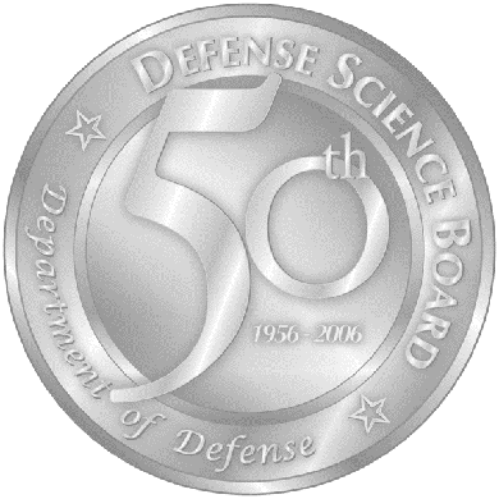
Defense Science Board
2006 Summer Study

on

Information Management for Net-Centric Operations



Volume I
Main Report

April 2007

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

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

The DSB 2006 Summer Study on Information Management for Net-Centric Operations completed its information gathering in August 2006.

This report is UNCLASSIFIED and releasable to the public.

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

DEFENSE SCIENCE
BOARD

28 March 2007

MEMORANDUM FOR: UNDERSECRETARY OF DEFENSE (ACQUISITION, TECHNOLOGY & LOGISTICS)

SUBJECT: Final Report of the Defense Science Board (DSB) 2006 Summer Study on Information Management for Net-Centric Operations (Volume I)

I am pleased to forward Volume I (Classified) of the final report of the Defense Science Board Summer Study on Information Management for Net-Centric Operations. Volume II, the Operations Panel Report, which examined the operational value enabled by information networks, will follow shortly.

This study examined the overall conceptual strategy for information operations and the operational value of proposed information networks. Operational scenarios included prevent and protect the United States against catastrophic attack, conduct large-scale counter-insurgency operations including stabilization and reconstruction, conduct global distributed, small-scale operations including counter-terrorism and humanitarian relief, and enable large-scale operations against near peer adversaries.

Observations revealed that complex distributed, ad hoc operations require new information management and command and control concepts. Further, all scenarios require a new information management capability because of the likeliness that a technically capable adversary will attack US and allied information systems. Findings and recommendations conclude that a combat information capability must be treated as a critical defense weapon system, that information assurance must be resourced and its risk managed accordingly, and that an innovative acquisition strategy is required to leverage true commercial off-the-shelf information technology.

I endorse the Task Force's recommendations and encourage you to forward the report to the Secretary of Defense.

William Schneider, Jr.

Dr. William Schnieder, Jr.
Chairman
Defense Science Board

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

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Report of the Defense Science Board 2006 Summer Study on Information Management for Net-Centric Operations

This Defense Science Board report recommends a new information management approach and combat information capability to respond to current and likely future national security challenges—challenges that require U.S. force to rely increasingly on information, more so than in the past.

For the past five years, the office of the Assistant Secretary of Defense for Networks and Information Integration and the Department of Defense Chief Information Officer have been assembling an underlying framework and architecture based on commercial Internet Protocol technology to address the increased information needs of today's military operations. This enterprise has the potential to bring significant information capability and operational value to users and decision makers at all levels within in the department.

This summer study addressed combat operations, information management, information assurance, and architecture requirements, as well as the architecture framework currently being pursued by the department. The study examined the overall conceptual strategy for the system and the operational value of the proposed information network. Additionally, the task force assessed cost/risk trades and technical network issues such as bandwidth, quality of service, availability, security, integrity for all missions and users, and knowledge management—all of which support the distribution of knowledge that will ultimately support effective decision making These considerations converged on the simple question of how to provide robust, useful information at all levels—from decision-makers to tactical users.

The findings and recommendations of this study can be distilled to three points

1. the combat information capability must be treated as a critical defense weapon system
2. information assurance must be resourced and its risk managed accordingly
3. an innovative acquisition strategy is required to leverage true commercial off-the-shelf information technology.

The members of the study are greatly appreciative of the important contributions of the government advisors; LTC Scott Dolgoff and Mr. Andrew Chappell, DSB Office representatives; Executive Secretary, Mr. John Mills; and the staff.

Mr. Vince Vitto
Co-Chair

Dr. Ronald Kerber
Co-Chair

Table of Contents

Executive Summary

United States national security challenges are much different than they were just a few decades ago. Besides having a much wider spectrum of characteristics and capabilities, potential adversaries have clearly changed and complicated the rules of military engagement to support U.S. security objectives. In "traditional" eras, the adversary was well-defined by lines of battle and clear means of identification. Today's military operating environment is far more complex: the adversary is dispersed, often mixed with civilians and other non-combatants; and targets are located in areas where there is great concern over collateral damage. Adversaries are adaptive, amorphous, and stealthy, and often do not have high-value targets that can be attacked. The adversaries' stealth enables them to neutralize the formidable U.S. operational advantages in more traditional warfare, thus making the U.S. reliance on information more pronounced than in past eras.

Over the past five years, the office of the Assistant Secretary of Defense for Networks and Information Integration (ASD [NII]) and Department of Defense (DOD) Chief Information Officer (CIO) have been assembling an underlying framework and architecture based on commercial Internet Protocol technology to address the increased information needs of today's military operations. This enterprise has the potential to bring the department, at all levels, significant information capability and operational value, and is a valuable defense weapon system. However, the reliance on commercial technology also increases the chances for U.S. adversaries to compromise the enterprise. In response to these challenges, the Defense Science Board was asked to assess the department's strategy, scope, and progress toward achieving a robust and adaptive net-centric DOD information management system.[1] Specifically, the task force spent time evaluating the current framework, architecture, processes, and organizational structures being

1. The terms of reference for this study are attached as Appendix A.

pursued to deliver the power of information networks to the DOD enterprise, as well as to external partners.

The task force addressed combat operations, information management, information assurance, and architecture requirements, as well as the architecture framework currently being pursued by the department. The task force examined the overall conceptual strategy for the system and the operational value of the proposed information network. Additionally, the task force assessed cost/risk trades and technical network issues such as bandwidth, quality of service, availability, security, integrity for all missions and users, and knowledge management—all of which support the distribution of knowledge that will ultimately support the missions and users in making effective decisions.

These considerations converged on the simple question of how to provide robust, useful information at all levels—from decision-makers to tactical users. The task force focused on support of combat operations, as it was felt to be the most stressing application of the system, as opposed to, for example, business processes and administration. However, it was recognized that all these applications are intertwined and must be operated as a whole. The task force did not examine the protection of the nation's total information network. Although critically important, it was deemed outside the scope of this study.

To set the context of the study, the task force addressed four operational scenarios:

1. Prevent and protect the United States against catastrophic attack.
2. Conduct large-scale counter-insurgency operations, including stabilization and reconstruction.
3. Conduct global distributed, small-scale operations, including counter-terrorism and humanitarian relief (such as Hurricane Katrina).
4. Enable large-scale operations against near peer adversaries.

The task force determined that all these scenarios require a new information management approach and combat information capability for the DOD, largely based on commercial information technology. However, adversaries can access similar capabilities from global commercial vendors. An adversary need not be large in size to capitalize on this capability. In fact, a technically capable adversary can realize a significant military or political advantage by disrupting the information technology supporting U.S. operations—whether or not the United States happens to be directly confronting that particular adversary.

To address this new information management approach and combat information capability, the task force focused on four major themes. Each theme is summarized here and then described in detail in subsequent chapters of this report.

Net-Centric Operations and Robust Information Management Enable Better Decision Making

The task force organized a number of panels of military operators (O-6 level and below) to identify information management needs and how information was managed to execute missions in Iraq and Afghanistan. It became quite clear from these discussions that the United States has considerable deficiencies in its ability to manage information to command and control units in the field.

In the experiences described by the operators, interoperability was poor, and there was significant *ad hoc* activity taking place at the unit level—*especially* at the lowest war fighting echelons. To counter interoperability, U.S. soldiers and Marines developed many systems and processes to move information from one "stove pipe" to another. This included use of personal cell phones sent by family members, chat rooms, web searches, *ad hoc* networks—any solution to get needed information to conduct operations and support commanders. Finally, it was noted that much of the acquired military capability to support these conflicts has been on supplemental funding and is not part of the "planned" system putting into question the long-term viability of these activities.

This *ad hoc* approach also applied during the rotation of units in the field. The task force found that, as operators entered the theater they basically "started from scratch." Personal, trusted, and comfortable relationships back in the continental United States ("reach-back") were reestablished. There was ineffective systematic transfer of databases from units exiting in the theater to the inbound units, leading to significant information disconnects as units rotated in-and-out of theater. The inbound unit could not fully exploit the work done by the previous unit. An effective method is still needed for organizing all this information and data, assuring it, and then making it available to the commander to enable intelligent and robust decisions.

Methods for information organization, retrieval, and display are required to enable commanders and soldiers to accurately perceive and understand the information presented to them. Improving a commander's access to, and understanding of, the information, combined with the ability to collaborate effectively with others, will inevitably lead to better military decision-making.

The task force proposes a combat information management architecture to support the Combat Information Capability (CIC). Three staff functions comprise this architecture:

1. **Combat information specialists**. At-the-ready for the soldier or right beside the commander to answer questions, to anticipate needs, and to assemble and present data.

2. **Knowledge managers**. A reach-back capability for the combat information specialist for information, data, and knowledge in a specific area.

3. **Subject matter experts**. Span a full range of topics and subjects and are the source of in-depth information of a particular subject from which a knowledge base can be assembled and continuously supported.

In addition to the staff functions described above, commanders need to understand, command, control, and operate information management systems at the operational level. Plans to monitor and protect the system, and respond to adversary actions (such as intrusion

or attack), need to be developed. Therefore, the services need to organize, train, and equip information management personnel to develop technological and procedural capability and participate in operational force exercises. Combatant commanders also need planning staff expertise to develop combat information planning annexes to go forward with this system and capability.

Intelligent management of information—whether in the military or civilian sectors—is no longer a choice; it is essential just to keep pace with the competition. Today, several industrial and commercial companies have been very successful at developing this type of organization and management structure, beginning with a lead individual (who also has business accountability) for a wide range of commercial applications and markets. In fact, the very livelihood of companies like large management consulting firms depends on being extremely proficient at this kind of knowledge and information management. The architecture described above basically adapts and institutionalizes best commercial practices to the military.

There are *many* opportunities to improve the current, distributed information management operations in the field. Today's complex distributed, *ad hoc* operations require a new Combat Information Capability to include:

- information management services for tactical users
- dynamic management of distributed intelligence
- intelligence, surveillance, and reconnaissance assets
- appropriate and necessary information assurance and security
- operations with degraded networks
- operations with coalition partners, non-government organizations, other agencies, and state and local governments.

Each of these requirements are touched on in the remaining themes and described in greater detail in the chapters of this report.

Information Dissemination and Management Relies on Global, Interoperable Commercial Information Technology

The information network architecture being developed for the Global Information Grid is based on an Internet-like model with the goal of separating transport from applications. The architecture is supported by a set of net-centric enterprise services, with databases with well-defined ownership and maintenance distributed throughout the network. Implicit in this architecture is: (i) a robust core at the transport level; (ii) a useful set of services; and (iii) a robust set of ever-increasing applications, as communities of interest are organized to define those applications. The services and other users must develop key applications, but in a manner that decouples the applications from the individual databases.

The task force was briefed on a number of the programs: Global Information Grid Bandwidth Expansion, Transformational Satellite Communication, Joint Tactical Radio System (JTRS). It was not the intention or the purpose of this task force to focus on the schedule, acquisition strategy, or technological issues associated with each of these programs. The task force however did consider two programs very important to information management and assurance. They are Net-Centric Enterprise Services (NCES) and High Assurance Internet Protocol Encryption (HAIPE).

Overall performance of the system can only be assured by developing a comprehensive model of the system, and testing additions and modifications with a systems engineering approach. Such an approach requires high-level analysis, as well as detailed systems modeling, to guide evolution of the system. The implications of programmatic and configuration changes within the overall system must be assessed, as well as information assurance weaknesses. The objective of this approach is to develop and monitor performance metrics, and to develop the capability to test the systems and applications for compliance with performance objectives.

Finally, end-to-end testing and technical control are imperative to stress the network for technical and operational parameters, as well as to understand and measure the formal risk management processes trading performance versus assurance. This system is being built predominantly with commercially available information technology, so new information assurance vulnerabilities are introduced as new capabilities are added.

The DOD does not have adequate resources within the offices of the ASD (NII), CIO, the Defense Information Services Agency (DISA), or the Under Secretary of Defense for Acquisition, Technology and Logistics (USD [AT&L]) to perform comprehensive systems analysis and engineering. While the task force believes the workforce should be improved, it was struck by the paucity of involvement of commercial experts in this needed systems analysis area. The task force believes experts from commercial industry be brought in (perhaps on short-term Intergovernmental Personnel Act tours) to assist the acquisition and systems engineering processes, and to identify commercial activities that could be brought to bear on the DOD enterprise.

As the task force surveyed the entire enterprise architecture and assessed the proliferation of commercial information technology, it was recognized that, although much focus has been placed on commercial-off-the-shelf (COTS) technology, it often means "enhanced COTS" or "value-added COTS"—that is COTS technology that has been modified by a large systems integrator. The DOD is already buying routers, switches, blade servers, and software directly from the General Services Administration catalog. So, a great deal of the information technology already in this system is true commercial information technology—in fact, the department is encouraging commercial instantiations of new information management and assurance approaches (e.g., HAIPE and NCES). However, the department currently uses the Joint Capabilities Integration and Development System (JCIDS) process that is designed for large-scale, requirements-driven acquisitions—a process that leads to "enhanced COTS" or "value-added COTS." A capability-driven approach is needed to develop and inject information technology components into the information enterprise.

Although the discussion above defined a Global Information Grid (GIG) core network supported and protected by HAIPE security devices, at the edge of the core are many tactical networks that can assume many forms, e.g., coalition, special operations, Army, Marines. To accommodate the information needs of the tactical user, the edge networks must support a minimum standard interface back into the GIG core. Since the users and operators in the edge networks are the ones who identify the information needed to carry out their mission; they should be able to pull that information from the databases within the system, using the common services provided by NCES.

The central problem identified by the task force is that the information needs of tactical users and edge networks are not being adequately addressed. The current focus is on communications—not on information management needs. Combat decision support tools are needed to provide reach-back, combat information, and database management. Commander's expectations must be managed within these tactical networks.

In addition, tactical communications devices being developed within the JTRS and other Service programs will not allow tactical users to keep up with the revolution in commercial wireless technology. Unique approaches are required to provide tactical users with inexpensive information management devices.

Commercial Information Technology Architecture Presents Critical Information Assurance Challenges

Information assurance is an enormously important issue: information assurance enables mission assurance. Information assurance is typically treated as if it were a network security and confidentiality matter. Yet it actually entails several additional issues, including integrity of the system, availability, quality of service, authentication, and attribution.

With the addition of each new module of capability, a degree of vulnerability is added. The clear need is for a formal risk management process that considers obvious benefits of net-centric operations along with the information assurance threats that are not as intuitive.

A formal risk management process needs to be embedded in the systems engineering and analysis processes, to assess the benefits of added applications against the impact of the introduced information assurance threats. There are many other potential threats in DOD networks, including offshore development of hardware and software. The information network is inherently vulnerable, and it needs to be designed and operated with the understanding that it is or can be attacked and/or compromised.

Use of a COTS-based information network is critical to keep the system capabilities close to those that are commercially available. *Yet, this is the first major U.S. defense system that is built on commercial, globally available technology.* This strategy therefore inherently raises the risk that adversaries can also exploit commercial technology. It also means that the system is more difficult to protect, especially as additional capabilities are added. COTS on the scale proposed will enable a system more robust than anything an adversary will likely assemble, but use of COTS is inescapably a double-edged sword from the I information assurance A perspective, because the high speed of COTS implementation may outpace the ability to maintain integrity and control of the system itself. This is why the provenance of the hardware and software being inserted into this system must be carefully monitored. Globalization and off-shore development greatly increases this threat. A three-prong strategy is needed for dealing with information assurance matters: an offense component, a deterrence and dissuasion component, and a defense-in-depth component.

"Combat Information Capability" is a Critical Defense Weapon System

At the start of this study, members thought the task force would focus on information management issues, the GIG, and a myriad of other technical issues, but as briefings were received from users, operators, and experts, concepts and thinking about this subject transformed. This system will touch and manage all DOD information resources, especially those in time-critical battle situations, and it needs to be treated at a critical defense weapon system. As a weapon system it

must be protected and operated in a manner consistent with its mission of protecting and defending the United States.

A critical defense weapon system requires enterprise-wide operational management, performance monitoring, and contingency planning functions. Operators must know how to operate the combat weapon system, and readiness assessments, throughput and performance, and trades and metrics to measure both performance and assurance must be available. Many defense assets will be connected via this system and system services must be prioritized and tested, and war fighters must train with the system.

The system will likely always be operated in a degraded mode and the assumption should be that adversaries are constantly attacking it. As a defense weapon system, doctrine; concepts of operations; tactics, techniques, and procedures; and contingency plans must be developed to address these threats. The system must be exercised regularly—with employment of deception—so U.S. commanders understand how to operate in degraded modes. Calibrated red and blue teams can be used to help with scenarios and develop exercises that are realistic. Commanders must be provided the necessary network status information to make risk-managed decisions about the mode of operation—such as available capacity or estimated extent of penetration.

A system test environment is needed for enhancements, assurance modifications, and new commercial capabilities to be tested before being inserted into the real system. In such an environment, red team attackers and blue team defenders can exercise solutions or offerings and improve skills without impeding actual operations. Ideally there should be several test range options, ranging from virtual (rapid simulation of applications and capabilities being considered for incorporation into the network system), to simulation (table top experiments), to live exercises (calibrated red/blue teams to introduce real-world system characteristics). Ultimately, live field exercises should be conducted to understand how to manage and protect the system realistically and effectively.

Recommendations

The task force proposes the following recommendations that cut across the four themes identified above, to develop the necessary strategies, policies, training, and countermeasures to use, protect, and manage this defense weapon system.

