology Symposium in June 2005.
- The research findings and analytical approach are being incorporated into the 2005-2006 core curricula of the Information Resource Management College, NDU.
- A book, expanding on the Battle-Wise research paper findings will be published in the winter of 2006. The book has a foreword by Rear Admiral Raymond C. Smith, USN (Ret.), former Deputy Commander at U.S. Navy Special Warfare Command, Coronado, CA; and an after word by Dr. Linton Wells, Acting Assistant Secretary of Defense (Networks and Information Integration) and Department of Defense Chief Information Officer.

Extending the User's Reach: Responsive Networking for Integrated Military Operations

David Gompert, Alf Andreassen, and Charles Barry

Nature of Project

The aim of the study is to identify a path for the U.S. DoD to improve the responsiveness of military information networks for joint warfighters. This is not a technical treatise about bits and bandwidth; it proposes no architecture or standards. Rather it looks at how military-operational information requirements relate to national strategy and at how those requirements are set and met. In particular, it considers how governance, economic power, and management processes within DoD should be aligned to maximize the prospects of meeting user needs.

This study relied principally on three methods to yield its findings:

- Review of important government documentation bearing on the use of information networking to support users in joint military operations.
- Interviews of persons from all the organizations involved in current efforts.
- Integration of strategic, military-operational, defense-institutional, technological, and economic perspectives and analysis.

Above all, this is an effort to widen the context in which defense networking is examined.

Project Summary

The DoD is now investing heavily in information systems to support net-centric military capabilities and joint operations. With such programs, it is creating a global backbone network and striving to get useful bandwidth and information services to the warfighter. Spending on communications and intelligence has grown by 50 percent since 2001, after declining in the 1990s. Such investment in networks is needed but not enough to harness the full power of information in national defense.

As long as it relies on its current business processes to design, fund, and acquire information systems, DoD will struggle to provide its users—joint warfighters—with the *access* to information and opportunities for *collaboration* that deeply integrated joint operations demand. In contrast to the primacy of users in creating information solutions in many sectors, and the Internet itself, DoD's users are under-represented, under-privileged, and under-utilized in these processes.

Findings

DoD cannot keep pace with, and thus readily exploit, powerful new information technologies that are propelled by larger, faster, and more fluid commercial markets. The protracted and inflexible ways DoD specifies its needs, allocates investment funds, and procures new systems are unsuitable for acquiring information solutions. This explains why DoD is a straggler in the use of Internet search technology and cellular communications, why customers within DoD increasingly bypass "the system," and why leading IT firms stay out of the defense market.

These anomalies will become more glaring and debilitating in the coming years:

- As demands grow for joint operational integration and, therefore, for information integration well below the Joint Task Force command level.
- As new technologies enabling users to seek and pull information from disparate networks flourish in the civilian world.
- As adversaries start to exploit information infrastructure and networking principles with growing ease and speed.

The strategic danger is that integration of U.S. forces will be delayed and discredited by the failure of DoD to provide joint user-responsive C4 solutions. Fixing this requires work at three levels: *technology, processes, and governance.*

The most momentous *technology* developments today are those that increase the power of networked end-users, both in finding and using information as well as in shaping solutions, on the grounds that they know best what information and collaboration they need. The new technologies that allow end-users to meet their needs and shape solutions are as important as distributed processing, the Internet, and mobile telecommunications, and they are changing whole industries for the better. The military potential of these technologies is especially great when considering the needs of warfighters to pull relevant information from, and collaborate across, disparate networks and organizational boundaries.

With such user-reach technologies, the problem of network interoperability can be solved without wholesale replacement of the embedded base of disparate, non-joint systems. Connectivity standards can become user-responsive and largely self-enforcing. The need for, and cost of, systems integration can be reduced, and solutions can be continuously improved. If DoD is serious about the "user-pull" principle, it must catch this new wave.

Yet, DoD is at risk of having to swim after this wave, as it has swum after others. Its processes for setting C4 requirements, allocating resources to meet those requirements, and then acquiring capabilities are ponderous and insensitive to the needs of war-fighting users in integrated operations. The separate military services, which dominate those processes, lack the perspective, ability, and incentive to meet joint C4 needs. Those who control money are network providers, not customers, and they do not put high priority on deeply integrated joint warfare.

The crux of these problems is that military-operational users are bereft of market power.

Recommendations

For joint C4, the following changes are needed to shift power to users:

- Requirements should be set by the joint war-fighting community—in particular, JFCOM, informed by needs of the other COCOMs. JCIDS is a step in the right direction but inadequate as a bureaucratic planning process.
- JFCOM should be responsible for seeking resources through the PPBE system.
- JFCOM itself should acquire information solutions, relying on either DISA or the military services as its procurement agents.

- A new C4 acquisition process should be in harmony with the rapid and continuous way the IT market works and should seek to attract IT firms. This requires reform of the Federal Acquisition Regulations as it applies to joint C4, not work-arounds and waivers.

Revising and using new business processes for joint C4 will require purposeful *governance*. As strategic stakeholder, the Secretary of Defense should articulate a vision and a standard:

- The vision is of deeply integrated and highly fluid joint operations.
- The standard is of unobstructed warfighter access to any relevant information and unbounded collaboration with any other warfighter.
- The Secretary of Defense should also set the conditions for success by instituting process reforms and ensuring that adequate resources are devoted to user-responsive networks.

In sum, *if* DoD aligns economic power with the joint community (the customer) in its processes; embraces the goals of deep integration, unobstructed access, and unbounded collaboration; draws the IT industry into its market; and elevates the role of the CIO, it can exploit the new user-responsive technologies and take a major leap forward in information integration, which is critical to a truly net-centric force.