1. The Department needs to recognize information capabilities as a combat system.

- Deputy Secretary of Defense should create and resource a Combat Information Capability
- United States Strategic Command (STRATCOM) must improve net-centric operations:
  - Joint Task Force Global Network Operations center must be improved to a world-class enterprise management capability.
  - Performance and readiness metrics must be developed.
  - Network management standards must be enforced across the enterprise.
  - Robust and redundant capabilities and operational procedures for information assurance must be developed.
- STRATCOM must establish a robust GIG test environment to examine the trades among performance, information assurance, and cost:
  - DOD CIO: Identify and prioritize emerging information technology and information assurance capabilities for testing.
  - U.S. Joint Forces Command (JFCOM): Create net-centric operations and information assurance learning and training experiences.
  - Combatant commanders: Conduct operational readiness exercises and tests.
  - STRATCOM, National Security Agency, and DISA: Validate and exercise a risk management system.

- STRATCOM and JFCOM: Identify resource requirements.

- Chairman, Joint Chiefs of Staff must develop a Combat Information Capability Strategic Plan

2. *Combat Information Capability requires a new approach to information management.*

- Deputy Secretary of Defense should direct DOD CIO to ensure the formation of communities of interest. These communities should be aggregated into capability portfolios to rationalize vocabularies and harmonize services and value-added services.

- Deputy Secretary of Defense should direct DOD CIO to ensure DOD process owners encourage creation of an information marketplace to include:

  - Delivering value-added services.

  - Developing resource incentives for making data visible and promoting information sharing.

  - Developing processes to ensure information quality.

- Deputy Secretary of Defense should direct the services to create and resource combat information positions to include:

  - Combat information support staff, combat information specialist, as well as knowledge managers and subject matter experts.

  - Provide commanders at 3- and 4-star level with combat information integration officers on their personal staffs.

3. *Create an enterprise-wide, robust information assurance strategy.*

- ASD (NII) should evaluate the information assurance funding over the Future Years Defense Program, focus on information assurance for the entire enterprise, and increase current funding where appropriate.

- DOD CIO and ASD (NII) should establish responsibilities and authorities for overall enterprise governance.
- DOD CIO and ASD (NII) should develop a robust systems engineering and risk management capability.
- ASD (NII) and USD (AT&L) should establish a defense-wide program to design, build, and operate an isolated network to improve GIG information assurance capabilities.
- DOD CIO, ASD (NII), and USD (AT&L) must establish plans, policies, and procedures for acquisition of COTS information technology systems from an information assurance perspective.
- USD (AT&L) and ASD (NII) must address critical programmatic issues with NCES and HAIPE.
- STRATCOM and JFCOM should devise an information assurance battle management doctrine, and tactics, techniques, and procedures.

4. Combat Information Capability must support tactical communications and leverage COTS information technology.

- USD (AT&L), DOD CIO, and ASD (NII) should support the tactical users at the edge of the core by:
  - Delivering robust, easily formed, meshed tactical networks that leverage commercial technologies.
  - Delivering information that adapts to tactical users display and bandwidth.
  - Implementing robust content staging to provide information caching forward to enable timely access.
  - Encouraging the production of future commercial capabilities that meet the department's needs.
  - Acquiring end-user devices as commodities, through the General Services Administration Schedule.

- Chairman, Joint Chiefs of Staff and USD (AT&L), should revise JCIDS and acquisition system policies to encourage rapid information technology procurement and to:
  - Exploit opportunity to purchase COTS information technology, which will require spiral acquisition processes.
  - Assure COTS systems remain true COTS with plug and play interfaces.

The bottom line: this Combat Information Capability must be treated as a critical defense weapon system, information assurance must be resourced and risk-managed accordingly, and an innovative acquisition strategy is required to leverage true COTS information technology.

Chapter 1. Introduction

The military's ever increasing reliance on information networks and its ability to provide wider access to information to support collaboration has transformed and improved the forces' capabilities and effectiveness in executing operations. Future challenges and the need to maintain adequate levels of security, integrity, and reliability will place new demands on information networks, processes, and personnel. The Defense Science Board was asked to assess the department's strategy, scope, and progress toward achieving a robust and adaptive net-centric information management capability for the Department of Defense (DOD).

It is well accepted that improved information at all levels will improve operational effectiveness, but, of course, that comes with some risk and penalties. The task force was asked to examine the operational value of the proposed information network and to pay special attention to the emerging missions it is designed to support—that is, counterinsurgency, counterterrorism, stabilization and reconstruction, response to catastrophic disasters, and defense of the nation against attack.

Over the past five years the Assistant Secretary of Defense for Networks and Information Integration (ASD [NII]) and Chief Information Officer (CIO) organizations within DOD have done a significant and remarkable job assembling an underlying framework and architecture based on commercial Internet Protocol (IP) technology, which has the potential to bring the department, at all levels of the enterprise, significant information capability and operational value. The task force was charged with evaluating the framework, architecture, processes, and organizational structures being pursued to deliver the power of information networks to the DOD enterprise, as well as to external partners.

Risks are associated with execution of programs to implement the network, as well as with meeting quality of service, availability, security, and integrity expectations for all missions and users. The task force was to assess cost/risk trades and technical network issues associated with the enterprise.

Lastly, the task force considered knowledge management in support of department goals. "Googling" for access to particular information is now a familiar activity, but it is not the appropriate application for the war fighter in the tactical battlefield who is seeking information in the middle of a firefight. Therefore, identifying effective methods to provide robust, useful information at all levels—from strategic decision-makers to the tactical user—was a major focus of this study. The focus would be on information discovery, sharing, collaboration, visualization, comprehension, and storage—all of which support the distribution of knowledge that will ultimately support the missions and users in making effective decisions.

The following operational scenarios derived from the threat assessment prepared for the most recent Quadrennial Defense Review were the basis for the task force:

- prevent and protect the United States against catastrophic attack
- conduct large-scale counter-insurgency operations including stabilization and reconstruction
- conduct global distributed, small-scale operations including counter-terrorism and humanitarian relief
- enable large-scale operations against near peer adversaries

As depicted in figure 1, these scenarios today have a very different battle management paradigm with a stealthy enemy dispersed in a civilian urban setting, as opposed to clearly defined, uniformed combatants and battle lines for engagement as in previous wars.

Under all scenarios a sophisticated and "state of the art" information management capability is required.

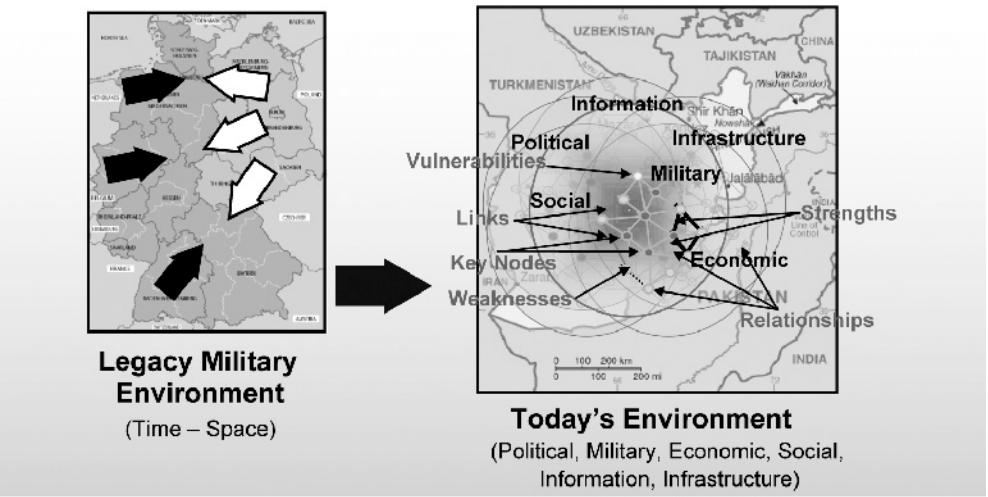


Figure 1. Evolving Threat Drives Need for New Combat Information Capability

Information systems technology has proliferated across the globe, driven primarily by the global economy and the Internet. The United States no longer holds a significant advantage in information systems technology. Today, more hardware and software is being built offshore than in the U.S., and that percentage continues to grow rapidly. Potential adversaries are technically very capable and are able to move information rapidly. Adversaries also clearly understand the importance of information to winning in combat and will therefore commit themselves to attacking U.S. command and control, communications, and information systems. These attacks may be kinetic attacks and/or non-kinetic attacks. The threat to the information system will continue to evolve as globalization and the information revolution force changes in structure and technology.

In our lifetimes, the information revolution has moved the world from a place where data can be moved at about 30 words per minute over field phones and 60 words per minute over radios to one in which it can be moved at roughly 1.5 *trillion* words per minute over wideband data links. At the same time, data acquisition through means such as satellites and data storage capabilities has increased at a similar rate. The impact of this revolution on information management capability on the national security environment is enormous. It would be especially detrimental if

there is not a U.S. national and DOD commitment to keep pace with almost "speed of light" advancements in information technology.

Globalization has radically changed the national security paradigm. Movement has been from a relatively isolated environment of the Industrial Age of the 20th century, where security meant "defense" and "containment," to the information age of the 21st century, a much more integrated environment with a smaller world (due to speed of light transmissions) where information is shared globally in very near real time, and national security is more complex and dynamic. Maintaining "national security" is no longer just a matter of protecting international borders. For example, "borders" in cyberspace must also be protected.

At the same time, there are more active global hotspots; the threat is increasingly using asymmetric tactics; and interoperability is still an issue with U.S. forces, as well as with many of U.S. coalition partners. The evolving threat characteristics considered during the course of the study include:

- dynamic and ever changing
- highly mobile and regularly move across international borders
- highly distributed
- stealthy
- adaptive and amorphous
- asymmetric
- when viewed in isolation—low value targets

Adversaries have become very skilled at neutralizing U.S. operational advantages. Two critical concerns evolved during the study:

1. U.S. adversaries are not only using their many skills in information technology to move information rapidly, but also they may develop a significant capability to attack U.S. information systems.

2. Commercial-off-the-shelf (COTS) information technology production—both hardware and software—is moving to Asia.

The implication of this trend on national security is alarming.

It should be noted that since Operation Desert Storm, the United States has reduced the size of its war fighting forces by 300 ships, 12 air wings, and 6 divisions. With a modernization budget that has essentially remained level and/or declined, the department has invested heavily in information technology; networks; precision; command, control, and communications; computers; and intelligence, surveillance, and reconnaissance (ISR). Essentially, the United States is engaging in a fundamental trade of massed forces for massed electrons. This trend has focused toward a capability to more precisely and surgically attack smaller units down to a single terrorist.

During its deliberations, the task force identified four major themes:

- Better military decision making (all echelons, all missions) is enabled by net-centric operations and robust information management.
- Information dissemination and management relies on global, interoperable commercial information technology.
- Commercial information technology architecture presents critical information assurance challenges.
- Field and operate a Combat Information Capability as a critical defense weapon system.

The findings and recommendations in this report are formulated around these themes.

While many of the implications of this task force's findings would also apply to, for example, management of administrative or financial systems within the DOD, the task force chose to build this study around the last theme because the combat environment is the most *stressing* application.

The task force defined a Combat Information Capability (CIC) as the ability to manage information and information sources to support commanders at all levels in any type of confrontation with an adversary to deliver the best data *to the last tactical mile*. This capability is built on a foundation that includes all the services on the Global Information Grid (GIG), information assets, databases, capabilities to manage information, and the ability to protect the GIG and its assets. These assets are brought together with real-time information, such as ISR data gathered from all sources. *This Combat Information Capability is an integration of assets, capabilities, applications, and databases that all work together to enable timely smart decisions in the field.*

Due to the enormous scope of this subject, the task force had to exclude many important subjects from consideration. While the members recognize that many "outside" networks are attached to the DOD infrastructure, this task force chose not to undertake the impact of an attack on national infrastructures outside the DOD networks. However, there must be protections on information that enters the DOD system from those outside networks.

The Bottom Line

As the task force evolved, it became clear that, given the way this system is to be fielded, *the Combat Information Capability must be treated as a critical defense weapon system* that will provide a great deal of capability to the United States. With this realization, a different mindset is required on how the system is used, managed, and protected.

The evolving national security scenarios demand increasingly distributed and dynamic operations. The network/COTS approach and strategy certainly enable new paradigms for sharing and using information. However, this capability also has the potential to significantly *increase* vulnerabilities to internal and external threats. It becomes a very attractive target for U.S. adversaries.

Therefore, the task force believes that the system and its capabilities have the potential to be under attack and, as a result, commanders must be prepared to operate in either a degraded or compromised mode.

Commanders need to understand this potential and be trained to operate under this scenario.

A major implication of the network/COTS approach is that DOD needs a new, innovative acquisition strategy so that full advantage can be taken of the capabilities of a true COTS system.

The task force's findings and recommendations can be distilled to three points, which will be repeatedly visited in the following chapters of this report:

- **DOD Combat Information Capability must be treated as a critical defense weapon system.**
- **Information assurance for this critical capability is critical and must be resourced and risk-managed accordingly.**
- **An innovative acquisition strategy is required to leverage true COTS information technology.**

Chapter 2. Net-Centric Operations and Robust Information Management

The Problem

The focus of most combat operations in the past several years has been overwhelmingly in the land domain. The distinguishing characteristic of this domain, with some exceptions, is its people-centric nature. This is distinct from the platform-centric nature of other domains or even more traditional conventional land combat warfare. The recent experiences of war fighters in the tactical environment, employing the currently fielded net-centric capabilities, provides the department a critical opportunity to validate the theory and promise of information management and networks at the tactical level. The power of information and accurate battlefield situational awareness is as old as conflict and warfare itself. The distinguishing difference between now and all of history is the explosion of information management and communication technology in this information age.

This rapidly developing technology presents many different challenges than our most recent differentiating defense technologies (nuclear weapons, submarines, fighter aircraft, stealth, and precision weapons), and, most importantly, is in the commercial sector. The fact that most of the technology is globally and commercially available means that U.S. adversaries can exploit it as rapidly as the United States can. This in fact implies that it would be very risky for the United States not to exploit the technology as rapidly and as prudently as possible. The validation of the network-centric operations (NCO) thrust of current DOD activities should also include a serious look at the risks, vulnerabilities, and challenges introduced by using this technology.

War fighters are singularly focused on capabilities that help them achieve their assigned missions. Sophisticated information capabilities introduced in the past several years have made a significant impact on the tactical battlefield. On the positive side the ability to share, communicate, and collaborate using vast amounts of information is changing the way

some commanders organize forces for combat. On the negative side is the continuous *ad-hoc* nature to tactical networking solutions. In some cases, the solutions to capability shortfalls are solved by adapting commercial capabilities outside programs of record. In other cases it is adapting programs of record through the use of civilian networking concepts like web chat.

The task force heard from four panels of operators at the 06 level and below who had just returned from Afghanistan and Iraq. Their observations varied according to their particular experiences but several themes can be easily summarized to a few critical issues. Information management was the war fighter's principal concern. Finding the needed information effectively and in a timely manner was very difficult for the tactical commander and staff. The information management challenge at the tactical level was couched in very practical terms: the war fighters want information management concepts that support, not restrict, concepts of operation. Commanders want improved access to ISR data and tasking plans at the tactical level. In some cases, this access is desirable without value-added analysis; in other cases intelligence processing is helpful as long as it is timely. Establishing information sharing and collaboration seamlessly for voice, data, and video without regard to organizational echelon is the desired end-state.

Deriving Major Information Needs from Operational Scenarios

The four operational scenarios developed during the Quadrennial Defense Review were examined to comprehend the major information needs for combat or crisis management operations.

When the four operational scenarios are examined in detail, certain major information requirements become clear for each scenario. These information requirements include data, communication and collaboration capabilities, and tools that would facilitate success in each of the respective scenarios. These needs are by no means exhaustive, but the ones listed below and shown in figure 2 are illustrative for the respective scenarios and they provide a good sense of the types of information required for today's security challenges.

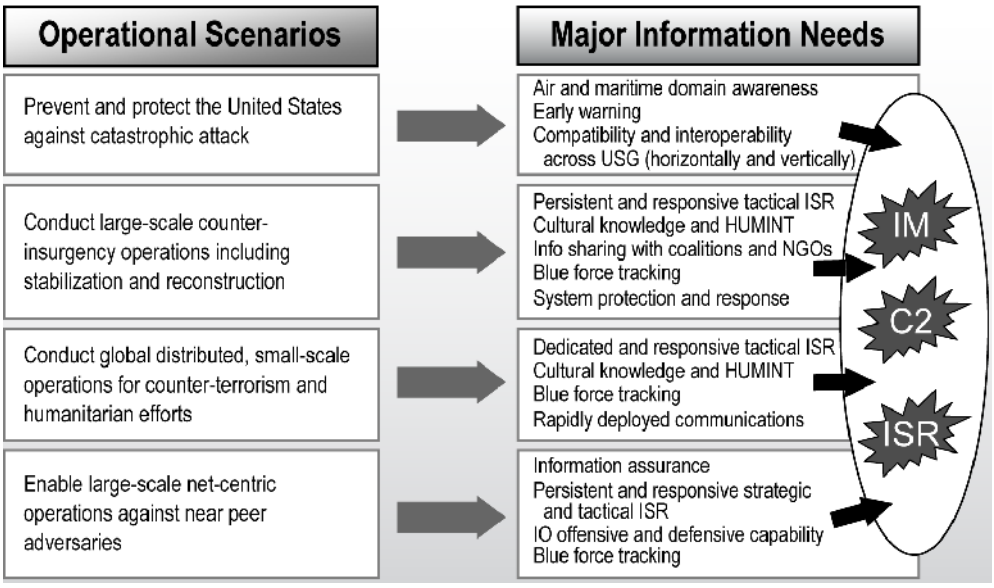


Figure 2. Assessing Combat Information

The examination of figure 2 shows that even with significant commonality across the scenarios, the major information requirements have some distinct needs for each operational scenario. Nonetheless, three major areas emerge as central throughout all scenarios:

1. Information management (IM)
2. Combat Information Capability command and control (C2)
3. Intelligence, surveillance, and reconnaissance

Moreover, information management, command and control, and ISR—taken as a whole—combine to form what the task force termed a "Combat Information Capability," a term that will be defined and developed in the subsequent discussion. There are significant capability shortfalls in these areas that need to be addressed. These gaps will also be discussed below.

Operational Gaps

Recent operations have re-enforced the endemic challenges of providing the right information at the right time in the right form. The ability of commanders to organize and manage information and related resources was limited by a host of complex interrelated issues. The most common refrain was visibility, access, and flexibility. In general, there is a significant gap in the ability to manage combat information, which includes the process of identifying, collecting, organizing, making available, assuring quality and authenticity, and protecting information, for operational use. Emerging information management techniques will provide essential mission functionality for the user to discover data and services, to understand and use information, and to collaborate with other users.

The second category is in the area of command and control within the scope of activities generally associated with information collection and management. Commanders at all levels recognize the necessity to understand the critical capabilities necessary for mission success. Many of the war fighters realize that "control" of assets is not the crucial issue. The challenge is a fundamental lack of ability to see, understand, and influence critical issues such as bandwidth, ISR management, and information sharing with coalition partners.

The third major area of concern from the tactical war fighters was the inability to access or fuse ISR data. The ISR data being referred to most often was in the form of imagery intelligence but would include the full range of sensor outputs to include human intelligence (HUMINT) reporting.

The often repeated statement "every soldier is a sensor" is meaningless unless the flow is two way and accounts for the nature of the environment in which the information is useful. Data collected at and for the ground tactical level (complex physical and human terrain) is by its nature incredibly cluttered. The nature of operations in this environment (ambiguity, time sensitivity and constraints, mobility) means that the sensors generally tell a commander less and less precisely than for example when compared to platform-centric environments.

Current State: Myriad of *Ad Hoc* Personal Connections

Information management is the process of identifying, collecting, organizing, making available, assuring quality, and protecting information for operational use. Information management provides essential mission functionality for the user to discover data and services, understand and use information, and collaborate with other users. This task force focused on the use of information management in support of military operations and combat information management, which is believed to be the most stressing application of the DOD information management strategy. The task force did not directly examine DOD business or administrative systems; however, some of the principles identified in this task force directly apply to those applications, e.g., true COTS and streamlining the acquisition process.

Unfortunately, current military operators are not enabled with a robust and world class combat information management system. Currently, combat information support is provided by a myriad of *ad hoc* personal connections that are established each time units rotate into theater, only to be broken when they rotate out. The scenario depicted in figure 3 shows a typical unit's *ad hoc* reach-back approach to comfortable and familiar sources.

Combat information management promises a number of benefits of including:

- More responsive and informed decision making—owing to more rapid and wider information sharing and enhanced presentation. This can provide forces with greater flexibility to adapt to unanticipated circumstances.
- Improved situational awareness—drawing on wider information sources and shared understanding (such as Command Post of the Future[2]).

---

2. http://www.isx.com/projects/cpof.php

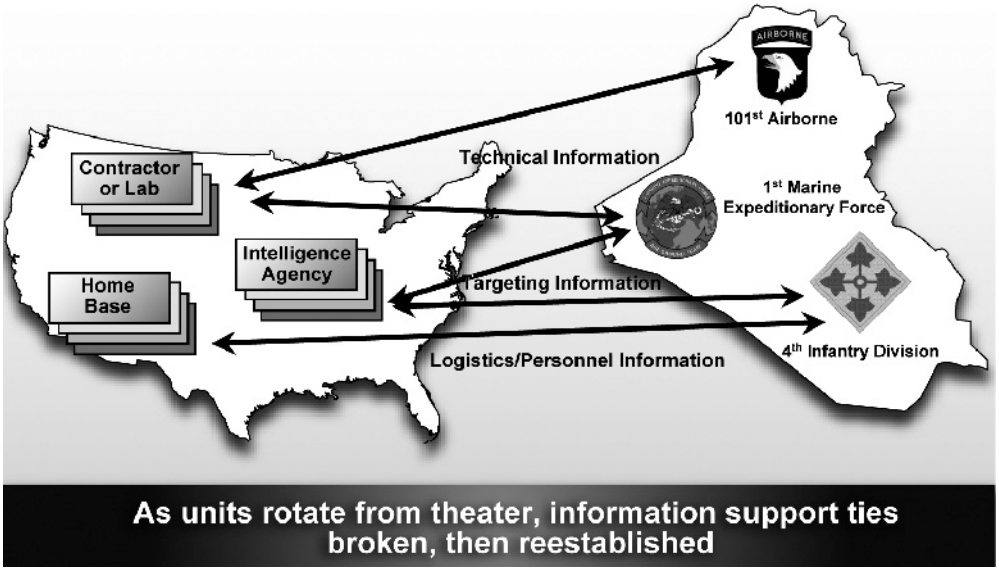


Figure 3. Current Status—Myriad *Ad Hoc* Personal Connections for Information Management Support

- Enhanced and timelier planning—resulting from greater collaboration and increased parallel activity. This can include the ability to operate with a smaller footprint forward as illustrated in the forward Air Operations Center in Joint Expeditionary Force Experiments.
- Improved synchronization in mission execution—resulting from increased coordination among distributed forces that can result in more rapid and effective operations and lower fratricide.

The Solution: A Combat Information Capability

The Combat Information Capability can best be described by referring to figure 4. The foundation is the Global Information Grid extended to the High Assurance Internet Protocol Encryptor (HAIPE) including information assurance elements of the Net. This design provides wideband capability with robust defenses. The elements involved in protecting and assuring the net assume that adversaries will attempt to deny this important capability. The information assets refer to data that are generally stored in data bases and sources available to the

war fighter. Sensor data, track data, and analysis of information would fit into this characterization.

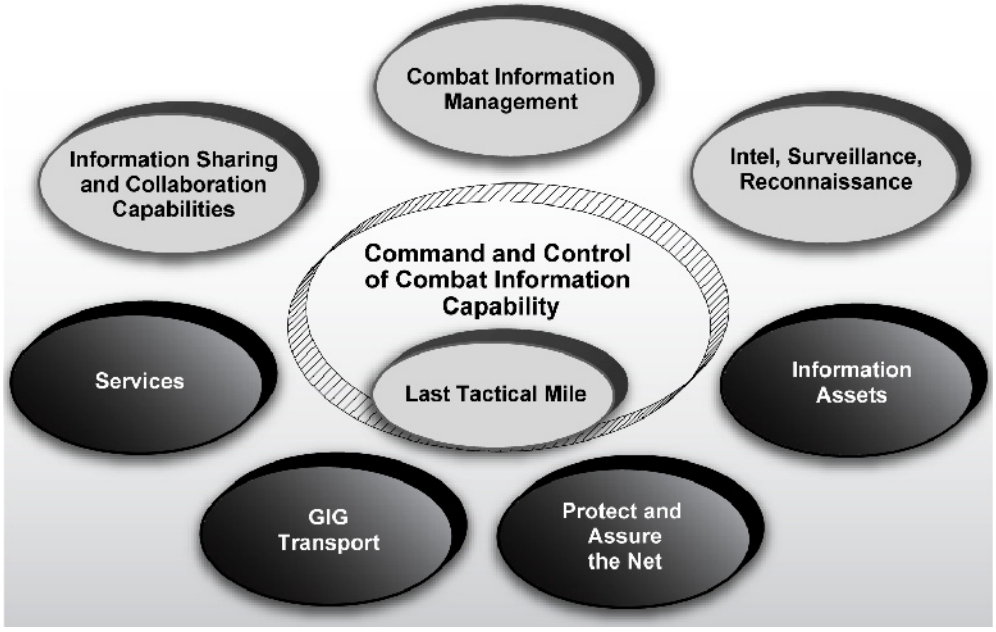


Figure 4. The Combat Information Capability

Services are the tools that permit discovery and exploitation of data, applications, displays, and persistent collaboration capability to satisfy combat information needs. These four elements are part of the CIC. Depending on the scenario, the GIG, the information assets, the services and protect/assure parts of the foundation can be separated from the normal business of the department to attain a higher priority, greater assurance and security, and more secure data bases and services by parsing.

The gray areas in figure 4 are focused on the operational and tactical level of operations and the recommendations to improve capabilities over the last tactical mile. The "last tactical mile," which generally lies outside the secure HAIPE protected core of the network, may have limited communications bandwidth, has unique security and assurance requirements and challenges, and warrants particular focus in this study.

The necessary requirements to support the "disadvantaged" war fighter are outlined later.

Combat information management refers to the process and structure to provide commanders and individual war fighters with educated and trained assistants and tools to understand and support combat information requirements. An information sharing and collaboration capability refers to the tools and communications that provide commanders and staffs the ability to share information dynamically and to collaborate for planning and execution. Command Post of the Future capabilities in Iraq are an excellent illustration of the value of collaboration. The ISR element refers to the ability to treat operational and tactical ISR assets as an integrated ISR "system" to obtain the most effective, responsive coverage from available assets. The data flowing from ISR assets may be made available simultaneously to the user and to the analyst.

To achieve maximum combat effectiveness, the commander must be able to control this war fighting capability as is done with other essential elements of combat power. The task force defined the needs that permit the commander to exercise command and control.

Taken together, these seven elements comprise a CIC.

Organizing Data for Robust Decisions

Command centers at both the strategic and operational levels, as well as tactical joint force elements, must have a common understanding of the location and identification of all battle space entities (that is, people, air vehicles, ground vehicles, ships, subsurface vehicles, space vehicles, buildings, bridges, and critical infrastructure components, for example). This information comes from a variety of sources, many of which are represented in the ovals on the left side of the figure 5. Under the concept of a net-centric force, it is envisioned that these sources will be networked and integrated together in such a manner that precise tracking and identification of all battle space entities will be achieved. It should be noted that some key work is already underway in the department under the auspices of the Joint System of Systems Engineering Office to integrate sensor inputs to

achieve unambiguous air track data so that a single integrated air picture can be created. Experts advise that the same software engineering approach that is being employed to create an unambiguous air track data environment can also be employed for the other domains (land, maritime, space, and perhaps cyberspace), thereby creating an unambiguous track data environment for all domains.

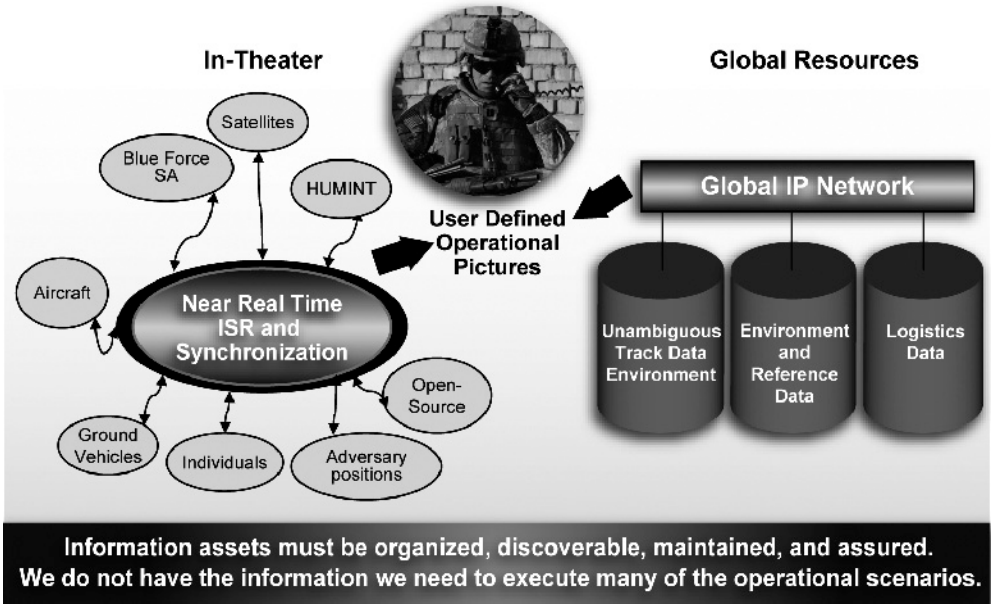


Figure 5. Organizing Data for Robust Decisions

This unambiguous track data environment created primarily via a well-synchronized, near real-time ISR tracking network (illustrated in figure 5) will then become a key information source that can be shared across all joint force elements via the GIG. The information from this key CIC data source, as well as information from the other data sources shown above, can then be displayed by joint force elements (users) in many different ways and on varying scales via user-defined operational displays. The displays needed at the tactical level may vary significantly from those required in a command center; however, the important premise that must be accepted and followed is that all user displays must use common data sources so that the information is consistent and authoritative across the entire joint force. A conceptual representation is depicted in figure 6.

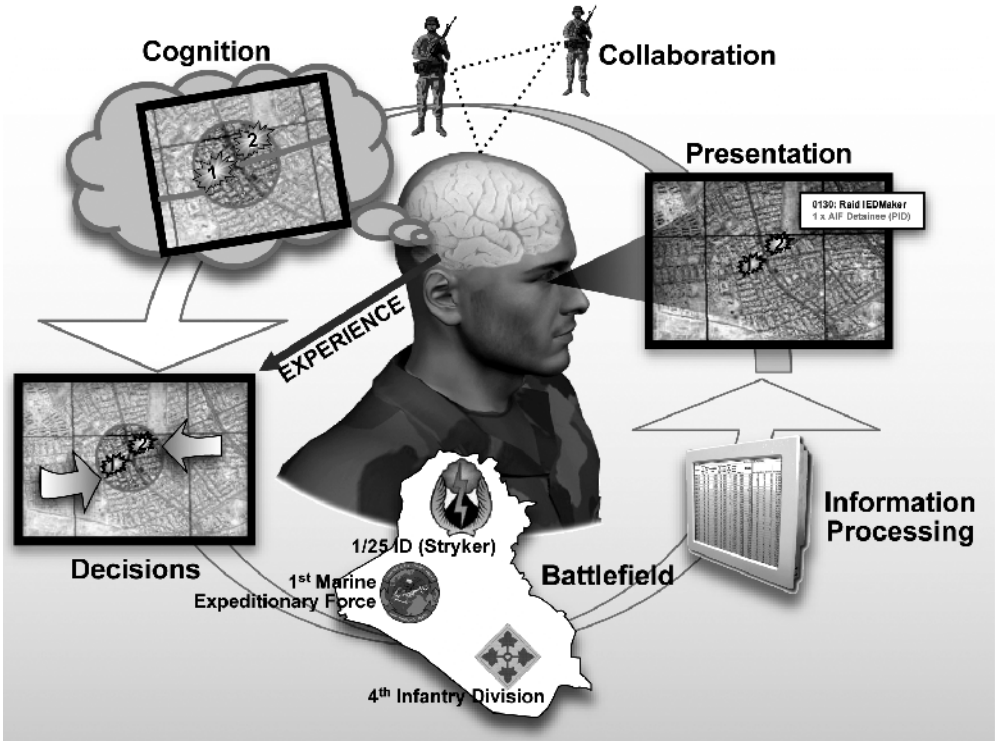


Figure 6. From Data to Effective Decision Making

Once the information is made available to the user, the next major problem to address is how to support that user in understanding the information. The solution lies in net-centric operations theory as articulated by, among others, Garstka and Alberts.[3] This theory addresses:

- The physical domain where strike, protect, and maneuver takes place across the environments of ground, sea, air, and space.
- The information domain, where information is created, manipulated, value-added, and shared. It can be considered the "cyberspace" of military operations.

3. Network Centric Warfare, August 1999, David S. Alberts, John J. Garstka, and Frederic P. Stein; "Power to the Edge," June 2003, David A. Alberts and Richard E. Hayes

- The cognitive domain, where the perceptions, awareness, understanding, decisions, beliefs, and values of the participants are located. These intangibles are crucial elements of network centric operations.

- The social domain, where force entities interact, exchanging information, awareness, and understandings, and making collaborative decisions. It overlaps with the information and cognitive domain but is distinct from both.

Cognitive activities by their nature are individualistic; they occur within the minds of individuals and are, therefore, the heart of decision making. These concepts can be applied to design of displays and training modules to enhance perception and understanding of all war fighters.

Proposed Combat Information Management Support

Combat information management involves the seamless, timely flow of information between and among a globally connected set of partners. The task force concludes, however, that commanders and tactical level combatants will need assistance in managing critical information needs until better information management tools can be created in the future. Thus, it is recommended that new skill sets be created called combat information specialists augmented by knowledge managers and subject matter experts. The details of all three are discussed below and the proposed information management architecture is shown schematically in figure 7.

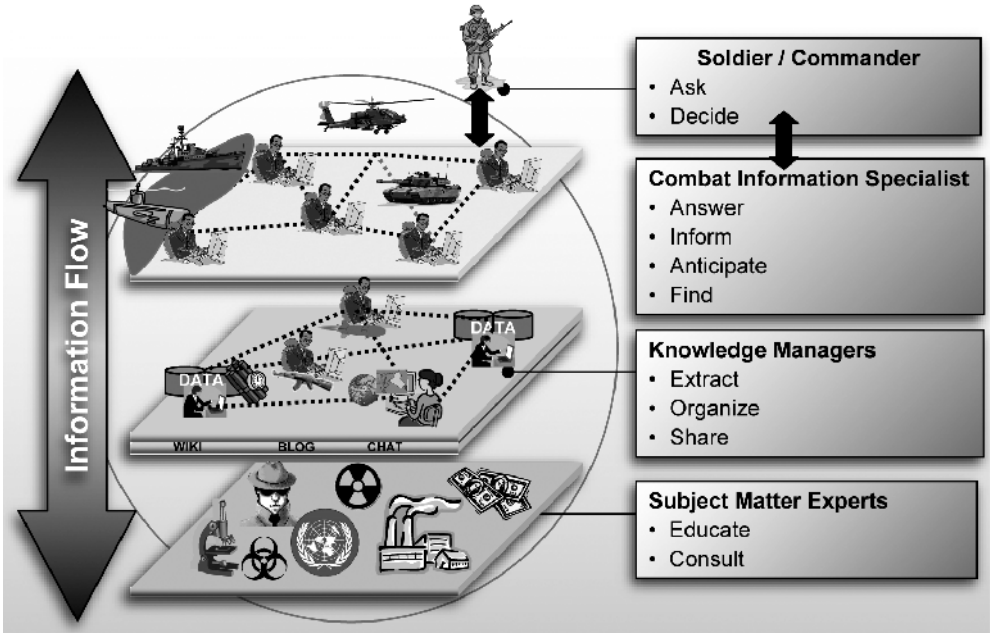


Figure 7. Proposed Combat Information Management

To date there has been an overall lack of focus and effort on managing information in the GIG—its creation, quality assurance, access control, and timely and appropriate dissemination. The private sector, especially those involved in businesses where a "knowledge advantage" provides a critical competitive edge, recognizes the value of information and invests in systems and people to exploit it. For example, Accenture (Accenture.com), a $15 billion global management consulting and technology services company, recognizes that their information base and experience is their most valued corporate asset and they treat it as such. They assign more than 150 information managers (called knowledge managers) to functional specialties such as oil, gas, insurance, and pharmaceuticals.