Project Impact

The study will be published by CTSNP in conjunction with the Office of the Secretary of Defense (Office of Force Transformation) as a CTNSP *Defense & Technology Paper* which is distributed broadly to technologists, scientists, and policymakers.

Information and Communications Technology (ICT) and Stabilization & Reconstruction

Stabilization and Reconstruction (S&R) Workshops: 28 October 2004, 16 December 2004, 18 February 2005, 10 May 2005

Nature of Project
These four workshops were the beginning of a series NDU is sponsoring in partnership with the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) and in collaboration with the Department of State, Office of the Coordinator for Reconstruction and Stabilization (S/CRS) and the Humanitarian Information Unit (S/HIU). The purpose of the study is to explore the information and communications technology (ICT) and relationships that are available to the S&R community, thereby increasing effectiveness and the capacity of the community to respond to S&R needs.

The first four workshops included participants from the U.S. interagency and selected non-governmental organizations (NGOs). The eventual intent is to gather members from the larger S&R community such as multi-national militaries, international organizations, businesses, host nations, and the media.

Project Summary
The workshops have three main foci: information and information exchange needs, information systems, and data. Attention thus far has been directed toward the existing and projected information systems for S&R operations. Education and training will be considered in future workshops.

Findings
As of July 2005

- Descriptions of baseline systems and their relationships have been developed for selected S&R operations.
- The DoD Net-Centric Data Strategy has been adapted for S&R operations.
- A preliminary characterization of information requirements for selected S&R functions has been completed.
- Detailed findings from the workshops have been captured in a paper delivered to Royal Military College, Kingston, Ontario, Canada.

Recommendations

- The development of an agreed ICT architecture for future S&R operations.
- Continued collection and sharing of lessons learned and best practices in the area of ICT.

Project Impact
The end product of the workshops will be a report on ICT Support of S&R Operations. This study, scheduled for release in winter 2006, will provide recommendations for

senior U.S. decisionmakers in S&R operations. Subsequent versions will be generalized to support the needs of other players in S&R.

The information learned in these workshops is supporting ASD/NII initiatives (e.g. World Summit on the Information Society [WSIS]) as well as the President's Greater Middle East Initiative).

NDU/CTNSP is providing numerous briefings to the S&R community based on the findings of the workshops, most notably key decisionmakers for DoD's Quadrennial Defense Review (QDR). Briefings have been provided to the Deputy Director of Operations for the Defense Information Systems Agency (DISA) and the Assistant Secretary of Defense for International Security Affairs (ISA).

The primer is supporting an HIU demonstration of ICT in September 2005.

Information Communications Technology (ICT) to Support Stabilization and Reconstruction (S&R) Operations

Stuart Starr and Larry Wentz, July 2005

Nature of Project

This paper highlights some of the challenges of Information and Communications Technology (ICT) support to S&R operations and discloses preliminary findings from three workshops sponsored by CTNSP.

Project Summary

Cultural and institutional roadblocks prevent the implementation of ICT capabilities that would enhance the sharing of information in S&R operations. S&R players must move beyond reliance on personal contacts and "old boy" style information sharing to the utilization of commercially available information technologies and implementation of organizational best practices. The net effect would be effective and prompt S&R collaboration among militaries, civil authorities, NGOs, international organizations (IOs), and the host country.

Findings

- Civilian and military information systems tend to be stove-piped, with limited coverage and capacity and little interconnection of the tactical military and civilian systems. The commercial Internet becomes the de facto information network.
- Informal and unofficial relationships play an important role in the sharing of information in S&R operations, making it difficult to serve a wider audience and to standardize information sharing processes.
- There is inconsistent use of standardized meta-data when collecting and providing S&R operation information. This makes it difficult to determine the credibility and currency of the information.
- The accessibility of the commercial Internet has increased sharing capabilities but also increases the difficulties of information management. Tacit knowledge, often imparted in briefings, discussions, and firsthand observation, remains an important source of information.
- There is no agreed overarching concept of operations (CONOPS) and system architecture for ICT support to S&R operations. Civil-military players often prefer an "old boy" networking approach to information sharing rather than employing technology to create a federated ICT network.
- Technology is available to solve many of the information sharing problems; however, cultural and institutional roadblocks within and between organizations prevent solutions from being implemented.
- The goal of the S&R community can be broadly divided into two macro-objectives: that data be *available* to the user and that data be *usable* by the recipient.

Recommendations

The following actions would enhance information sharing in S&R operations:

- Ensure that civilian (governmental and nongovernmental) and military organizations work to create a *common culture of trust* in information networks.
- Conduct an assessment of information needs and existing knowledge prior to S&R engagement in order to identify the gaps in data, information and knowledge.
- Provide standardized metadata (e.g., source, date, definitions) for all collected and shared information so that it can be pooled, compared, verified, mapped, and used for analysis.
- Establish collaboration networks as a means to capture and share tacit knowledge and dismantle organizational stovepipes.
- Employ visualization to represent complex data and information, display patterns and relationships, and depict a geo-spatial common operating picture.
- Demonstrate the practical applications of new information tools and technologies and use collected data and information to answer questions and respond to identified information needs.
- Recognize the value of tacit knowledge gained from field experience, collaboration, and learned expertise.
- Promote the use of new tools and technologies, such as personal digital assistants (PDAs), Global Positioning Systems (GPS) Geographic Information Systems (GIS), and virtual collaboration networks; provide advanced training to ensure that personnel use them effectively and routinely in their work.
- Create an environment of willingness to conduct more open sharing between the civilian and military participants.
- Seek achievement of an agreed strategy, CONOPS, systems architecture, and standards for ICT support to S&R operations.
- Develop an ICT technology roadmap with near, mid and long-term goals.
- Seek agreement on organization arrangements for creating and maintaining a civil-military collaborative information environment, including managing the systems supporting the distribution of information.
- Develop an ICT support to S&R operations primer that would outline shared understandings of participants' roles and capabilities, principles for information exchange, tool kits and fly away package options, and best practices.
- Develop and acquire ICT fly away packages for use by civilian government and military participants that facilitate information sharing with IOs and NGOs and can be left behind for building host nation capacity.