Information managers collect, process, and store for dissemination to interested parties the latest and most important information in their domain. They know the most relevant sources, the best subject matter experts, and identify the best practices in their focus area. They are responsible for both quality and content of information in their domains. They ensure that the full company's knowledge base is

available to all company representatives who interface with customers. Their focus is on the information and its management, not on the technology for its storage and delivery—though they rely heavily on an effective technical base. Typically these managers are also practicing consultants that organize the knowledge and ensure all newly collected or generated knowledge by anyone in the company is systematically added to the database.

Current DOD doctrine does not explicitly recognize the management of combat information as a critical military resource. Accordingly, both services and combatant commanders need to create combat information positions and associated concepts of operations. Figure 7 illustrates roles and example responsibilities of key players in a proposed approach to the provisioning of combat information management. In that proposed approach, combat information management support ranges from near-real-time intelligence (such as provided by combat information specialists) to longer-term substantive analysis (such as provided by knowledge managers and subject matter experts).

In particular, the creation of three distinct levels is recommended. At the first level, closest to the operator in space and time, combat information specialists answer, find answers to, and anticipate questions from commanders and operational users in the field. In developing answers to those questions, they may collaborate with combat information specialists supporting other units and commanders and/or they may work with knowledge managers who identify, discover, extract, organize, catalog, and maintain information about a selected set of topics. Knowledge managers, and others, use subject matter experts, who provide in depth knowledge, advice, and consultation in highly specialized areas.

Effective combat information management will require further refinement of roles and responsibilities, as discussed below. It will require development of concepts of operations and staffing plans. It should build on current service and combatant command efforts in this direction, as well as intelligence community assets. Success will require dedicated and trained staff at multiple echelons, although in many cases this will be possible through the redefinition of existing staff. A primary result will be

seamless, persistent, expert information support as units rotate in and out of the theater.

Combat Information Specialist

Combat information specialists answer operational requests, anticipate and track operational information needs, and disseminate critical information to combatants, both in mission rehearsal/ preparation and in real-time support of mission execution. They are integrated into units at all echelons, have intimate understanding of the unit's missions and objectives and, as such, are essential elements of the unit fighting team. They have access to classified information typically at the SECRET level, and possess an extensive network of contacts for information and intelligence. They share information with peers in the combat theater, can act as information liaisons with coalition forces, and provide knowledge managers with assessments of the value of information, as well as after action reviews, which knowledge managers will assimilate into their individual domains as appropriate. This skill is envisioned as a military occupational specialty.[4] In fact, the Air Force has defined an information manager specialty.[5]

Knowledge Manager

Knowledge managers are responsible for obtaining, organizing, maintaining, and sharing operational and technical knowledge in a specific focus area. For example, there might be knowledge managers focused on improvised explosive devices, surface to air missiles, Islamic culture, regional economics, or regional politics. While they are not necessarily subject matter experts, they need to have knowledge of the best sources of information and possess an extensive network of expert contacts. While they need not be physically collocated with operators, they are intimately aware of operational concerns and discover operational insights via their interactions with combat information specialists and users. One key role they play is as arbiters of quality.

4. See: http://en.wikipedia.org/wiki/Military_Occupational_Specialty
5. See: http://usmilitary.about.com/od/airforceenlistedjobs/a/afjob3a0x1.htm

Services provided by knowledge managers are shared across units, with dozens initially deployed, growing to hundreds at steady state, dynamically altering according to changing information needs. Knowledge managers are experts in a particular area and they are drawn from a variety of military skills.

Subject Matter Experts

Subject matter experts possess in-depth, long-term professional knowledge in a field of specialization. They perform detailed studies and analyses of specific domains (such as improvised explosive devices, surface to air missiles, Islamic culture). They are on call to advise the knowledge manager, combat information specialist, or users as needed. They may come from any sector including university professors, national laboratory scientists and engineers, the intelligence community, and military specialists. An essential enabling service will be the maintenance of a database of experts that can be semi-automatically generated using commercial tools (e.g., Tacit.com, AskMe.com).

Enabling These Roles

Several existing technologies can support each of these roles. These can include wikis, blogs, and collaboration tools. Also key to this approach is defining and staffing new military occupational specialty. Some service activity has already anticipated this need. These new positions help move data laterally across the enterprise activities helping what previously had been stovepiped, inaccessible data.

Imperatives for Enhanced Command and Control

Today, commanders take the command and control of functional areas of combat capability as a given. In terms of combat information, they manage their C2 staff to make sure they get the best information in the right form at the right time. To fully realize the potential of NCO, commanders need to take control of their information and the associated infrastructure (the CIC). This ultimately involves two major elements. First, all commanders clearly recognize that this is one of the critical leadership tasks. Second, the commander will need the staff,

tools, and processes to allow him to get the best situational awareness possible from the CIC.

As much as a fully capable information system available throughout a mission is needed, adversaries are well aware of U.S. dependence on that capability, and they have or may develop capabilities that will allow them to disrupt the CIC in a variety of ways. U.S. actions may also disrupt the capability. The commander must be able to maintain current situational awareness of the CIC and translate the current status to mission capability. The commander must also be aware of enemy efforts to disrupt operations, so that an attack can be countered and a response anticipated to any battle damage of the capability.

As the commander and his/her staff develop mission plans, contingency plans are necessary to plan for degraded operations. The degradation could be in a variety of areas, such as bandwidth, availability, latency, corrupt data, coverage, or protection. Sometimes the result may be an opportunity to operate differently motivated by a change in the situation.

The CIC offers both a challenge and an opportunity. The challenge is stated above. The opportunity is to take a giant step forward by integrating additional Combat Information Capability into the overall command and control function. Commanders need to be able to command and control critical information. This will tend to bring together both kinetic and non-kinetic attack elements into a unified system and, as a step along the way, provide a unified approach to the world of the cyber C2, which historically has been stovepiped and treated in very separate systems. The classic legacy ground battalion/task force tactical operations center with multiple, non-integrated wax pencil map boards is an example of stovepiping by physically co-located staff elements. This unification of C2 processes will allow commanders to have a tool set that supports managing cyber actions and will also allow management of the CIC to support other attack actions.

Specifically, an intellectual foundation is essential for developing future combat information concepts, educating commanders on the art of combat information dominance, and directing commanders to develop concepts of operation and contingency plans for operating with degraded networks.

In order to make this a reality, each service will need to organize, train, and equip cyber capable forces. Training must include network operation and the information management functions that have been discussed. New tools and processes need to be developed for combat information specialists and knowledge managers. These personnel will need to be trained on their tools and the procedures. This training will need to extend to virtual and field exercises such as mission rehearsal exercises, where the command and control of the CIC is exercised along with other joint war fighting capabilities.

Finally, information management staff expertise should be leveraged to doctrinally evolve a combat information planning annex. Similar to other planning annexes such as logistics, the mission plans will address all of the issues with deploying, operating, and defending a CIC in support of operational mission.

Intelligence, Surveillance, and Reconnaissance—an Essential Part of the Combat Information Capability

The war fighter is dependent on ISR sensors for most dynamic combat information. While some part of sensor data is usable only when analyzed, much reconnaissance data requires immediate access because of the time-critical nature of combat operations. Thus, delayed or denied access to ISR information has a significant impact on combat operation effectiveness. Currently, combat information needs compete with national intelligence needs for space asset coverage. The uncertainty of satellite coverage causes operational commanders to rely more on theater controlled assets to ensure coverage, usually to the detriment of lower priority requirements. The lack of knowledge of planned national ISR capability limits integration into the operations tempo and sub-optimizes a limited resource.

Thus, the department needs to recognize the value of treating all space-based airborne (manned and unmanned) systems, and ground and maritime sensors as elements of a single system. Ground combat units are acquiring hundreds of unmanned aerial vehicles with improving sensors. Ground sensors are becoming more effective. All these systems can be more valuable when the data is integrated with other sensor data. The key is to network-enable all ISR data and metadata to ensure timely availability to the war fighter. This capability, when fully implemented, will reduce lead times for dynamic tasking of sensors, thereby greatly reducing the time to respond to time critical targets.

Combat Information Capability needs to be created and resourced across the department, since all military commanders must undertake new ways to execute command and control of their combat information resources and capabilities. In order to maintain oversight, these new capabilities must be monitored by creating a Defense Readiness Review System category for CIC readiness.

To enable the commander to take full advantage of this CIC, Joint Forces Command (JFCOM) needs to develop training programs to prepare commanders to effectively command and control this capability.

A CIC must contain the following capabilities:

- execution elements of a combat information support staff: combat information specialists, knowledge managers, and subject matter experts
- robust combat information management training and education and the capabilities to support such activity
- proper tools and tactics, techniques, and procedures for commanding this new capability.

The CIC must deliver dynamic, integrated ISR capabilities, which will provide operational commanders with visibility of the tasking of sensors and then allow the commanders to effectively plan theater assets.

Recommendation: Create and Resource a CIC

The Deputy Secretary of Defense shall direct:

- JFCOM to establish a training program to prepare commanders to execute command and control of their Combat Information Capabilities.
- The services to create and resource combat information positions, to include combat information support staff, combat information specialists, as well as knowledge managers and identification of subject matter experts. Also, commanders at the three- and four-star level need to be provided combat information integration officers on their personal staffs.
- U.S. Strategic Command (STRATCOM), Under Secretary of Defense for Intelligence, and ASD (NII) to deliver dynamic, integrated ISR capabilities that enable operational commanders to have visibility into national sensor tasking plans, including reducing lead times for dynamic tasking of assets.

Robust Information Management

The GIG is the information technology base (transport, storage, security) underlying a global military information service. Serious attention is required to the "information" aspects, in addition to the "information technology" aspects. However, the Clinger-Cohen Act has carefully defined the "CIO" role, emphasizing—almost exclusively—the information technology portion of the topic. The definition and expansion of this position is required to include managing information content, quality, timeliness, focus, currency, pedigree, relevance, accuracy, and completeness. This new definition will recognize the evolving role of the "CIO" as the earlier, more hardware- and software-oriented definition focused more on assuring interoperability, which is clearly an accepted principle in the evolving information technology and information management world.

Current DOD CIO responsibilities and functions as outlined in DOD Directive 5114.1 (May 2, 2005) are primarily focused on information technology management issues rather than on information content management issues. For example, the DOD CIO responsibilities include:

- evaluating the performance of information technology programs
- reviewing the DOD budget request for information technology
- developing and maintaining the DOD information assurance program
- ensuring the interoperability of information technology systems
- maximizing value and assessing the risk of DOD information technology acquisitions
- prescribing information management policies
- maintaining a DOD Records Management Program
- overseeing development and integration of the GIG
- increasing use of commercial information technology solutions
- ensuring compliance with information technology standards to enable interoperability

While essential to the effective operation of the department, a concomitant set of responsibilities is necessary to oversee the management of information.

Recommendation: Focus on Information

The Chief Information Officer shall expand the responsibilities of all CIO organizations throughout the DOD combatant commands, services, and agencies to:

- establish means and processes to review and assess accuracy, credibility, pedigree, and currency of posted information
- champion policies for information quality, access, and sharing
- implement and distribute incentives for information sharing

- create positions and manage the implementation of the combat information specialists, knowledge managers, and subject matter experts
- identify opportunities for new services in support of user needs.

Chapter 3. Information Dissemination and Management

The Technology Context

Technology advances in the last half of the 20th century fundamentally altered concepts of how people interact with each other, what functions machines can perform, and how the increasing availability of information can reshape day-to-day activities. The Defense Department has embarked on a complex, multi-year transformation to exploit these new concepts for the national security advantage of the United States.

Perhaps the dominant change in this period was the arrival of the Internet. Conceived as a result of Advanced Research Project Agency initiatives in the 1960s, the Internet provided extraordinary opportunities for innovation and led to the creation of vigorous private-sector initiatives to capitalize on its potential. A few characteristics of the Internet—notably its simple standards, lack of a central authority, and public nature—made it the inspiration for much of the technical innovation in the world today. The Internet, with higher level standards that have more recently emerged, is the model for the future Defense Department information environment.

The Internet model has several qualities that align with DOD needs:

- The simple data transport standards enable the interconnection of diverse devices (computers, phones, radios, and televisions, for example). These interconnections have proven to be robust and scalable. Millions of devices can participate together in networks.
- Higher level standards enable information sharing among people and machines. Electronic mail, electronic maps, imagery, and video are common elements of day-to-day life.

- Commercial innovation is bringing new capabilities to market at a rapid pace—a pace unachievable by traditional government processes.
- The ability to rapidly share information and knowledge offers the promise of more productivity. In the case of the defense mission, there is the promise of making U.S. forces faster, smarter, and more lethal than any enemy, through information support to decision-making and execution.

The Internet model also has several drawbacks:

- The Internet model poses challenges for information assurance. In particular, the desire to isolate systems to protect them makes them ineffective for the purposes of sharing information and knowledge.
- The global availability of the commercial Internet means that others, including enemies of the United States, can take advantage of the Internet model without large infrastructure investments in communications and software. The historic advantage U.S. forces have had in these areas is being minimized.
- The pace of innovation has led to shortened product life cycles, implying continual investment to avoid obsolescence.
- The dependence on software, which may have undocumented and undesirable features, has increased.
- The ability to create or modify information environments has not kept pace with rapidly changing requirements and national priorities.
- Management concepts for programs and capabilities work best when applied "vertically;" that is, when each program controls its interfaces and performance criteria to be independent of all others. But to take advantage of the Internet model, capabilities must be implemented "horizontally;" that is, when each program shares its capabilities and data with others and is dependent on them.

The following explores an approach to bring the advantages of the Internet model to the Defense Department while mitigating the disadvantages. Changes to the department's processes for enterprise architecture, technology acquisition, and information management are required. Several recommendations are made to align ongoing programs of record, and further recommendations are made to help maintain the alignment for the future through governance and system engineering processes.

Building the Enabling Capabilities

The foregoing section described the opportunities, along with some cautions and risks represented by the rapid advance of commercial information technology in general and the Internet revolution in particular. The DOD, under the banner of the GIG, is undertaking a set of initiatives—and making substantial program investments—to seize these opportunities, mitigate their risks, and ultimately deliver an enterprise-wide information infrastructure to enable network-centric operations. The delineation of a capability-driven architecture, the execution of an enterprise-level system engineering activity, and the maturing of the new portfolio management process are key elements of the DOD strategy for achieving NCO capability objectives.

This section both describes and assesses the GIG architecture, system engineering, and portfolio management processes and products as understood by the task force, based on presentations from and discussions with government personnel.

The key questions are:

- Whether the architecture provides realizable direction toward fielding NCO-enabling capabilities.
- Whether there is a robust system engineering process in place to translate the architecture into actionable program guidance, and for informing potentially difficult cross-program, cross-organization decisions, as needed, to achieve "horizontal" capabilities.

- Whether the portfolio management process can be informed by system engineering and matured to maximize enterprise capabilities, not just to address the inevitable programmatic issues.

Architecture

Fundamentals

At one level, a basic set of architectural goals can be expressed in terms of building an "Internet-like," layered information infrastructure which:

- provides ubiquitous networking among information providers and users
- makes information readily accessible, discoverable, and "understandable" across the network
- enables
  - information sharing across the enterprise
  - the development and sharing of a rich set of value-added information services and applications
- assures the security, integrity, and availability of the network and its information by:
  - eliminating bandwidth and computational constraints to the maximum extent possible
  - adopting or adapting commercial products and technology whenever possible while
  - recognizing and responding to uniquely demanding DOD and intelligence community considerations, especially information assurance.

Such a broad formulation of goals, though useful, does not provide a complete basis for guiding and assessing programs and initiatives, or for making decisions. Addressing this issue, the ASD (NII) strategy has been to establish and promulgate—and adopt for "regulatory" purposes—a relatively short list of fundamental architectural principles

viewed as crucial to the building of NCO-enabling capabilities. These principles generally take the form of "design tenets" or "information handling paradigms."

Design Tenets

1. **Internet Protocol (IP) adoption as the "convergence layer."** The adoption of the IP commercial standard not only provides for interoperability among heterogeneous systems and devices (currently known and unknown), but also offers the transformational capability to flexibly handle all types of information (such as video, voice, and data) as "converged" streams of packets. The transition to IP-based packet routing/switching and away from dedicated circuits is central to the information handling agility, level of interoperability, and scalability envisioned for the GIG.
2. **"Infinite" bandwidth core/backbone**. This tenet calls for a "core" network, within the larger overall enterprise, which effectively eliminates bandwidth as a constraint within that "core." Its realization involves the exploitation of optical transmission links in a way that will be elaborated below. The resulting "essentially infinite" bandwidth largely addresses a legitimate concern about adoption of IP—the need to over-provision to assure quality of service.
3. **End-to-end encryption across the core/backbone ("black core")**.
   The concept of end-to-end encryption is a cornerstone of the architecture in terms of information assurance. Particular emphasis is placed on maintaining the "all black" flow as information transits the core network, understanding that "red' gateways may be required at the interface between the core and users/systems that lie beyond the "edge" of this core (particularly tactical users who may not be equipped with information assurance devices that "extend" the core).
4. **Data-centric implementation**. The separation of the data from applications and its labeling/tagging enable the capability to have multiple users and/or applications operating on the

same information at the same time, dramatically increasing a user's ability to satisfy his/her own needs and allowing the concurrent development and execution of value-added applications. This design tenet precludes "burying" data within a particular user application and relates closely to the "post-in-parallel" paradigm discussed below.

Information Handling Paradigms

1. **Post data in parallel (as information is created and/or received in "raw" form).** This approach calls for posting data—labeled/tagged as above—before user/application filtering occurs. The intent is to preserve the "raw" data for value-added use by all/any users with appropriate access, including for purposes that cannot be foreseen. This is fundamental to the notion of information sharing, starting at the source. It also enables innovation and unplanned exploitation among users with appropriate access.
2. **User-driven information sharing**. With the foundation provided by data that has been posted and labeled/tagged and is "discoverable"—and with appropriate protection mechanisms—users have the capability to satisfy their own needs for information and to broadly share with others. The potential transformational notion of "smart pull" is facilitated in addition to the paradigms of "smart push" and "publish and subscribe." Sharing is facilitated by establishing a common data dictionary within defined communities of interest.
3. **Need to share vice need to know**. This principle, using a vocabulary that has strongly emerged since 9/11, addresses information sharing challenges when faced with legitimate (though sometimes abused) obstacles in terms of security, privacy, competing mission needs (such as protecting chain of evidence), constraints with respect to U.S. versus. foreign entities. It implies sometimes difficult tradeoffs and the implementation of assurance mechanisms that are not now in place, such as dynamic allocation of access (based on situation or roles of individuals, for example).

4. **Collaboration at all levels**. This paradigm, like "need to share vice need to know," can be viewed as a special case of information sharing. It is singled out as being of particular operational importance and as demanding particular capabilities from the system. For instance, it implies the provision of common or at least interoperable information services spanning video, voice, and data and operating both in "essentially infinite" and "disadvantaged" bandwidth situations.
5. **Reach-back for critical information and combat operations support**. This principle provides for reach-back, from the theater of operation, to the continental United States (CONUS) or sanctuary locations with substantial information support resources (data, exploitation tools, expertise). This imperative is driven heavily by the priority on leveraging the ever-increasing quality and quantity of ISR information—raw and exploited—that offers critical support to the war fighter.

Note that the fundamental design tenets of "infinite bandwidth" and full end-to-end encryption apply to the core only, not to the networks/systems beyond the core. This is a reflection of realities as one moves into the tactical domain (e.g., disadvantaged users from a communications standpoint). Extending these attributes as far down toward the individual combatant and weapon platform is, however, a priority objective. As will be elaborated below, selective extensions of wideband communications and of the "black core" into the tactical world are offered by major transport programs-of-record—terminals for mobile users with embedded devices supporting IP level end-to-end encryption.

Information Management Architecture

Figure 8 illustrates the information management architecture, including layered elements that ride on top of transport, such as data, enterprise services, community of interest services, and applications. The enterprise services consist of four product lines:

1. Service-oriented architecture framework
2. Content discovery and delivery
3. Collaboration
4. Defense online portal

Information assurance and network operations cut across these levels. Communities of interest leverage these services and subgroups of them are organized into capability portfolios (such as command and control, ISR, joint logistics, and joint network-centric operations).

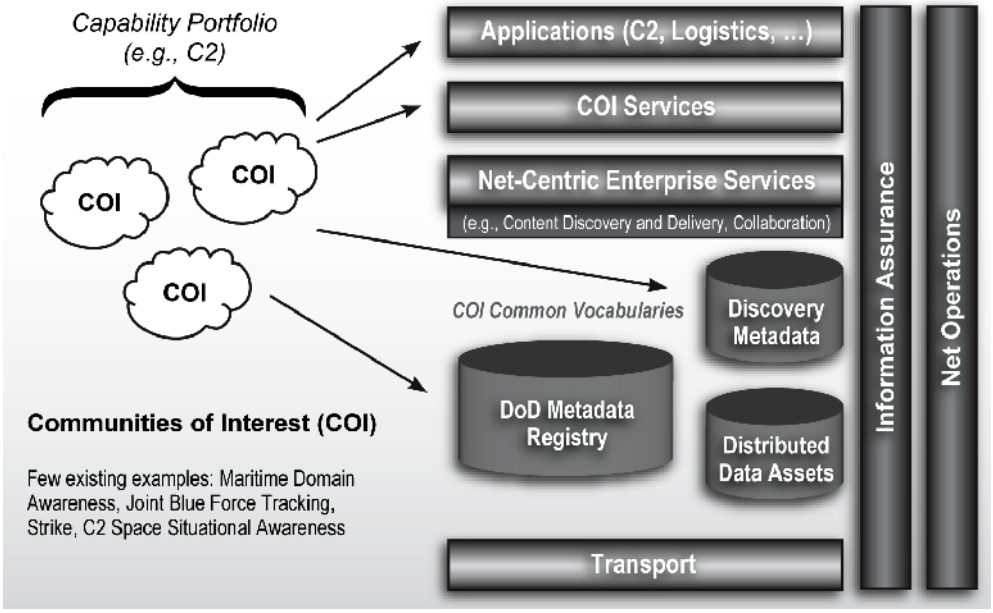


Figure 8. Information Management Architecture

A key concept of net-centricity is to support the "unanticipated user." Accordingly, security services include strong authentication and authorization services consistently applied across the GIG. These services provide a basis for establishing trust relationships across stovepiped security enclaves. Individual users are validated using certificates, described by attributes about roles, provided visibility to information described by sharing policies, and permitted information access based on policy decision enforcement.

Net-Centric Data Strategy

Net-centric information architecture concepts enable an unprecedented volume of data in a multitude of formats to be shared enterprise-wide. The challenge is to make this data accessible, discoverable, and understandable to every appropriate DOD user. The complexity of the DOD environment introduces challenges—scale, stress, security, range of war fighting/business areas, and multiple lines of authority. The data strategy must support this range of data sources, functions, and environment, enabling the exchange of information between producers and consumers.

The key attributes of the DOD network-centric data strategy are:

- ensuring data are visible, available, and usable when needed and where needed to accelerate decision-making
- "tagging" all data (intelligence, non-intelligence, raw, and processed) with metadata to enable data discovery (by users and machines)
- posting all data to shared spaces to provide access to all users except when limited by security, policy, or regulations
- advancing the department from defining interoperability through point-to-point interfaces to enabling the "many-to-many" exchanges typical of a net-centric data environment

The strategy also introduces management of data within communities of interest rather than standardizing data elements across the department. The strategy separates data from application encouraging interoperability and access, extensibility, and more robustness access control.

Communities of Interest

A community of interest operates in DOD as a collaborative group of people that must exchange information in pursuit of shared goals, interests, missions, or business processes. Communities of interest provide an appropriate focus of net-centric related efforts—to agree on standard community vocabularies, to expose data for discovery and

sharing, and to present common user communities to facilitate providing Net-centric Enterprise Services (NCES) web service capabilities.

The DOD CIO has been active in forming an initial set of communities of interest, including Joint Blue Force Tracking, Strike, Maritime Domain Awareness, and Command and Control Space Situational Awareness. To establish information sharing among its members, a community of interest must:

- Decide what it will specifically accomplish, and the supporting information products that will be required.
- Establish an information model for collaboration, begin to build a common vocabulary, and standardize data. This requires establishing a community of interest data model and framework, including a common taxonomy, vocabulary, and schema. The resultant metadata standards become part of the DOD Metadata Registry.
- Determine what community of interest information sharing capabilities are needed and how the NCES must support it. The NCES services include enterprise web services such as directory, discovery, and security services. Some information sharing capabilities may be unique to the community of interest and require specific services. For example, a user-determined operational picture is enabled by NCES where each community of interest user can personally subscribe and configure information to their particular needs.

Recommendation: Information Management

DOD process owners (Chairman Joint Chiefs of Staff, USD [AT&L], Program Analysis and Evaluation, CIO, Comptroller) shall:

- encourage creation of an information marketplace
- develop resource incentives for making data visible and delivering value-added services
- promote risk-managed information sharing
- deliver value-added services that assess quality of information

The Deputy Secretary of Defense shall ensure:

- DOD components accelerate formation of communities of interest, both top-down and bottom-up (the latter encouraging spontaneity of organization).
- Mission area leads aggregate communities of interest into capability portfolios to rationalize capability portfolio vocabularies and harmonize community of interest services and value-added services.
- USD (AT&L) direct Milestone Decision Authorities to reflect community-of-interest-related capability portfolio goals in direction to program element offices and program managers.
- DOD CIO and designated communities of interest leads co-chair appropriate information technology acquisition boards.

Application Acquisition

While core enterprise services need to be standardized and relatively enduring, the application level demands much more flexibility, rapidity of deployment, and diversity to support user innovation in the face of changing needs, particularly at the "edge." While there are pockets of such application development, the practice is not widespread in DOD. Programs such as Net-Enabled Command and Control (NECC) are intending the rapid, incremental delivery of application capability. However, the initiation of the program was lengthy, roughly five years from the initial identification of need to the first delivery of capability. Approximately half that time was spent on developing the documentation (of several hundred pages) that specified the needed capabilities. Such a process is not responsive to the immediate and changing needs of the users in the Combatant Commands.

Accordingly, process owners need to revise the Joint Capabilities Integration and Development System (JCIDS) and acquisition system polices to encourage rapid, flexible delivery of application capability increments. Particular steps that should be taken include:

- Change JCIDS focus from detailed specifications to key, high-level capability needs. Such needs should be decided upon relatively quickly and not subjected to a lengthy staffing process.
- Streamline the acquisition resourcing process to allow rapid initiation of development efforts. One possible approach is to allocate funds to a general account without detailed program specification, and then assign funds from this account as specific development efforts are approved.
- Foster innovation by drawing on a diverse set of developers, with a particular emphasis on those from the commercial sector. The philosophy is to maximize capability delivery by allowing any source to provide value-added application services without reliance on a large program structure or detailed capability needs specification.
- Apply the streamlined processes to deliver capabilities in spirals. This entails delivering initial capabilities to operational users prior to defining the entire suite of desired capabilities, capturing feedback from user experience with these (and subsequently delivered) capabilities in operations or exercises, and allowing change of capability development plans in response to this feedback.
- Foster informal development of limited capabilities outside the JCIDS process (even if streamlined as noted above) to get "good ideas" into the hands of users as soon as possible. Developers would work in close collaboration with operational users who test the application capabilities in experiments and exercises. If the delivered capabilities prove worthwhile, then more formal development would be applied if necessary; if the capabilities did not prove worthwhile, the development would be terminated.

Recommendation: Streamline Information Technology Acquisition System

Chairman, Joint Chiefs of Staff and USD (AT&L), revise JCIDS and Acquisition System policies to encourage rapid information technology procurement:

- Significantly reengineer JCIDS for information technology away from detailed specifications to key, high-level capability needs.
- Apply the streamlined JCIDS process to deliver capabilities in spirals. Also focus on "buy and dispose" concepts from commodity type acquisitions (hand-held communication devices, for example).
- Recognize and exploit opportunity to purchase information technology and services as a commodity where practical (routers, switches, blade servers, identity management services).

Research and Development

While human skill and expertise will be the single most important factors contributing to the success of combat information management in network-centric operations, technology that supports that expertise promises significant performance enhancements. Indeed, knowledge managers in commercial enterprises are armed with an array of technical tools for organizing, analyzing, storing, and sharing information. Below is a discussion of the need for similar tools to support the combat information specialist—note that some tools employed by industry may be adopted wholesale; however, others will need to be adapted and yet others developed to meet the unique needs of combat information support. As suggested in figure 9, information management technologies can enhance combat decisions by automatically processing information (extraction, summarization, correlation); generating user tailored and/or contextually situated presentations, supporting a range of cognitive tasks (focus of attention, pattern detection, and comparison, for example); and decision support (such as applying knowledge and experience to generate, assess, and select among alternative courses of action).

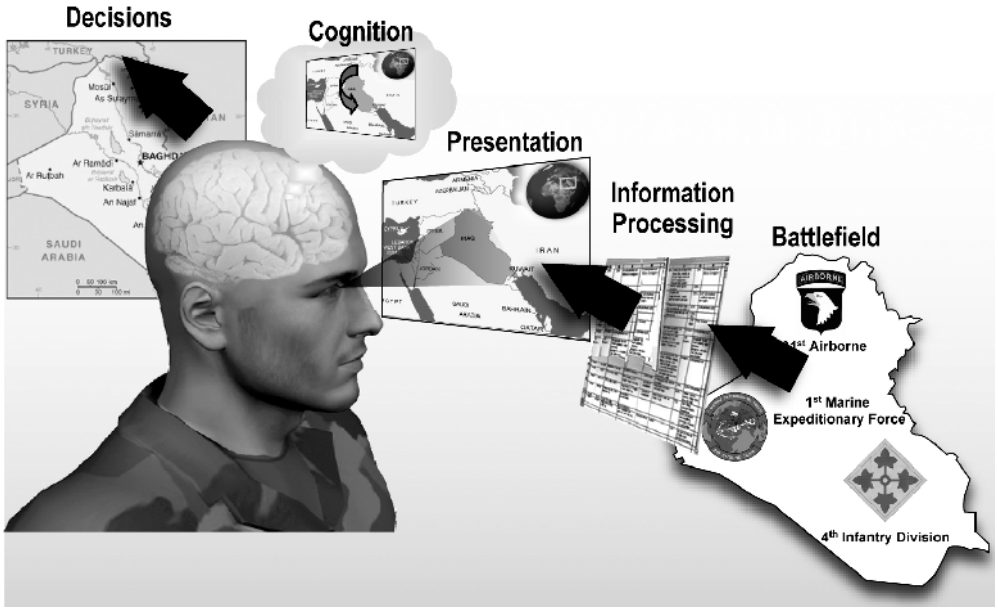


Figure 9. Information Management to Enhance Combat Decisions

Information Discovery

In each of these areas, research promises advances that can transform operations. For example, in the area of information discovery, intelligent analysis of content promises several benefits. Automated metadata tagging of documents can be used to annotate massive collections of reports and captured documents to provide enhanced search and discovery. Operations will require advances beyond the state of the art to include 95 percent accurate entity tagging (that is, people, organizations, and locations) and 80 percent accurate event extraction in English and foreign language text (current state of the art is around 90 and 50 percent, respectively, for text.[6] Soldiers also require automated voice transcription of after-action reports to increase the timeliness and coverage of reporting. Forces also need automated content extraction from multimedia, such as unmanned aerial vehicles or surveillance video, as well as audio intercepts and reports. Operators also require tools for semi-automated assessment of quality and

6. See: trec.nist.gov.

relevance of information. Locating quality information rapidly on a dynamic network that might be degraded under attack coupled with the need to provide more fine-grained (subdocument) access control, suggests that services such as Uniform Resource Names can help resolve information references and provide more reliable and fault tolerant access to information.

Information Understanding

In addition to more effective discovery of information, advances are needed to enhance cognition and information understanding in the context of missions. Increased information understanding can lead to a 50 percent improvement in situational awareness and a two times speed up in understanding. Advanced understanding tools are required to automatically associate, cluster, fuse, and summarize information. For example, automated document summarization (SUMMAC[7]) has been shown in science texts to reduce text by 80 percent with no information loss. Understanding the meaning and implications of information are important and will require effective application of knowledge representation and reasoning. For example, ontology management tools (creation, merging, refinement) can be applied to enhance semantic machine-to-machine interoperability.

Tools for information triage (based on relevance, priority, and quality) to counter information overload as well as tools to counter denial and deception will become increasingly important. Finally, operators need context-aware presentations that are sensitive to a variety of environmental factors (location, time, and device) as well as to the psychological, perceptual, cognitive, and social characteristics of the user and groups. Addressing all dimensions of context management (time, location, mission, user role, ongoing dialogue) promises more efficient and effective operations, particularly for (bandwidth, presentation, attention, and memory) disadvantaged users. A key future capability will be to learn users' context, information needs, and preferences through observation. As this technology matures it will

7. http://www-nlpir.nist.gov/related_projects/tipster_summac

allow the staff functions of a combat information specialist, knowledge manager, and subject matter experts to become more fully automated.

Information Sharing

In addition to improved machine understanding, effective information management requires enhanced, machine-facilitated, human-human interaction. Information sharing between the United States and coalition partners can be enhanced with semi-automated dissemination that leverages information bases that are tagged both in terms of discovery metadata (bibliographic, security) as well as content metadata (entities and events in the text). Semi-automated dissemination and tailored information packaging promises to reduce requests for information from the field by over 50 percent (of Joint Intelligence Center Pacific[8]) by dissemination to appropriate classification (sensitive but unclassified, SECRET, TS) and/or release (coalition, nongovernment organization), based on both security and content mark-up. Tools that facilitate knowledge elicitation (such as leveraging but extending beyond DARPA ASSIST to support effective automated debriefing) are needed to support functions such as semi-automated capture, processing, and dissemination of after action-reviews and lessons learned. Finally, enterprise collaboration services (such as presence and awareness) need to provide context-based, mission- and role-tailored discovery, collaboration, and sharing.

Information Marketplace: Warrior Tracking and Behavior Analysis

Enabling the management of and fostering the growth of an information marketplace will require mechanisms to understand user information needs, tools to design information services and control and tailor delivery, and mechanisms to assess the quality of delivered services. Information and information services monitoring will require mechanisms to audit and analyze user information consumption and utilization behaviors. To create richer models of the information

8. http://jicpac.com/web/about_jicpac.html

marketplace understanding will need to go beyond instrumentation of warrior behavior to include:

- surveys
- post-mortems
- more generally, ethnography of information service providers and consumers
- analysis of social drivers (identity and reputation, rewards and incentives)

Recommendation: Information Management Research and Development

Director, Defense Research and Engineering (DDR&E) establish and extend programs for:

- Information discovery
  - auto generation of metadata/auto-tagging
  - tools for assessment of quality of information
  - content extraction from unstructured text/video/audio
  - advanced discovery tools
- Information understanding
  - fusion and association
  - cognition and information understanding in the context of missions
  - knowledge representation and reasoning (ontology)
  - context aware presentation
- Information sharing
  - knowledge capture
  - context-based, mission, role tailored discovery, collaboration, sharing

- collaboration—presence/awareness, tailored
- Semi-automated dissemination

- Net warrior tracking, behavior analysis
  - audit, capture, analysis of use/change
  - surveys, post-mortems, instrumentation, ethnography

System Construct

The basic system construct for implementation of the GIG NCO-enabling architecture is depicted in figure 10 below. This greatly simplified depiction is intended to convey key features of the architecture in "physical" terms. Several programs-of-record, those viewed as delivering particularly key capability "building blocks," are indicated. Although dealt with in more depth in a subsequent section, these elements are shown here to make this description of the construct more tangible.