Project Impact

The paper was presented to military and civilian S&R experts at the conference "Cornwallis Group X: Analysis for New and Emerging Societal Conflicts", March 21-24, 2005, Royal Military College, Kingston, Ontario, Canada.

Learning from Darfur: Building a Net-Capable African Force to Stop Mass Killing

David C. Gompert, Courtney Richardson, Richard L. Kugler, and Clifford H. Bernath, July 2005

Nature of Project

The scope of the project was to examine what would be needed to empower the international community to conduct effective, decisive, and forcible humanitarian interventions in African mass killing conditions. The report concluded that an African Humanitarian Combat Force (AHCF) should be developed. The AHCF would be a standing combat force to stop or prevent genocide based upon "network-capable" principles of speed, awareness, survivability, supportability, connectedness, and lethality. This project relates to other research on the use of IT for stabilization and reconstruction and humanitarian efforts.

Project Summary

The study examines two hypotheses. First, that well-prepared net-capable African combat forces, with the right operational and intelligence support from Western militaries, could intervene decisively to defeat mass-killing forces under most plausible conditions. Second, that such a force is possible in the foreseeable future, provided African and key Western countries focus, cooperate and commit resources. The study describes the Darfur mass killing, applies net-capable principles to the Darfur mass killing conditions, develops the AHCF, outlines a possible operation, discusses the construction of the AHCF, highlights policy issues, and formulates recommendations.

Findings

- Mass-killing perpetrators are killers and not fighters; they are effective against unarmed civilians, but ineffective against trained forces willing to engage in combat (e.g. Sierra Leonean gangs and Democratic Republic of Congo (DRC) gangs were quickly addressed by British Special Forces and French troops respectively).
- The West has the means, but due to other national security interests, lacks the will to intervene, whereas African nations have the will, but lack the ability to intervene.
- Given the need to prevent and halt mass killing, a credible combat intervention force is needed to convince killing forces that they can not use violence. This force would have to be trained, organized, and mandated to engage and defeat the killers, as necessary.
- Darfur exemplifies typical mass killing conditions in Africa: large numbers of defenseless civilians killed over wide areas; killing forces that lack the ability to engage in real combat; government that lacks the ability to stop the killing; alliances of convenience; and underdeveloped infrastructure. A humanitarian combat force that works along the principles of speed, awareness, survivability, supportability, connectedness, and lethality would be most effective in deterring and stopping mass killings. Thus, such a humanitarian combat force would be "network-capable"—using high-quality special operations forces, deployable

sensors and other intelligence, high-speed data links, command and control modules, ground mobility, rotary and fixed wing aircraft and precision weapons.
- The benefits of such a force design include reduced force requirements, reduced logistics requirements, greater dispersal, greater integration of operations because of increased battlefield awareness, and greater lethality because of networked assets and precision weapons.
- Current capacity-building efforts for Africa are valuable and establish a solid baseline of peacekeeping capabilities. However, these programs do not cultivate peace-enforcement capabilities.
- African-Western partnership is needed to evolve from the current capability to an effective AHCF. Western input will diminish over time as African capabilities improve.
- Policy issues include mandates and rules of engagement, intelligence sharing, technology sharing, use of Western troops, minimizing misuse of enhanced capabilities, and command and control issues.

Recommendations

- African and Western governments and institutions should discuss the route towards an AHCF without delay.

Project Impact

- The research was published by CTNSP as *Defense & Technology Paper* 15 and is available on the CTNSP website at: http://www.ndu.edu/ctnsp/Def_Tech/DTP%2015%20Darfur.pdf.
- The concept of boosting African peace operations capabilities has been introduced to the draft of the current QDR.
- The authors have been consulted on a number of draft bills for Congress on African development and security matters.

Appendix B: Brief Biographies of Contributors to CTNSP IT Studies

Gordon Adams is a Professor of the Practice of International Affairs and Director of Security Policy Studies at the Elliott School of International Affairs, The George Washington University. He was Deputy Director of the International Institute for Strategic Studies and Associate Director for National Security and International Affairs at the White House Office of Management Budget. He has written extensively on U.S. and European defense budgeting and planning and on transatlantic defense policy.

Alf A. Andreassen is a Principal and co-founder of the Paladin Capital Group Homeland Security Fund, and serves as a member of the Boeing Corporation Homeland Security Senior Advisory Board. He has served on the Board of Advisors for the National Security Agency and on the Chief of Naval Operations Executive Panel. He has served on many corporate Boards of Directors, including as Chairman of Circadence Corporation, an information technology company; AgION Technologies, Inc., an antimicrobial solutions company; and PrivaComp, a medical information company. He has also served on numerous government-sponsored Boards and Task Forces. Dr. Andreassen holds a Doctorate in Physical Chemistry from Cornell University and a postdoctoral fellowship in Materials Science.

Charles Barry is a retired U.S. Army officer associated with National Defense University since 1993 as a military analyst specializing in transatlantic relations, defense information systems, U.S. grand strategy, and Army force structure. Mr. Barry has been qualified as a military strategist for more than 20 years and is considered an expert on strategy, international relations, and information systems related to command and control. He also consults on public-sector organizational development, productivity, and resource management. His current areas of concentration include DoD operational network integration, joint stabilization and reconstruction operations, and international capabilities in support of U.S. military operations. Mr. Barry is a doctoral candidate in Public Information Resource Management at the University of Baltimore.

Guy Ben-Ari is a consultant with the Defense Industrial Initiatives Group at the Center for Strategic and International Studies, where he specializes in U.S. and European defense technology policies. Prior to joining CSIS he was a research associate at the George Washington University's Center for International Science and Technology Policy and a consultant for the European Commission and the World Bank focusing on innovation policy and evaluation.

Alan Berman currently is a private consultant. He has an extensive background in defense research and technology. His areas of expertise include; space operation capabilities and satellite system development, information operations, the management of basic research programs, the development of surveillance systems, and the development of advanced weapon systems along with their associated combat management and data

integration systems. His previous positions include Dean of the Rosenstiel School of Marine and Atmospheric Sciences at the University of Miami and Director of Research at the Naval Research Laboratory. He has provided analytic studies and management support for the Applied Physics Laboratory of Pennsylvania State University and for the Center of Naval Analyses. He has served on numerous Government advisory and scientific boards including panels of the Defense Science Board, the Naval Studies Board of the National Research Council, the Naval Research Advisory Committee, and on Laboratory over sight panels of the Department of Energy

Clifford H. Bernath is the Senior Fellow at the Africa Center for Strategic Studies (ACCS), National Defense University. He is developing programs that help U.S. officials better understand African issues and that help African officials better understand U.S. policies and programs in Africa. Prior to his arrival at the ACSS, he was the Director of Conflict Prevention and Resolution at Refugees International (RI), an advocacy NGO that generates humanitarian assistance and protection and works to end the conditions that create population displacements. His focus at RI was to study ways to improve UN peacekeeping missions as a means of shortening or preventing armed conflicts that cause population displacements and human rights abuses. He served for 21 years in the U.S. Army, including a tour as an Infantry officer in Vietnam. He also worked in the Pentagon in a variety of career civil assignments, including Principal Deputy Assistant Secretary of Defense for Public Affairs, and Director of the American Forces Information Service.

Hans Binnendijk holds the Roosevelt Chair of National Security Policy at the National Defense University and is Director of the Center for Technology and National Security Policy. He previously served on the National Security Council as Special Assistant to the President and Senior Director for Defense Policy and Arms Control (1999-2001). From 1994 to 1999, Dr. Binnendijk was Director of the Institute for National Strategic Studies at the National Defense University. Prior to that he was Principal Deputy Director of the State Department's Policy Planning Staff (1993-1994).

Gerald Borsuk is the Superintendent of the Electronics Science and Technology Division, Naval Research Laboratory (NRL), Washington, DC. He is responsible for the in-house execution of a multi-disciplinary program of basic and applied research in electronic materials and structures, solid state devices, vacuum electronics, and circuits. He is also responsible for the coordination and oversight of the Electronics Focus Area Program at NRL. Dr. Borsuk serves as the Office of Naval Research (ONR) representative for electronics basic research to the Office of the Secretary of Defense and is chair of the Tri-Service Scientific Planning Group for Electronics. He was Navy Deputy Program Manager and Technical Director for the now completed DARPA/Tri-Service MIMIC and MAFET Programs. He was the Department of Defense technical representative for Electronics to the Wassenaar Arrangement dealing with export control. He also served as DoD representative to the President’s National Science and Technology Council’s Electronic Materials Working Group. Dr. Borsuk received a Ph.D. in Physics from Georgetown University in Washington, DC in 1973. He is a fellow of the IEEE, a member of the American Physical Society, a member of the AVS, a member of the Sigma Xi, and the Navy’s Deputy Member to the Advisory Group on Electron Devices

(AGED). He has 37 technical publicans, four patents and eleven invention disclosures. He is also the recipient of the IEEE Frederick Philips Medal, the IEEE Harry Diamond Memorial Award, the IEEE Millennium Medal, and an IR-100 Award for his work on high-speed CCDs.

Paul Bracken is a leading expert in the study of global competition and the strategic application of technology in business and defense. He teaches *Business, Government, and Globalization* which examines comparative capitalism and business restructuring in the U.S., East Asia, and Europe. He also teaches the core Yale School of Management course *The Strategic Environment of Management*; and *Strategy, Technology, and War* which examines technology and innovation landscapes in business and defense. Dr. Bracken is a member of the Council on Foreign Relations and was a visiting professor at Beijing University. At Yale he is a Fellow of Silliman College and a member of the Elizabethan Club. Before joining the Yale faculty, Professor Bracken was on the senior staff of the Hudson Institute for ten years, where he directed the management consulting arm of the Institute. Dr. Bracken holds a Ph.D. (Operations Research) from Yale University, and a Bachelor of Science degree (Engineering) from Columbia University.

Richard Chait is currently a Distinguished Research Professor at the Center for Technology and National Security Policy, National Defense University. Other academic positions include Visiting Professor appointments at both Air Force Academy (2003-2004) and West Point (1983-1984). He has also held several Senior Executive Service positions including Director of Army Research, and Chief Scientist, Army Material Command. On assignment from Carnegie Mellon University, he was also Senior Technical Advisor, Office of the Air Force Deputy Assistant Secretary for Research, Development and Engineering. Prior positions in the private sector have included the National Academy of Sciences as Director, National Materials Advisory Board, and early in his career as Staff Engineer, United States Steel Corporation. Dr. Chait has graduate degrees in Metallurgical Engineering and Solid State Science and has published over 70 open literature papers/reports and is co-editor of 3 books.