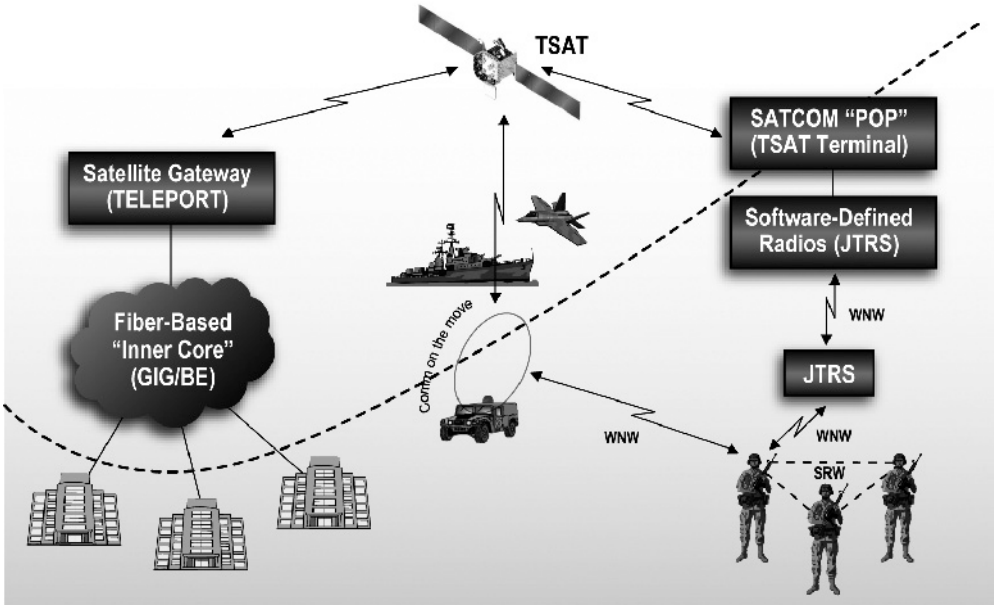


Figure 10. Key Transport

The architectural notions of (1) a core/backbone network providing "infinite' bandwidth and IP level end-to-end encryption among users and providers located in the CONUS or in selected sanctuaries, and (2) interfaces with, and extensions to, tactical level users/platforms (including mobile), were introduced above. More specifically, the NII-delineated architectural construct, as depicted in figure 10, consists of:

- A two-level core/backbone network with the noted "infinite bandwidth" and IP-level end-to end encryption attributes.
  - An "inner core" with meshed, fiber-based connectivity among CONUS and selected sanctuary locations outside CONUS, implemented by the Global Information Grid/Bandwidth Expansion (GIG/BE).
  - An "outer core" that extends from the "inner core" to theater locations via wideband satellite communications and, using Internet terminology, provides a core network "point-of-presence" (POP). The Transformational Satellite Communications System (TSAT) is a key capability to achieve this.
- A set of wireless, line-of-sight-radios/devices beyond the core but (1) interfacing to its "edge," either directly or through "intermediaries" (e.g., the Army's Warfighter Information Network—Tactical) and (2) providing IP-based capability along with substantially greater capacity than current tactical radios. The Joint Tactical Radio Systems (JTRS) program is the principal new capability. There are also a variety of legacy upgrades and commercial options being considered in the interim.
- Exploiting the above transport architecture, the conduct of network-centric operations will enable communication:
  - among users and providers who are directly connected to the "inner core" (such as various intelligence nodes and major fixed bases)
  - between users and providers directly connected to the core and those beyond its "edge," with satellite-based reach-back as a key feature

- among user and provider communities of interest or enclaves that reside beyond the edge

Note that, as depicted, both TSAT and JTRS (or some equivalent) provide critical capability from the viewpoint of the tactical user. TSAT will uniquely provide relatively wide bandwidth connectivity to small, ground-mobile platforms, supporting "command and control on the move;" JTRS is designed to provide both a wideband networking waveform (WNW) for meshed inter-netting among mobile platforms and tactical C2 facilities, with the soldier radio waveform (SRW) providing analogous capability among individual combatants.

Though the communications foundation for NCO is surely a crucial enabler, the delivery of operational capability in terms of "information as a weapon" is found at the upper layers of the architecture. In this regard, two features of the architectural construct stand out:

1. Adoption of a service-oriented architecture, meaning the provision of a common set of software-instantiated middleware services that are accessed from across the enterprise network and enable applications/users to exploit the network and its data (a discovery service or an identity management service, for example).
2. Adoption of a community-of-interest strategy to facilitate mission-driven information sharing, meaning the creation of a collaborative group of information users and providers who organize around a mission (such as maritime domain awareness, space situational awareness) and develop a common vocabulary for machine-to-machine information exchange.

Finally, it can not be over-emphasized that there are serious information assurance challenges that go beyond the implementation of the "black core" and will impact the architecture in ways that are only now emerging. This topic is the subject of a separate chapter.

Observations

As discussed above, architecture fundamentals have been articulated and a basic system construct, a top level system design, has at least been outlined. The bottom line architectural findings are:

1. The architecture, as understood by the task force, is viewed as sound and as constituting positive direction to the department's efforts to field an NCO-enabling information infrastructure.
2. On the other hand, it is not articulated consistently or elaborated substantively in any one place or product. Also, there are crucial interpretational and definitional issues regarding the meaning of the fundamental tenets and paradigms as evidenced in both dialogue with government presenters and within the task force itself. This may well impede "unity of action."
3. More fundamentally, even if the architecture were "perfect," there is the critical job of translating its fundamentals into tangible, actionable program guidance and assuring that the department's set of implementing programs yield coherent "horizontal" enterprise capability.

The concerns identified here are addressed in the following discussion of system engineering.

System Engineering

It can be argued that the department faces an unprecedented system engineering and related governance challenge, given the scale of the enterprise and the need to build inherently "horizontal" capability in the world of "vertical" programs and organizations. Addressing this challenge is a central element of treating the NCO-enabling information system as a critical combat capability or as a "weapon system." This section characterizes the ongoing enterprise system engineering activity and develops a set of recommendations. A later section addresses the governance issue in the context of the "portfolio management" process that has emerged from the Quadrennial Defense Review.

Ongoing Efforts

An "enterprise-level" system engineering activity is needed to:

- translate the architectural fundamentals into tangible program guidance
- analyze and trade among program and design options with a constant focus on overall enterprise functionality and performance
- support cross-program and cross-domain decision-making

A critical objective is to assure coherence among the key programs developing and delivering the essential "building block" capabilities. Synchronization of delivery across programs from a mission capability standpoint, is another objective. Figure 11, below, without even penetrating the detail, illustrates the challenges.

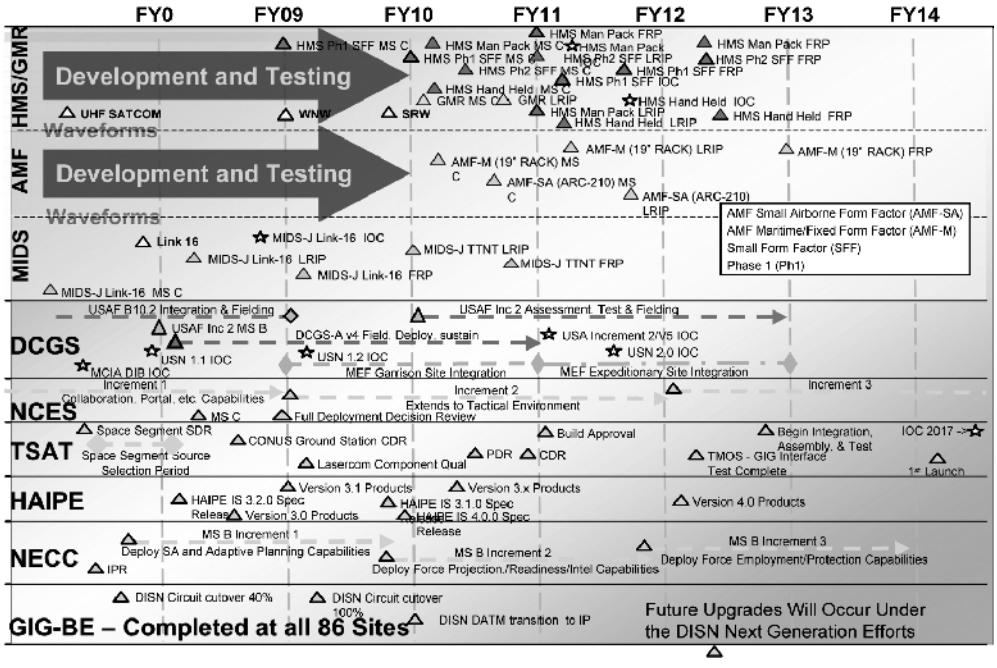


Figure 11. Net-Centric Programs Schedule

The ASD (NII) established an Enterprise-Wide System Engineering (EWSE) office in 2004. The Defense Information Systems Agency (DISA) is assuming increasing responsibility for this function with continuing NII oversight and involvement. The ongoing efforts are struggling with the differences between executing a system engineering process at the enterprise level as opposed to the individual program level. Formalistic specifications, flow-downs to "subsystem" specifications, and work break-down structures, are neither desirable (too constraining) nor practically realizable (scale and complexity). It is noteworthy, in fact, that the larger technical community is only now struggling with the art and science of large scale, complex—read "enterprise"—system engineering. So, the department is breaking new ground in some respects. This fact, along with the obvious "horizontal" versus "vertical" governance and authorities issues, yields the term "unprecedented."

The NII-led EWSE activity is executed by a core team of government, federally funded research and development center, and contractor personnel, plus "coalition of the willing" (and available) service and agency participants. There is surely good news in terms of (1) serious technical work on critical enterprise-level issues, such as assuring quality-of-service across the network, (2) development of initial guidance products that lay out standards that would assure interoperability and Internet functionality, and (3) at least the beginnings of an analytically-based effort to estimate and bound end-to-end performance from a user standpoint.

Observations

Positives notwithstanding, the task force developed a set of concerns about the current activity:

- The effort attempts to be comprehensive in terms of the scope of mission and functions (such as GIG support of DOD business processes as well as war-fighting). This is understandable and, in fact, appropriate, given the NII/CIO charter. However, comprehensiveness does not allow clear focus on the delivery of combat information capability.
- The technical work exhibits a tendency to over-engineer and over-optimize across a broad range of issues without clear prioritization based on mission functionality and performance

impact. For instance, the analysis of end-to-end latency versus different quality of service and precedence schemes is important, but only if the latency differences matter from an operational standpoint.

- The strategy for influencing programs seems to rely on relatively detailed, prescriptive guidance documents (network-centric implementation documents) with enforcement through control and compliance processes. This is different from limiting prescription to a few, absolutely crucial elements of guidance, and then actively engaging collaboratively with programs on the longer list of issues and trades that need attention from an enterprise viewpoint. (The involvement of "coalition of the willing" service and agency program participants, noted above, is inherently spotty and does not constitute adequate engagement from the viewpoint taken here.)
- Despite good intentions and plans, it appears that the effort devoted to analysis, simulation, and test-bedding (at least to date) has been extremely limited. Not only does the serious execution of such work constitute good engineering practice, but such work is particularly crucial at the enterprise level. At this level, scale and complexity defy confident predictions based on appropriate engineering analysis of design integrity and end-to-end performance.
- The efforts to date have focused almost exclusively on "transport layer" issues and guidance. This too, is understandable due to "essentially infinite" bandwidth as a key foundation tenet, large, complex, and costly programs-of-record needing front-end guidance (especially TSAT). But, as per a major theme of this study, "it's all about the information" when targeting combat value. It is understood that the need to re-focus priorities toward the upper layers (enterprise services, data, and applications) is being reflected in current EWSE planning.

Capability Portfolio Management as a Key Element of Governance

DOD needs to manage information technology investments as capability portfolios to efficiently and effectively deliver capabilities to the war fighter, and maximize return on investment to the enterprise. Portfolio management goals include:

- Transitioning from program-by-program investment management to end-to-end portfolio management that ensures portfolio recommendations are reflected in the JCIDS, the defense acquisition system, and the Planning, Programming, Budgeting, and Execution System processes and decisions.
- Expediting the capability to advance network-centric operations by collectively assessing net-centric transformation and synchronizing capability delivery across the department's infrastructure.
- Minimizing programmatic, technical, and operational risks by choosing the best mix of investments within the portfolio.
- Leveraging opportunities to collaborate with other portfolios to advance mission effectiveness, identify and manage interdependencies, and foster net-centricity.
- Expediting convergence toward net-centric capabilities; reducing unnecessary capability duplication; capitalizing on "best of breed" information technology solutions already fielded; and improving efficiency, cost-effectiveness, awareness, and access to capabilities and services across the enterprise.

A minimal governance regime, led by the DOD CIO and informed by GIG architecture principles and systems engineering, is required to make and oversee execution of capability portfolio recommendations. The governance regime must drive the department-wide information technology capability by aligning similar initiatives and coordinating investments, overseeing the development and deployment of the department's information technology infrastructure, and rigorously enforcing policy and decisions with attention to execution and accountability.

As recommended above, system engineering should focus on war fighting capabilities, and concentrate on the key specifications for the GIG core and the interfaces to the tactical enclaves at the edge. Systems engineering informs the capability portfolio management process by describing the technical issues and trade-offs, and recommending courses of action.

To resource the transition to a net-centric environment, opportunities to reduce operations and maintenance expense must be identified. Operations and maintenance costs to support disparate, non-compatible information technology systems grow significantly over time and are hidden in the undefined operations and maintenance cost elements of the services. This means finite resources are being ever more consumed by non-centric systems. Capability portfolio management and the governance regime must generate sufficient savings to resource the needed transport, services, and information assurance capabilities.

Technical Workforce

The challenge of developing enterprise-wide information management (and more broadly, GIG) capabilities is great, given the complexity and scale of the deployed capabilities. This requires a highly competent technical workforce on the part of DOD. Over the years, the technical depth of DOD's workforce has decreased. The problem is further compounded by the facts that skills in new technical areas are needed for information management (and, more generally GIG) development and more rapid development is required. Advanced information technology and information management skills, as well as development velocity, are much more in evidence in the commercial sector than in the DOD.

Recommendations: Governance

USD (AT&L) and DOD CIO establish effective net-centric governance:

- aggressively implement comprehensive capability portfolio management (such as requirements, resources, acquisition, testing, operations, and sustainment)

- re-orient enterprise wide systems analysis and engineering:
  - to focus on war fighter capabilities and performance metric development
  - to concentrate on informing the capability portfolio management process
  - on key specifications for the core and interfaces to the edge
  - to establish and assess key performance versus assurance trades

The Under Secretary of Defense for Personnel & Readiness develop a strategy to establish an adequate technical workforce to deliver net-centric capabilities. Particular objectives to be accomplished by this strategy should include:

- Establish a small cadre of world-class experts within government to develop the net-centric technical vision and implementation plans. Attracting such individuals from the commercial sector for career employment in DOD would be difficult. However, rotating individuals in from that sector (such as for three years in a Defense Advanced Research Projects Agency (DARPA)-like model) could prove feasible because the opportunity to work the unprecedented technical challenges confronting DOD without permanently giving up their commercial employment could be attractive.
- Ensure DISA has the necessary staff and expertise to execute its increasing role in developing and operating net-centric capabilities. Since DISA reports to the ASD (NII), it should play a lead role in determining and advocating the need for the staff required at DISA for its mission.
- Ensure adequate systems analysis and engineering expertise to determine design trades and conduct technical analyses. Significant systems analysis and engineering expertise exists across the DOD components. DOD leadership (particularly the USD [AT&L] and the DOD CIO) should work to bring this expertise to bear in as collaborative a manner as possible to address enterprise needs affecting information management

(and the GIG as a whole), and augment this workforce with new staff as necessary.

Providing an adequate number of technical operators and training for those personnel for running deployed capabilities. The services and agencies would be responsible for providing personnel and their training to support the needs of the combatant commands for the operation of both networks and services.

Current Key Programs

In reviewing the important architecture principles and construct for the future DOD information management system, the task force examined those current programs-of-record that form the principal basis for building and realizing the architecture. These programs are described as follows:

- **Global Information Grid/Bandwidth Expansion.** The GIG/BE program provides an extensive fiber-based IP network infrastructure. It is being acquired by DOD, ultimately with plans to have nearly 100 nodes operational world wide. This terrestrial infrastructure will support extremely high ("infinite") bandwidth, and forms the fundamental "inner core" backbone for the GIG transport layer. As of August 2006, this program had completed 86 nodes worldwide, and initial operational testing and evaluation is ongoing.
- **Transformational Satellite Communications System.** A large scale DOD program to extend the GIG/BE to theater POP and to provide significantly enhanced intra-theater communications. The major segments include:
  - Space. A five satellite constellation with each satellite cross-linked with laser communications as well as optical links for transfer of IS data collected by airborne platforms.
  - Mission operations. The TSAT Mission Operations System (TMOS).

- Terminals. A family of terminals for fixed ground and mobile platform use, including small dish radio frequency terminals supporting command and control on-the-move.

The program is currently following a block acquisition strategy, with Block 1 including the first two satellites and Block 2 the remaining three satellites. The first satellite is scheduled for launch in 2014, and Block 1 will have limited laser as well as radio frequency communications. The Block 2 satellites will have the full optical and radio frequency capability, with those launches starting with satellite #3 currently scheduled for 2017. Key technical issues being addressed currently that are vital to system realization include timing and tracking of the in-satellite processing router as well as acquisition and angular pointing technical challenges for the laser communications system.

- **Joint Tactical Radio Systems.** JTRS is a family of radio systems based upon software waveforms that, when implemented, will extend the TSAT point of presence to the tactical (vehicle) and individual combatant, in effect pushing the edge of the network core outward toward the individual war-fighter. JTRS radios will also provide for meshed, IP-based inter-netting among enclaves of tactical users. The key waveforms to enable this extension and associated *ad hoc* tactical networking were uniquely developed to support tactical operations. These unique waveforms are the wideband network waveform and the soldier radio waveform. In addition, the JTRS capability has an objective to include numerous legacy waveforms, and depending on the JTRS variant, would be inter-operable with potentially up to 32 different waveform types. (A decision was made to eliminate cellular waveforms from the JTRS program, thus not enabling COTS cellular handsets interoperability with JTRS.) Due to schedule issues with the JTRS program, the Army and the Air Force have been aggressively pursuing interim approaches to enable the solider radio and wideband network waveforms to be fielded immediately, particularly within SINGARS/EPLARS.

- **Network-Centric Enterprise Services (NCES).** NCES is a set of basic common software services to be operated on the unencrypted ("red") side across the GIG enterprise. These services, when fully operational, will enable information providers to post or share information, to discover other information resources, and to collaborate dynamically. Core services currently planned include collaboration, service management, storage, application, messaging, user assistance, discovery, security management and information assurance, and mediation. Plans for acquisition include, (i) buying available (mature) commercial products, (ii) adopting services using proven specifications and existing web-service technologies, and (iii) if necessary, creating new services via software development.
- **High Assurance Internet Protocol Encryption.** HAIPE is an acquisition program that provides IP-level traffic protection via end-to-end encryption, routing, and network services. HAIPE can be standalone or embedded in a host platform, and provides the functionality of protecting a node or enclave. The HAIPE program and its resultant products are expected to form a key component of the GIG information assurance architecture. Although the HAIPE program as planned does not encrypt all data (some bypassing occurs such as with signaling and quality of service bits in the data stream), the key payload information is encrypted. The current realization of HAIPE (v. 1.3.5) is already being used within the DOD, with four commercial vendors having demonstrated compliance with the government specification. By mid 2008, it is expected that the compliance standard will be 3.0, a software upgrade that will provide enhancements such as improved bandwidth efficiency, added ability to do remote upgrades, and enhanced discovery and quality of service.