John C. Cittadino is president of JCC Technology Associates, Inc., founded in July 1987 to provide technical and managerial consultant services to government and industry on C3I, Information Technology, Space, Navigation and Air Traffic Control Systems. He currently chairs an Army Senior Advisory Group on C4ISR R&D programs supporting Army Transformation. He recently departed the Army Science Board after 6 years service and presently serves as an active consultant to the Board. He has served as a consultant to the Defense Science Board on C3I subjects. In 2000-01 he chaired a Joint Senior Advisory Group (JSAG) to the Assistant Secretary of Defense (C3I). He is also a member of the American Institute of Aeronautics and Astronautics C4I Technical Committee and past Chair of the National Defense Industrial Association (NDIA) C4ISR Executive Committee. From March 1977 to July 1987, he served in the Office of the Secretary of Defense as the director, Theater and Tactical Command, Control and Communications. From July 1968 to March 1977, he served as program manager for the Army's Navigation/Control Systems (NAVCON) responsible for the formulation and execution of the technical program encompassing the design, development, production

and operation of the Positioning and Navigation System (PANS) and the Air Traffic Control System (ATMS). Mr. Cittadino received his BS in Mechanical Engineering from New Jersey Institute of Technology in 1955. He received his Master of Science Degree in Operations Research/Engineering Management from Stevens Institute in 1964. He is a 1976 graduate of the National Defense University, Industrial College of the Armed Forces (ICAF).

Donald C. Daniel is a Principal Research Engineer with the Georgia Tech Research Institute and a Distinguished Research Professor with the National Defense University's Center for Technology and National Security Policy. He is also a former Air Force Deputy Assistant Secretary for Science, Technology and Engineering and was the first Executive Director of the Air Force Research Laboratory. Throughout his career, Dr. Daniel has been involved extensively in international activities having served on numerous NATO and other policymaking panels and boards. He is currently the Chairman of NATO's Research and Technology Board.

Don J. DeYoung served as the Center for Technology and National Security Policy's project manager for the Congressionally mandated Section 913 DoD Laboratory Relevance study. Mr. DeYoung is on detail to the Center from the Naval Research Laboratory (NRL) where he is the Executive Assistant to the Director of Research. In that position he investigates general management issues, conducts special studies, and develops responses to Navy, DoD, and congressional policy. He has served as a Navy analyst on two DoD base closure projects-Base Realignment and Closure (BRAC-95) from 1994 to 1995, and VISION-21 in 1997. Mr. DeYoung received the Navy Meritorious Civilian Service Award in 1995 and the ONR Group Achievement Award in 1997. He has a master's in Public Administration from Syracuse University and a master's in National Security Studies from Georgetown University.

Robert C. Fonow is Managing Director of RGI Ltd., a consulting firm providing cross-cultural troubleshooting and turnaround services for the international telecommunications, Internet and broadband industries. He has completed turnaround assignments as President of Sprint Japan, General Manager of Scientific Atlanta Shanghai, President of SFA Datacomm in the United States, VP Global Operations for Red Cube in Zurich, and General Sales Manager of ITT Worldcom in London. He is currently on assignment with a Swiss investment group on merger and acquisition due diligence and troubleshooting in Russia and China. Mr. Fonow was educated at The London School of Economics and Political Science (MSc.Econ) and the University of Wales, Lampeter. Prior to entering university, he served in the United States Air Force in electronics intelligence and communications in Japan, Italy and England. He is a member of the International Institute for Strategic Studies in London and is an adjunct Research Fellow at the National Defense University Foundation writing on the geopolitics and international relations of the Internet and telecommunications industry.

Jacques S. Gansler, former Under Secretary of Defense for Acquisition, Technology, and Logistics, is the University of Maryland’s Vice President for Research and the Roger C. Lipitz Chair in Public Policy and Private Enterprise. As the third-ranking civilian at

the Pentagon from 1997 to 2001, Professor Gansler was responsible for all research and development, acquisition reform, logistics, advance technology, environmental security, defense industry, and numerous other security programs. Before joining the Clinton Administration, Dr. Gansler held a variety of positions in government and the private sector, including Deputy Assistant Secretary of Defense (Material Acquisition), assistant director of defense research and engineering (electronics), executive vice president at TASC, vice president of ITT, and engineering and management positions with Singer and Raytheon Corporations. Throughout his career, Dr. Gansler has written, published, and taught on subjects related to his work. He is a member of the National Academy of Engineering and a Fellow of the National Academy of Public Administration. Additionally, he is the Glenn L. Martin Institute Fellow of Engineering at the A. James Clarke School of Engineering, an Affiliate Faculty member at the Robert H. Smith School of Business and a Senior Fellow at the James MacGregor Burns Academy of Leadership (all at the University of Maryland). For 2003 – 2004, he served as Interim Dean of the School of Public Policy

David C. Gompert is currently a Senior Fellow at the RAND Corporation. From 2004 to 2005, Mr. Gompert was Distinguished Research Professor at the Center for Technology and National Security Policy, National Defense University. From 2003 to 2004, he was the Senior Advisor for National Security and Defense at the Coalition Provisional Authority, Iraq. He has held senior government appointments at the State Department and the National Security Council; senior executive positions at the RAND Corporation and in the information technology industry; and teaching posts at the National Defense University and the United States Naval Academy. Mr. Gompert's positions have included president of the Systems Management Group at Unisys and president of RAND Europe. He has published extensively on international affairs, national security policy, and information technology. Mr. Gompert holds a Master of Public Affairs degree from the Woodrow Wilson School, Princeton University, and a Bachelor of Science degree in engineering from the United States Naval Academy.

Stuart E. Johnson is Deputy Director and a Distinguished Professor at the Center for Technology and National Security Policy, where he occupies the Chair for Force Transformation Studies. He specializes in the impact of technology on defense planning and the transformation of U.S. military forces to meet the challenges of the 21st century. He served in the Office of the Secretary of Defense (PA&E) and was Director of Systems Analysis at NATO Headquarters in Brussels. He directed the International Defense programs at the RAND Corporation, overseeing a study program to support allied ministries of defense. His publications include studies on strategy and force planning, coalition operations with European allies, and the science of command and control. Dr. Johnson is a Phi Beta Kappa graduate of Amherst College (1966) with a B.S. degree in Chemistry, and obtained his Ph.D. from the Massachusetts Institute of Technology in Physics, in 1971. Dr. Johnson did post-doctoral work in Physics at the University of Leiden, Netherlands, 1971-72.

Kenneth Jordan is an independent consultant with experience in systems engineering in the areas of space systems, communications, military C^3I, and project management. Dr.

Jordan is presently supporting the Office of Naval Research (ONR) in developing research priorities in Net-Centric Warfare, the Defense Information Systems Agency (DISA) in the systems engineering for the Global Information Grid (GIG), and USSTRATCOM in the area of Transformational Communications Architecture. From 1979 until 2005, Dr. Jordan was with Science Applications International Corporation, from 1992 as a Corporate Vice President. During that time he was responsible for programs in the C^3I arena including communications networking, satellite communications, and air force mission planning systems. He worked on projects for DARPA on advanced C4I systems, information technology assessment, and has supported the Advanced Battlespace Information System (ABIS) Task Force. He also led a group in the modeling and analysis of strategic C^3I systems, including the use of numerous command and control, network and propagation models to analyze the effectiveness of strategic C^3I systems in a stressed environment. In the 1970s, he held several positions in the Department of Defense including Director, Strategic and Space Systems in the Office of the Secretary of Defense, and Principal Deputy Assistant Secretary for R&D, U.S. Air Force. Work prior to 1973 was comprised mainly of leading a group of communications satellite engineers at MIT Lincoln Laboratory. He received his Doctorate in Science from M.I.T. in 1960.

Franklin Kramer is a Distinguished Research Fellow at the Center for Technology and National Security Policy. Mr Kramer was Assistant Secretary of Defense for International Security Affairs from March 1996 to February 2001, and Deputy Assistant Secretary for European and NATO Affairs from January 1996 to March 1996. He has also served as the Principal Deputy Assistant Secretary of Defense for International Security Affairs from 1979 to 1981, and as Special Assistant to the Assistant Secretary of Defense for International Security Affairs from 1977 to 1979. Mr. Kramer is the chairman of the board of the World Affairs Council of Washington, D.C.; chairman of the Committee on Asian and Global Security of the Atlantic Council and on the Executive Committee of the board; a Capstone Professor at George Washington University Elliott School of International Affairs; and on the board of directors and board of advisers of other organizations. Mr. Kramer has been a partner with the Washington, D.C. law firm of Shea and Gardner. Mr. Kramer received a B.A. cum laude from Yale University in 1967 and a J.D. magna cum laude from Harvard Law School in 1971.

Richard Kugler is a Distinguished Research Professor at the Center for Technology and National Security Policy, National Defense University. His specialty is U.S. defense strategy, global security affairs, and NATO. He advises senior echelons of the Office of the Secretary of Defense, the Joint Staff, and the interagency community. He is the author of multiple books, journal articles, and official studies on U.S. defense strategy and programs as well as NATO and global security affairs. Dr. Kugler has his doctorate from the Massachusetts Institute of Technology.

Irving Lachow is a Professor of Systems Management at the National Defense University and Director of the Information Resource Management College's Advanced Management Program. Previously, Dr. Lachow was a Senior Associate at Booz Allen Hamilton, where he managed projects in the areas of IT Strategy and Planning for

numerous government clients. Dr. Lachow has extensive experience in both IT and national security. He has worked for Digital Signature Trust, the RAND Corporation, and the Office of the Deputy Under Secretary of Defense (Advanced Systems and Concepts). Dr. Lachow received his PhD in Engineering & Public Policy from Carnegie Mellon University. He earned a B.A. Political Science and a B.S. in Physics from Stanford University.

John M. Logsdon is Director of the Space Policy Institute of The George Washington University's Elliott School of International Affairs, where he is a Professor of Political Science and International Affairs. He has written and published widely on US and international space policy and history.

Joseph N. Mait is on the staff of the U.S. Army Research Laboratory (formerly Harry Diamond Laboratories), where he has been since 1988. From 2002 – 2004 he was on special assignment to the Center for Technology and National Security Policy, where he served as a Senior Research Fellow. Dr. Mait leads basic research activities in optics and photonics. He also served as the Sensors Directorate Associate for Science and Technology. He is an Adjunct Associate Professor of Electrical Engineering at the University of Maryland, College Park, and a Fellow of the professional societies SPIE and OSA, as well as a senior member of IEEE.