Recommendations: Transport Programs

This task force purposely did not perform an in-depth review of the various applicable DOD programs of record. However, in the process of examining the overall state of progress in developing component

capabilities, the task force did extract the following observations and recommendations:

- The overall vision of moving the department toward its information management vision would be helped if the financial incentives that, in effect, subsidize voice traffic on GIG/BE would be matched with comparable incentives to encourage use of the GIG/BE for data. In addition, existing teleports can be used to extend the core for GIG/BE. The task force also encourages integration of the Distributed Common Ground System Integration Backbone with the GIG program as soon as possible.
- The task force encourages the TSAT program to develop wide field of view optical receivers to mitigate some of the acquisition and pointing issues as well as to augment bandwidth. The TSAT program should also emphasize inter-theater communications in its design and development.
- Due to the importance of achieving the key JTRS functionality and war fighter capability as rapidly as possible, the task force recommends that the JTRS program prioritize deploying the wideband network and soldier radio waveforms to key weapons and sensor links.

Recommendations: NCES and HAIPE

The task force is very concerned about the DOD's dependency on two critical programs in achieving its network-centric information management vision: NCES and HAIPE. The success of these two programs is required to achieve DOD's net-centric vision. Each program has a number of key issues that need to be resolved and therefore are highlighted separately by the task force.

Net-Centric Enterprise Services

Issue. The NCES development and delivery appear to be highly complex as currently planned by DOD. The acquisition strategy and related governance offer several areas of risk. For example, the task force is concerned about the depth of critical skills required by the

government to effectively perform source selection and subsequent program oversight in this new acquisition approach. A related concern is the complexity of governance where a single overall integrating contractor and individual service providers are all potentially operating under separate service level agreements, offering potentially confusing lines of authority and governance. An additional concern regarding the NCES is their attractiveness as an information assurance target due to their ubiquity across the enterprise and their residing unencrypted outside the black core.

USD (AT&L) and ASD (NII) must address critical Network-Centric Enterprise Services programmatic issues:

- Rapidly attain and sustain pace with commercial capabilities.
- Expand current efforts establishing a collaborative development and testing environment.
- Establish clear lines of authority and responsibility for delivery and operation, ensuring that the NCES and NECC initiatives are synchronized.
- Take special care in the design to include information assurance. NCES is not protected by encryption and, being in the "red," is a significant target. Attention must be paid to this potential vulnerability.

High Assurance Internet Protocol Encryption

Issue. There remain some difficult unresolved technical issues in the HAIPE program, such as achieving an efficient means of achieving HAIPE-to-HAIPE discovery through the black core. In addition, there remain issues with successful implementation of typical level three network services across the HAIPE functionality (such as quality of service), and, in general, of keeping pace with the state of technology in commercial networks.

USD (AT&L) and ASD (NII) must address critical High Assurance Internet Protocol Encryption programmatic issues:

- Rapidly attain the functionality to support existing and future trusted commercial network services that allow the outward expansion of the black core; and
- Continue research and development (R&D) on IP address discovery and mobile *ad hoc* networking.

Tactical Edge Networks

The architectural and programmatic considerations discussed above apply to all users within the chain of command. Particular attention, however, must be paid to users beyond the core who operate with "tactical edge" networks. These users will typically be mobile and require information management support to maintain situation awareness and to synchronize operations. Much of the information needed by these edge networks will be provided by direct exchanges among them and with immediate higher echelon headquarters, but they will also reach back to the core for some information, as well as send tactically derived information back to the core. Furthermore, much of the necessary information will not be held in some formal database but rather be derived from verbal or message accounts of the tactical environment, although that information should be posted to the core as soon as feasible.

The tactical users typically have more limited capabilities than at higher echelons. Particular factors are:

- the need to operate in a physically stressing environment
- limitations in bandwidth capacity
- restricted size and capability of display devices
- potentially frequent disconnection from the broader network

Attention is being paid to improving tactical communications. However, the particular aspects of information management to support tactical users, while critical for mission success, are a largely neglected subject.

Accordingly, the task force recommends that the services, in conjunction with combatant commanders, tailor information management to support delivery to and from the edge. Particular steps that should be taken include:

- Delivering applications that adapt delivery to tactical user bandwidth capacity and display capability. These applications would involve automatic and manual content and presentation filtering making use, for example, of metadata tagging.
- Implementing content staging to furnish information caching forward providing more timely access to the information.
- Ensuring standards-based tactical interfaces with the core to allow ready access to information in the core, as well as delivery of tactically gathered information back to the core.
- Providing ready means for reengagement of frequently disconnected users (such as services to synchronize data stores).
- Developing concepts of operations and policies for the combat information specialist and knowledge manager that explicitly take into account the needs and limitations of tactical users.
- Ensuring the survivability and reconstitution of the system both in terms of network connections, as well as in terms of information and applications (such as peer-to-peer information sharing and applications).

All these information management improvements should be made along with improved tactical communication networks, preferably through the provision of robust, *ad hoc* meshed tactical networks and peer-to-peer information and application management. For rapidity of deployment and to keep abreast of the latest technology, these tactical networks should leverage commercial technology to the maximum extent feasible.

War Fighters Need Special Combat Information Devices

Providing combat information to the edge will require innovative devices that will be low power, rugged, operate in a variety of light conditions, integrate voice and data communication, and essentially be the single portal to the tactical fighter for combat information, communication, and collaboration. This device needs to recognize the realities of the tactical environment, and thus be simple and intuitive to operate. This portal device could potentially be adapted from commercial technology, as illustrated in figure 12. Cell phones, personal digital assistants, and portable game devices should all be explored as candidates to meet this important operational need.

Figure 12. War Fighter's Combat Information Portal

The operational device should provide war fighters the following capabilities:

- voice and data communication with the core mission team as well as other entities, such as a combat information specialist, joint forces, coalition forces, and nongovernment organizations
- collaboration in support of situation awareness, planning, mission rehearsal and execution
- blue force positional information
- situation reports such as SALUTE reports
- access key status elements such as CIC and network status
- stage key mission information locally, as well as queue key communications when the network is down

For this device to be practical, it will need to have the following characteristics:

- low power
- operate in a wide variety of lighting conditions without compromising a combatant's position
- rugged to withstand the rigors of combat
- sufficient storage for staging content and queuing communications

Commercial capability can be easily and economically adapted to meet this requirement. The objective is to have these devices so inexpensive that newer generations of technology can be quickly fielded to maintain the tactical advantage and avoid technical exploitation by an adversary. The use of commercial data and communications devices to form true COTS capability within edge networks must be compatible and interoperable with the last points of presence defined by the backbone core network. These points of presence may be a TSAT, WIN-T or JTRS terminal. Tactical networks must also be capable of forward staging and caching of critical applicable data needed for specific tactical objectives.

Recommendation: Support Tactical User at the Edge of the Core

USD (AT&L) and DOD CIO, ASD (NII):

- Deliver robust, easily formed, meshed tactical networks that leverage commercial technologies.
- Deliver applications that adapt delivery to tactical users' display and bandwidth (exploit information metadata).
- Implement robust content staging to provide information caching forward to enable timely access.
- Ensure standards-based tactical interfaces with core.
- Develop unique and local security strategies.
- Resource information management staff to support tactical users.
- Reintroduce cellular waveform into JTRS.
- Analogous to the approach to the HAIPE initiative, offer incentives to the private sector to implement soldier radio waveform into the core waveform set in the commercial world—encourage the production of future commercial capabilities that meet the department's needs.
- End-user devices (such as Blackberry and Treo) are commodities, and should be acquired using commodity acquisition methods, such as the General Services Administration Schedule.

Chapter 4: Critical Information Assurance Challenges

Network/Information Assurance as a Strategic Issue

Contemporary DOD and related national security net-centric operational environments have serious current and future problems related to maintaining confidentiality, availability and integrity of information. Information assurance is a descendant of information security, an older discipline that worried almost exclusively about keeping secrets—the "confidentiality" of data. The change in nomenclature was made to accentuate the fact that there must be concern not just with the confidentiality of the data but also with its integrity and availability.

Although the nomenclature has changed, too often the emphasis remains on confidentiality. There is reason to argue that in the martial context, with the coming of net-centric operations and the unforgiving dependence on information from afar, there should be much more concern with integrity and availability. One salutary outcome of the persistent storm of attacks on the Internet is that some—the denial of service attacks, and distributed denial of service attacks—have sensitized DOD to the issue of availability.

Consider integrity, the fact that a malicious user may have changed the data, not just randomly, but according to some intelligent design. Two equally bad outcomes: one fails to notice and acts on deliberately misleading information; or, one notices and can no longer have trust in any of the data or, both happen sequentially. The loss of trust either in the ability of the system to deliver any information, or correct information is most insidious. Loss of integrity raises one of the most vexing challenges: how to restore trust in the "network" once you have lost it.

The threats to the networks and related communications, and information technology architectures and components, are neither well

appreciated nor fully understood. In particular, there appears to be a high level of naiveté among network participants about information assurance risks and issues, or even outright hostility to having to deal with information security communities and problems.

Given that the network environment is, and will continue to be, heavily comprised of COTS hardware and software, which are increasingly being developed offshore, reducing the threats to networks will be a complex, relentless, and often frustrating undertaking. Even more significantly, there are important network trends and aspirations in being able to maximize information at the edge of the network with previously disadvantaged users. In effect, the larger the network, the more points of vulnerability to the networks is introduced. Finally, the DOD acquisition system is currently not capable of keeping up with the speed of COTS, nor is there any notion of how to harness the speed of COTS (or to provide incentives for the high speed invention of COTS) to DOD's network and information assurance advantage.

Formalized Risk Management

The nature and character of both future insider and outsider risks to the network may be more pervasive then in any earlier time in DOD history, and DOD must develop strong and formalized "risk management" processes and tools to continually evaluate and define directions for mitigating the threats.

In the case of information systems, cost is determined in the marketplace, as is the case with COTS. When a potential vulnerability is pointed out, there's a tendency to balk at the "exorbitant" cost of hardening that capability—the true cost of information assurance.

Further, there is a myriad of known vulnerabilities and an endless supply of bad actors. Too little insight into their actual motives and capabilities, doctrine, tactics, techniques, procedures, and their "political will" is known. This is especially true with respect to the more-to-be-feared high-end adversary, generally state-sponsored, well-resourced, and highly disciplined—unlikely to mindlessly reveal their true capabilities and intentions. These parameters, quantitative costs, and

values are essential to rational risk management. Presently, DOD does not have a good handle on them.

Threats

As dependence on networked capabilities grows, along with the ability to demonstrate improved military capabilities, adversaries will become increasingly motivated to attack information infrastructures. Dependence is, perhaps, the ultimate asymmetry and it has not escaped notice. There is ample evidence that U.S. adversaries have recognized this potential vulnerability and are aggressively developing doctrine, tactics, and technology to attack this soft underbelly.

Therefore, to leverage the net-centric operational advantages with high confidence, an adversary's capabilities, intentions, and specific targets within the GIG and extended networks must be deeply understood. Insight into an adversary's offense is a necessary but not sufficient condition for performing effective risk management. Equally important is to understand the effectiveness or shortcomings of various defensive tools and approaches in mitigating an adversary's operations.

There are several factors that contribute to the complexity and criticality of balancing the utility of net-centric and consequence of compromise. First, current dependency on information technology infrastructure is extremely high and the dependency of the envisioned net-centric architecture will be significantly greater. This increasing reliance provides an escalating motivation for an adversary to target elements of the architecture. There is growing evidence that many adversaries will recognize this vulnerability as an asymmetric opportunity and will develop strategies, organizations, and associated capabilities to target these systems.

Second, a significant and increasing percentage of the technology used to build these systems is COTS. Even if this technology is acquired from U.S. companies, the provenance of the technology is increasingly foreign. The complexity of both the microelectronic and software components is enormous. Consequently, the challenge of discovering malicious constructs introduced by an adversary through

these life-cycle opportunities is exceedingly difficult. As will be shown, this aspect alone provides considerable benefit to an opponent.

Finally and closely related to the dependency issue, the impact of a defensive failure (confidentiality, integrity, or availability) is enormous and will likely grow to unacceptable levels unless mitigating strategies are discovered and employed. Alternatively, new approaches (war modes and hedging, for example) and architectures can be developed such that the compromise by an adversary will have reduced impact.

With these factors in mind, can these adversarial advantages be sufficiently offset to warrant the desired benefit? This task force concludes that the current state of the defense will be considerably outmatched by a sophisticated, well resourced, and motivated opponent. To more deeply appreciate the basis for this conclusion, a characterization of such an adversary is needed.

A sophisticated and effective intelligence organization, intent on conducting aggressive and modern espionage operations against its opponent's end points, will possess many of the following capabilities and characteristics:

- worldwide presence
- mature operational tradecraft (allows for full and non-alerting integration of case officers, assets, and technology into the target environment)
- diverse network of trusted foreign and domestic partners
- worldwide secure communications and logistics
- integration of human and technical operations (mutually supportive)
- effective security and counterintelligence program (keeps its operations and assets secret)
- mature mid-point collection
- integration of offensive and defensive missions (mutually supportive)
- comprehensive training program for all aspects of business

Figure 13 illustrates how an adversary possessing these capabilities can meet its offensive objectives across a broad spectrum of targets. A common misperception of the threat to information technology systems is based upon an adversary utilizing a small portion of the tools available to them. This is largely based on the everyday view of hacker-related exploits on the Internet. Unfortunately, an adversary has a very rich array of tools to use: surreptitious entry, spies, signals intelligence (SIGINT), clandestine technical collection, and cyber attacks. The synergistic and mutually supportive nature of these tools, in combination with the factors discussed above, can yield powerful offensive results.

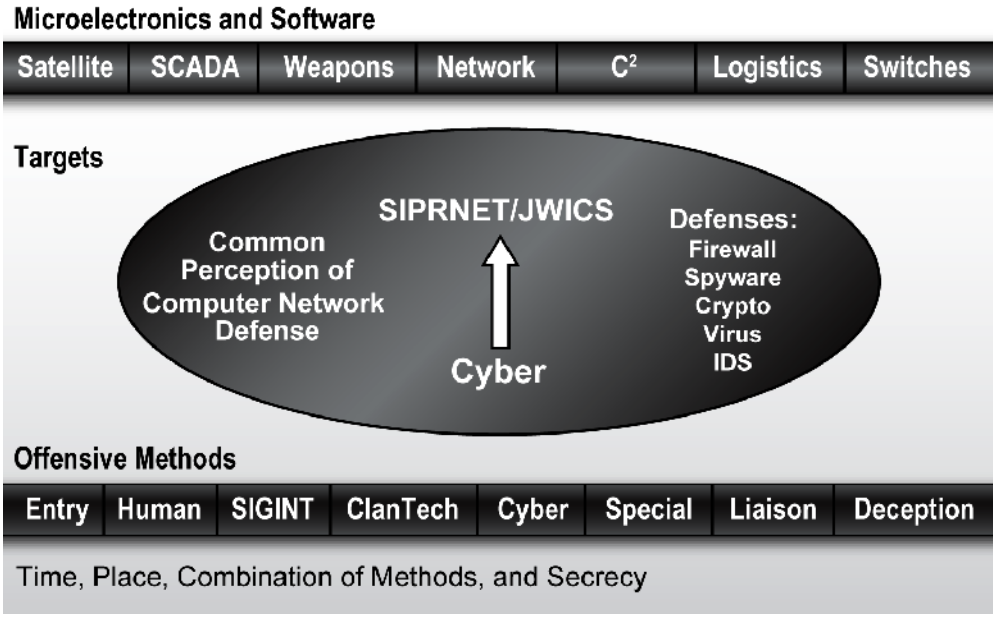


Figure 13. The Information Assurance Threat and Computer Network Defense[9]

9 For a more comprehensive treatment, see James R. Gossler, "The Digital Dimension," in Sims and Gerber, *Transforming U.S. Intelligence*, Chapter. 6, pp. 96–114.

With this context, the defensive challenges are daunting. New and well-resourced approaches must be developed to offset these offensive advantages. As will be shown, the innovative application of offensive techniques to support defensive objectives shows great promise.

The Insider Threat as a Priority Case. The information age insider threat can not only conduct espionage, the insider can also dramatically and broadly threaten the functionality of networks. It is important to focus on the insider threat as a priority, and ensure that the network quickly points at security violations by insiders.

Information Assurance Strategies. Maintaining an enduring, highly functional, and assured network-enabled environment is fundamentally strategic to managing the information, situational, support, and command dimensions of conflict in the 21st century. DOD will have total dependence on these networks for virtually every aspect of national security administrative and operational wartime tasks. The current mixed strategies of simultaneously working with COTS to reduce overall vulnerabilities (by increasing *protection*) while also strengthening monitoring, detection, analysis, and *responses* on the network may not be sufficient assurance in the face of the capable adversary, nor the best approach for the longer term. More detailed strategies need to be devised that *combine* offense, defense-in-depth, and deterrence and dissuasion options into combined effects for information assurance. Steps have been taken to think about and test the validity of these strategies in the context of now, next, and after-next temporal domains.