Justin Perkins is a former Research Associate with the Center for Technology and National Security Policy, National Defense University. Before working at the National Defense University, he served as the Chief Operating Officer for World Blu, Inc., a consulting firm pioneering the field of organizational democracy, and as co-founder and director of Afrique Profonde, a human rights organization in Congo. He also has been involved with several small businesses and served for several years as a water resource administrator for the State of Colorado. Mr. Perkins holds a Masters of Business Administration from the University of Colorado and a B.A. in History and World Perspectives from Principia College.

Paul W. Phister, Jr., is currently the Air and Space Strategic Planner at the Air Force Research Laboratory's Information Directorate in Rome, New York. In this role, Dr. Phister is responsible for developing the Directorate's information technology investments portfolio for the years 2011 to 2029. Dr. Phister represents AFRL/IF on all activities relating to space and related technologies applicable to space development and operations. Dr. Phister is a recognized command and control subject matter expert and has supported the Air Force in near-, mid-, and long term command and control strategic investments. Dr. Phister spent 25 years in the military, where he has worked primarily in intelligence and space systems development and operations. Dr. Phister is a senior member of the IEEE, as well as a licensed software engineer from the State of Texas.

Courtney Richardson is a Research Associate at the Center for Technology and National Security Policy, National Defense University, where she focuses on network-centric warfare issues. She has previously worked at Jane's in London, and volunteered with the United Nations Information Center in Washington, DC. She has a MA in

Security Policy Studies from the Elliott School of International Affairs at the George Washington University and a BSc in International Relations from the London School of Economics and Political Science.

Desmond Saunders-Newton has served as the Deputy Director of the Pre-Conflict Management Tools (PCMT) program and co-program head of Computational Social Science Modeling (CSSM) initiative at the Center for Technology and National Security Policy. In conjunction with his appointment with the Center, Desmond heads the Social Computation and Complexity Directorate of BAE Systems Advanced Information Technologies' Intelligence Innovation Division, and is an Adjunct Associate Professor in the University of Southern California's School of Policy, Planning & Development. Prior to joining NDU, he served as the AAAS Defense Science & Technology Fellow in the Office of the Deputy Undersecretary of Defense for Advanced Systems & Concepts (DUSD/AS&C). He subsequently served as a senior consulting scientist in several technical offices of the DARPA. Dr. Saunders-Newton has published and presented over 100 professional and technical papers in areas including advanced computational models, information operations, and computational social science. He serves as the Associate Editor for Research Method and Statistics of the Social Science Computer Review, a member of the Advisory Board of the Public Policy and International Affairs program, and the sits on the External Advisory Board of George Mason University's Center for Social Complexity. Dr. Saunders-Newton earned his Ph.D. in Policy Analysis (concentration in Computational Policy Analysis), as well as a M.Phil in Policy Research, from the Pardee RAND Graduate School of Policy Studies. He also received a Master of Public Policy (concentrations in International and Quantitative public policy) from the University of Michigan's Ford School of Public Policy, and a B.A. in Physics from Lawrence University.

Albert A. **Sciarretta** is president of CNS Technologies, Inc., and conducts technology assessments as well as designs and executes operational demonstrations for an Army Research Laboratory sponsored NATO urban sensor demonstration and an Army Aberdeen Test Center (ATC) Joint distributed live-virtual-constructive test event. He has provided similar support to Defense Advanced Research Project Agency (DARPA) urban warfare experiments, an OSD Smart Sensor Web experiment, and a Defense Modeling and Simulation Office (DMSO) Joint Operations on Urban Synthetic Terrain (JOUST) demonstration. His current efforts include assisting the Defense Test Resource Management Center (DTRMC) and the Army's Battle Command, Simulation, and Experimentation Directorate (BCSED) in the development of science and technology investment strategies. He is a frequent volunteer participant in committees of The National Academies and DOD. He is a retired Army officer, whose service included operational assignments, instructing at the U.S. Military Academy, serving on an armored vehicle technology task force, and assisting the Chief Scientist, U.S. Material Command. He has a BS in General Engineering from the U.S. Military Academy, and has both an MS degree in Operations Research and an MS degree in Mechanical Engineering from Stanford University.

Stuart H. Starr is a Distinguished Research Fellow at the Center for Technology and National Security Policy and the President of The Barcroft Research Institute where he consults on national security issues, teaches courses on systems acquisition and assessment, and participates on Department of Defense science boards. His primary interest is in issues associated with command and control, strategic planning, modeling and simulation, and the acquisition of complex systems-of-systems. He has served as the Director of Plans, The MITRE Corporation; Assistant Vice President for Systems Planning and Evaluation, M/A-COM Government Systems; Director of Long Range Planning and Systems Evaluation, OASD(C3I); and Senior Project Leader, the Institute for Defense Analyses. He is a member of the Army Science Board and has participated on numerous Defense Science Board, Air Force Science Advisory Board, NATO, and National Research Council studies. He has a BS (Electrical Engineering) from Columbia University and MS and PhD degrees in EE from the University of Illinois. He is a former National Science Foundation Fellow, a Fellow of the Military Operations Research Society, an Associate Fellow of the American Institute for Aeronautics and Astronautics, and a senior member of the IEEE. In 2004 the Military Operations Research Society awarded him the Clayton Thomas Medal for lifetime accomplishments in operations research.

Larry Wentz is a Senior Research Fellow at the Center for Technology and National Security Policy, National Defense University and consults on Command and Control (C2) issues. He is an experienced manager, strategic planner, and C4ISR systems engineer with extensive experience in the areas of multinational military C2 and C3I systems interoperability, civil-military operations and information operations support to peace operations. He is an author and lecturer on multinational C4ISR systems interoperability, Information Operations and Civil-Military Operations. He was a contributing author to the AFCEA International Press books, *The First Information War and CYBERWAR 2.0* and Canadian Peacekeeping Press books, *The Cornwallis Group Series*. The NDU/CCRP press published his book, *Lessons from Bosnia: The IFOR Experience* and the CCRP press published his book, *Lessons from Kosovo: The KFOR Experience*. He has lectured at the Canadian International Pearson Peacekeeping Training Centre, the NDU School of Information Warfare and Strategy, the George Mason University Program on Peacekeeping Policy and the DIA Joint Military Intelligence Training Center. Mr. Wentz has a Bachelor of Science in Electrical Engineering from Monmouth College and a Masters of Science in Systems Engineering and Operations Research from the University of Pennsylvania's Moore School of Engineering.

Ray A. Williamson is Research Professor of Space Policy and International Affairs at the Space Policy Institute of The George Washington University. He has published widely on space and satellite programs and edited *Dual-Purpose Space Technologies: Opportunities and Challenges for U.S. Policymaking* (Space Policy Institute). Previously, he was Senior Associate in the Congressional Office of Technology Assessment.

Elihu Zimet is a Distinguished Research Professor at the Center for Technology and National Security Policy and is currently working on issues related to the role of technology in military transformation. As a member of the Senior Executive Service

(SES), he headed the Special Programs, and subsequently, the Expeditionary Warfare Science and Technology Department at the Office of Naval Research (ONR). He directed basic research, applied research, and advanced development programs in missile, gun and directed energy weapons, aircraft, avionics and propulsion, low observable and counter-low observable technologies. He also provided technology support to the Marine Corps through his oversight of several Advanced Concept Technology Demonstrations including Cruise Missile Defense, Precision Satellite Targeting System, and Extending the Littoral Battlespace. For many years Dr. Zimet served on NATO AGARD and RTO technology panels. He was twice awarded the Meritorious Presidential Rank Award in the SES and the Distinguished Civilian Civil Service Award.

Appendix C: Abbreviations and Acronyms

ACTD	Advanced Concept Technology Demonstration
AFRL	Air Force Research Laboratory
AHCF	African Humanitarian Combat Force
ASD(NII)	Assistant Secretary of Defense(Networks and Information Integration)
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CECOM	Communications Electronics Command
CIA	Central Intelligence Agency
CIS	Communications and Information Systems
CIT	Commercial Information Technology
CJCS	Chairman, Joint Chiefs of Staff
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
COCOM	Combatant Commander
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CRDA	Cooperative Research and Development Agreement
CTNSP	Center for Technology and National Security Policy
CTTO	Commercial Technology Transition Office
CWID	Coalition Warrior Information Demonstration
DAU	Defense Acquisition University
DDR&E	Director, Defense Research and Engineering
DeVenCI	Defense Venture Catalyst Initiative
DISA	Defense Information Systems Agency
DoD	Department of Defense
DSCA	Defense Security Cooperation Agency
DTIC	Defense Technical Information Center
EMISARS	Early Military Involvement Speeds Acceptance and Results
FAR	Federal Acquisition Regulations
FCS	Future Combat Systems
FFRDC	Federally Funded Research and Development Center
HASC	House Armed Services Committee
IA	Information Assurance
IC	Intelligence Community
ICT	Information and Communications Technology
ICT	Institute for Creative Technologies
IDA	Institute for Defense Analyses
IER	Information Exchange Requirement
INSS	Institute for National Strategic Studies

IO	Information Operations
IPv6	Internet Protocol version 6
IPR	Intellectual Property Rights
IPT	Integrated Process Team
IR&D	Independent Research and Development
IRMC	Information Resources Management College
ISR	Intelligence, Surveillance, Reconnaissance
IST	Information Systems Technology
IT	Information Technology
JCS	Joint Chiefs of Staff
JFCOM	Joint Forces Command
JS	Joint Staff
JTF	Joint Task Force
LSI	Lead System Integrator
M&S	Modeling and Simulation
MCO	Major Combat Operation
MCWL	Marine Corps Warfighting Laboratory
MILSPEC	Military Specification
NATO	North Atlantic Treaty Organization
NCO	Net-Centric Operations
NDU	National Defense University
NEC	Network Enabled Capability
NGA	National Geospatial-Intelligence Agency
NGO	Non-Governmental Organization
NIAG	NATO Industrial Advisory Group
NORTHCOM	Northern Command
NRF	NATO Response Force
ORTA	Office of Research and Technology Applications
OSD	Office of the Secretary of Defense
OTA	Other Transactional Authority
PEO	Program Executive Officer
PM	Program Manager
PPBE	Planning, Programming, Budgeting, Execution
PSYOP	Psychological Operations
R&D	Research and Development
RAI-NC	Rapid Acquisition Initiative–Net Centric
RDEC	Research, Development and Engineering Center
RFP	Request for Proposal
RTO	Research and Technology Organization
S&T	Science and Technology
S&R	Stabilization and Reconstruction
SBIR	Small Business Innovation Research
SE&I	System Engineering and Integration
SOCOM	Special Operations Command
SOS	System-of-Systems

SPAWAR	Space and Naval Warfare Systems Command
SPO	System Program Office
STTR	Small Business Technology Transfer
TARA	Technology Area Review and Assessment
UK	United Kingdom
USA	United States Army
USAF	United States Air Force
USC	University of Southern California
USN	United States Navy
VCJCS	Vice Chairman, Joint Chiefs of Staff
WSIS	World Summit on the Information Society