Defense-in-Depth. Defense-in-depth is the first line of defense against network vulnerabilities. The following lists the components of a credible defense strategy:

- strong leadership and governance oversight, processes, and investment
- a logically separate network (isolated from threats) to provide order wire, key distribution, and support for restoral functions
- run-faster acquisition that allows responsive and pervasive insertion of the latest COTS in order to present a constantly changing target environment to the adversary

- a robust and diverse set of government, industry, and academic R&D programs focused on high-leverage information assurance solutions and offerings such as identity, encryption, hardware and software assurance, security tagged architectures, and deep packet inspection
- hedging strategies and technologies for the future
- making the networks behave differently in combat
- protection of hardware and software supply chain
- establishment of a TargetNet/TestNet environment for designing, developing, testing, and exercising attack, defend, and exploit capabilities
- development of new security and sharing concepts that simultaneously maximize the provision of information while simultaneously protecting sensitive sources and methods

Deterrence and Dissuasion. Attacking U.S. information systems is undeniably attractive to adversaries. It represents the one chance to level the playing field, and if sufficient chaos is created, it can perhaps tilt the playing field in the adversaries' favor. All efforts must be orchestrated toward deterring any would-be opponent, mischief maker, or malicious bystander to execute such attacks, and if they do, ensure the ability to "fight through" and prevail. Adversaries need to be assured that their attacks against U.S. information systems will be detected, that U.S. functionality will be restored, and that there is the capability to operate securely with requisite system availability and integrity in degraded and wartime modes. More importantly, an adversary needs to know that the U.S. possesses powerful hard and soft-kill (cyber-warfare) means for attacking adversary information and command support systems at all levels. Deterrence and dissuasion strategies relate to:

- intrusion detection and attribution
- disproportionate response options and adversary consequences
- use of wartime modes
- managing the fight when under attack and operating in degraded modes

The utility of any information-managed net-centric system will be directly related to the confidence users have in the reliability and quality of the service. There is no approach that can guarantee that any system of the type being proposed and procured can be completely secure and all functions performed with 100% assurance. The price of introducing progressively higher levels of assurance is to induce greater cost and diminished functionality. It is inherently a risk management system of trade-offs and compromises for which there is no magic formula. The *greatest degree of assurance for the net-centric system that is being created can only be achieved by a balanced strategy*. A balanced strategy is one that places emphasis on sound defensive measures and an aggressive, sustained, and highly secure offensive program. The system that is sought will not have credibility with the users or potential adversaries if one is done without the other.

Every potential adversary, from nation states to rouge individuals, could be targets of an integrated offensive capability. Adversaries should be forced to invest in their own security; and should be compelled to consider the consequences of an attack on U.S. systems resulting in highly undesirable consequences to their own security. U.S. offensive penetration of an adversary's information systems, both offensive and defensive, is the essential ingredient in achieving an indication and warning capability.

Stratified Network Design

Intelligent Design

The network-centric information management system is based on the Internet design—initially the design of the ARPANET. It is a deliberately "flat" network. Every entity on the network—every node, every switch, every piece of subscriber equipment—has an IP address. This is a design that allows every communicant full access to their IP address. This is quite different from the model of the plain old telephone system where the telephone number is not yours to manipulate. In IP networks, subscribers can effect (and, thus, affect) the switching and signaling (the routing and/or apparent routing) of information. In other contexts, this attribute is referred to as "in-band signaling."

Security and Control "Over-Net"

There are compelling reasons to want to take certain information and information services—network and security management services, in the broadest sense—out of band. That is, some things should be out of the grasp of subscribers, who have no legitimate need to touch them. The premise is that the most likely entry point for an evildoer is through the subscriber network, if, for no other reason than the "circle of trust" is bigger. Whether an insider or an intruder, the mischief should be localized with a substantial, additional barrier in the way of seizing, disabling, or corrupting the network. Other, more traditional processes, such as authentication and compartmentation, should limit the extent of any breach in confidentiality and, so, could profit from being less accessible to ordinary subscribers. Incidentally, it is likely that the underlying security services that enable identity management, also should ride the "over-net" and not the base subscriber net.

It is clear that the DOD, the original force behind the Internet, would be best served if such a stratified control layer used commercial equipment and software. More importantly, it would be most beneficial if the protocols became the (international) commercial standards, just as occurred with the Internet. In fact, it would be ideal if commercial service providers adopted the same control layer notion. It is, therefore, highly recommended that the developers work from the outset with major vendors and national and international standards bodies. In this sense, it's believed that, having done it with the Internet proper, DOD can once again "invent COTS."

The Information Assurance Battle Management Layer

Such a stratified network might also be used to manage the information assurance battle space, to provide situational awareness, command, and control of dynamic defense and, perhaps, offense—that is, a protective reactive strike. Some consideration might also be given to using such a network for the most critical command and control—nuclear, for example—or its backup and/or recall. However, caution should be applied: the more general-purpose this strata

becomes, the more nodes and users, and the more diversity, the more likely that it will lose its stratification.

Before extensive acquisition or deployment, a great deal of attention should be given to developing the concepts of operations for the layer. to flush out any serious information assurance concerns such as those expressed above. This should also allow for a decision to be made about how to operate the control layer—such as a layer for each level (JWICS, SIPRNET, and NIPRNET), or one control layer that restores, JWICS which, in turn, is used to restore SIPRNET, and so on. It is unlikely that one-control net acting across all three levels is desirable.

Elsewhere, it has been argued that the network is a critical combat system. This concept ties nicely to the notion that the stratified network control layer or security OverNet is the network battle management layer. As such, it should become an increasingly important part of the fight and should, therefore, be integrated into other command post functions. This will be especially true if there is movement towards an active defense of the network.

A good test bed might be the Army's Command Post of the Future, an executive level decision support system providing situational awareness and collaborative tools to support decision making. Situational awareness and key management functions should be accessible to a commander and fully integrated into his CIC. These network activities should integrate more like the way that logistics and transportation service providers integrate into the commander's business management space.

Information assurance is the high risk, long pole in the network enablement tent. Moving toward an acceptable level of assurance for DOD and related national security information is a supremely difficult and complex task. This area has been dramatically under-resourced, and the governance, oversight and organizational structures have been weak given the high stakes. There also needs to be a dramatically improved understanding of the threats and vulnerabilities by the users of the systems.

To achieve an acceptable level of assurance, red, blue, and green teaming needs to be strengthened. In addition, exercises, strong test and evaluation, and better concepts of operations need to be pursued. The success of such activities requires a viable and responsive, even an animated design, development and test environment, involving operators in activities where the network is degraded or non-functional, challenging restoral organizations with continuous wartime scenarios for managing the network in degraded modes and when under attack. DOD needs to ensure a holistic view of networks, so that the NII, joint, and agency programs of record are fully harmonized and synchronized with service programs, and those of the key allied partners. Equal attention needs to be paid to the plug and play nature of the applications layer, sitting on top of the services and transport layers for high speed insertion into the network, but ensuring expedited addressing of applications layer information assurance issues.

Architectures, Building Codes, Standards, Systems Engineering and Integration (especially at the enterprise level), Certification and Accreditation. Finding the proper balance of individual and collective focus and energy on each of these critical dimensions of network and information assurance acquisition is one of the most critical aspects of successful network design, development, and deployment. Deploying and continually upgrading operationally responsive network environments is the prime objective for DOD. A premium needs to be placed on maximizing the building codes, standards, advanced systems engineering, systems analysis, and the rapid certification of the information assurance aspects of network deployment.

Managing Partnerships. Relationships with DOD, the Director of National Intelligence (DNI), science and technology organizations, industry, laboratories, academe, and even foreign R&D organizations and activities need to be aggressively pursued and offered strong incentives. In particular, DOD needs to ensure that industry and academe have the requisite operational, network, and information assurance domain knowledge to make viable contributions in this strategic technology area.

Focusing on the Information, Information Sharing, and Security Reform. The DNI office has recently published an

Information Sharing Plan. The plan contains objectives, guidance, and processes, and stipulates actions, but does not describe specific detailed approaches and methods for maximizing sharing (while simultaneously protecting sources and methods). Providing better guidance on how information is to be shared will be the next major thrust of the DNI Information Sharing Office. It is important that such efforts be pursued aggressively, so that the information has assured delivery to all classes of customers, while the most sensitive aspects of the data are protected from both insiders and outsiders.

More important, information age challenges including information assurance require new security frameworks and thinking. The need to have a top level review of U.S. security policy and organization for the 21st century has been previously recommended by the Defense Science Board, as well as national commissions, but no national review effort has been tasked either by the executive or legislative branch. Such an effort is overdue.

Recommendations: Defense-in-Depth and R&D Agenda

Defense-in-Depth: Governance

- ASD (NII) should evaluate the information assurance funding over the Future Years Defense Program, focus on information assurance for the entire enterprise and increase current funding where appropriate.
- DOD CIO should establish responsibilities and authorities for end-to-end information assurance and security design.
- DOD CIO must formalize overall governance, systems engineering, and risk management enterprise-wide to focus on information assurance.
- STRATCOM and JFCOM should devise an information assurance battle management doctrine and tactics, techniques, and procedures.

Defense-in-Depth: Information Technology COTS Insertion

DOD CIO, ASD (NII), and USD (AT&L) must:

- Establish plans, policies and procedures for acquisition of COTS information technology systems from an information assurance perspective, which includes identifying and establishing information technology hardware and software provenance.
- Manage processes for rapid information technology insertion from a mission assurance and risk management perspective.
- Align and combine rapid acquisition processes and system engineering, certification, and accreditation activities.

Defense in Depth: Security Over-NET

ASD (NII) and USD (AT&L) should establish a defense-wide program to design, build, and operate an isolated network to improve GIG information assurance capabilities:

- hardening—out-of-band" critical signaling
- restoring trust—assured "order-wire" for reconstitution
- re-keying—assured critical key distribution

NSA, with DISA and the National Institute of Standards and Technology, should encourage commercial industry to incorporate new security architecture and design principles within evolving COTS networks:

- protocols and building codes
- international standards
- market development

Research and Development Agenda

DOD needs to cast its R&D net far and wide, and focus on those existing and potential high leverage information assurance solution areas, and move them more rapidly to the network market. The task force believes there are several powerful un-evolved areas that need attention:

DDR&E and STRATCOM develop research agenda to include:

- security usability
- self-aware networks
- adaptive networks
- detection and diagnosis
- deep packet inspection, intrusion detection system
- new design principles (resilience)
- hardware and software assurance
- static and dynamic analyses
- identity and access management
- formalized information assurance risk management
- security metrics
- encryption, public key infrastructure, digital signature
- security-tagged architectures, trusted platform model
- wireless security and performance
- dealing with adversary recovery of friendly information technology on the battlefield
- enhance information assurance at the data level

A classified annex to this report deals with certain aspects of threats, information warfare and information operations, wartime modes, making COTS behave differently, and hedging strategies and technologies for preventing exploitation of adversary recovered network components.

Chapter 5. A Critical Defense Weapon System

Combat operations, anticipated scenarios, and adversary actions require a new Combat Information Capability This capability will be an enormous operational advantage for the war fighter. A CIC must be resourced, managed, and protected as a critical defense weapon system. Today information management systems tend to be managed more as a technology asset and curiosity than as a critical defense weapon system.

Commanders need to have the responsibility and authority that will allow them to take control of both their information and the associated infrastructure. Only after commanders are empowered can they move forward with developing the tools and processes to control this critical capability.

In addition to empowering commanders, there is a need to develop effective leaders that can lead in a net-centric environment. A net-centric leader must do more than simply be knowledgeable about information systems technology. They need to be leaders in the information age, which means they need to understand all aspects of how information can be used to provide a competitive advantage to their forces. One of the interesting aspects of unleashing information in an organization is that it will have the effect of flattening the organization, which usually creates a more rapid response entity.

One of the elements that need to come with a critical defense weapon system is an effective and robust training capability. The training cannot simply be to a fixed set of processes, but instead needs to focus on the principles of information management that will support flexible processes. This training needs to be connected with realistic operational exercises; therefore it is not simply an academic activity but one that will prepare the war fighters for combat.

In addition to the preparation of the personnel, another aspect of a critical defense weapon system is operational performance. Operational management must include the ability to monitor the status of the system, to establish operational priorities and trade-offs, to detect and deny intrusion, and evaluate performance based on a set of operational metrics.

Another element of a critical defense weapon system is the identification and development of the set of the tools necessary for daily operation. This set includes tools such as a help desk to support a wide range of users, tools for backup and restoration of the database, and network diagnostic tools. The combination of these tools with corresponding policies, doctrines, and procedures compromise a complete system operational management approach. Part of the day-to-day management of the system is the collection of new requirements that emerge from innovative uses of the tools. Many of these requirements can be satisfied with the development of new techniques and procedures. However, occasionally these requirements will require developmental activities. To accommodate both the emergent and new development requirements, an innovative governance and acquisition process must be put in place that will allow this CIC to keep pace with commercial technology. Instrumentation should be put in place to provide analysts the ability to monitor and understand how the system is being used and the impediments to reaching its full potential. Finally, in addition to a day-to-day systems management process, a longer term review process to assess progress and adjust strategic direction should be put in place.

Operating with Degraded Systems

Commanders at all levels must be prepared to operate with degraded information systems. Reduced network capacity may be the result of denial-of-service attacks or other combat actions. Corrupted data may be caused by network penetration or insider action.

For the tactical commander, operating with degraded systems (weapons, communications, logistics, maneuver) is not an anomaly but the norm. It is this defining quality of the tactical environment that requires modifications to the current deployment of net-centric

capabilities. Any solution to the challenges at the tactical level must start with the nature of the tactical environment and not the nature of the technical challenge. Two significant concerns voiced by tactical commanders when talking about leveraging the power of information fall into the category of redundancy and robustness.

The redundancy of the network and the critical data that rides on the network is a key attribute given the immediacy of enemy actions, the environment, and even unintentional errors. A practical, current understanding of how the various networks are working together and what options exist to restore or work around failures is a key requirement for commanders on a net-centric battlefield. Attention must be paid to the development of cueing capabilities to monitor and notify of intrusion and data corruption.

Robustness of the information systems employed is required for more than the obvious redundancy implied in the engineering sense of the term. A system that is robust will empower tactical commanders by instilling confidence that the information systems are every bit as capable as other tactical capabilities.

Commanders need cyber warfare capabilities to deal with an adversary's attempts to deny the unit's information capability. Defense operations require trained, skilled cyber warfare specialists and leaders who understand cyber warfare. The commander needs to take offensive cyber actions to protect the unit's capability and to adversely affect the adversary's capability. For example, the response to a penetration could be to steer the attacker into a honey pot for deception.

Commanders must develop concepts of operations; tactics, techniques, and procedures; and contingency plans to ensure that combat operations will continue with degraded information capabilities. Commanders need the necessary network status information to make risk-managed decisions about mode of operation, including available capacity, estimated extent of adversaries' penetration, corrupted information, prioritization of decreased capability, and implementation of planned degraded operations.

Combat units need to exercise regularly in degraded modes and use calibrated red and blue teams to understand the effectiveness of contingency plans.

Recommendation: Net Operations

STRATCOM must:

- improve the Joint Task Force-Global Network Operations center to world-class management capability
- develop and monitor performance and readiness metrics
- develop robust and redundant capabilities and operational procedures for information assurance
- enforce network management standards across the enterprise

Operators Need a System Test Environment

Operators need a realistic GIG architecture test environment to permit the testing of proposed new systems and applications, permit red and blue teams to examine potential attack and intrusions of the system, and test defensive and offensive information assurance approaches. This system must be capable of assessing the trades among performance, information assurance, and cost. It is recommended that the test environment include a range of options from virtual table top experiments, to simulation capabilities, to live real-world field exercises for operational testing and training.

Such a test environment has significant advantages of flexibility, speed, and completeness. It will permit system engineering analysis of the operational capability of the system under different configurations, with the addition of new commercial capabilities before they are added, and in degraded modes.

Recommendation: Test Environment

STRATCOM must establish a robust GIG test environment to examine the trades among performance, information assurance, and cost. Specific actions include:

- DOD CIO identify and prioritize emerging information technology and information assurance capabilities for testing.
- JFCOM create network operations and information assurance learning and training experiences.
- Combatant commanders conduct operational exercise tests and mission rehearsals.
- STRATCOM, NSA, and DISA validate and exercise a risk management system.
- STRATCOM and JFCOM identify and resource requirements.

Operate Effectively with Partners

One of the defining aspects of today's military environment is that it has moved well beyond simply joint service operations. Today's operations are fully integrated with key interagency, state, and local government; alliance; coalition; host nation; international; and nongovernmental organizations. Each of these actors generally operates on its own distinct network. Although sustained operations during the past decade in the Balkans, Iraq, and Afghanistan have led to the development of tools and arrangements for information sharing and collaboration, these efforts have typically been *ad hoc* and have not allowed for the true integration of all elements of national and international power.

Because future contingencies will almost certainly require the collaboration of U.S. forces with interagency, coalition, and nongovernmental actors, DOD must work to improve and institutionalize its ability to work effectively with partners in all stages of combat, stabilization, and reconstruction. CENTRIXS, for example, has been the vehicle for collaboration between U.S. and coalition forces during Operations Enduring Freedom and Iraqi Freedom. CENTRIXS

has been successful in many ways, but it is limited because it does not address information sharing with non-military partners, and it will not allow for U.S. and coalition forces to plan and operate on the same network. Although it is vital for operational security reasons that U.S. forces maintain this firewall between U.S. military networks and the networks of coalition and non-military partners, it is equally vital that the department work to find ways to improve the current situation in this area. Technical solutions will be helpful in this regard, but policy and process solutions are likely to be of equal or greater importance.

Recommendation: Interaction with Partners

DOD CIO develop policies and practices necessary for information sharing outside U.S. military (U.S. government agencies, allies, coalition, nongovernment organizations):

- clarify release authorities and amend as necessary
- define standards and best practices for information sharing and collaboration in both classified and unclassified domains
- provide for rapid stand-up of information sharing and collaboration following onset of a contingency

Critical Defense Weapon System

The most significant recommendation of the task force is for the Deputy Secretary of Defense to recognize the importance of the CIC as an essential combat capability and declare it as a critical defense "weapon system." This means that the essential elements of the CIC will be planned, programmed, and resourced as a weapon system like other weapon systems. The CIC weapon system must be built to degrade gracefully when attacked. The assumption is that the GIG and the network operations to the HAIPE will be provided as planned and the weapon system, which includes support of the war fighter in the theatre, will be provided in a single portfolio.

This proposal is similar to the Air Force decision to recognize the Combined Air Operations Center and its extended elements as a weapon system. Then the manning, equipment, training, exercise, R&D, and other elements are programmed, planned, and resourced. The

consequence has been a more combat-ready capability and planned improvements over the period of the Future Years Defense Program.

A significant challenge will be to decide what programs will make up the weapon system elements. The communications and information management capability required in the battlefield should be part of the weapon system. The proposed information management support elements, such as combat information specialists, knowledge managers, and subject matter experts should be included. Particularly, the support for the war fighter outside the HAIPE should be included.

Given the scope and complexity of the total DOD information management system and its critical importance to U.S. combat capability, a comprehensive strategic plan is needed. This strategic plan is necessary to guide the development of a Combat Information Capability including:

- required resources
- timeline for key milestones for implementation
- addressing the major actions required to develop a Combat Information Capability
- training commanders to effectively command and control information management infrastructure and capabilities
- exercises and experiments for realistic operational scenarios
- information organization and access objectives
- doctrine for combat information capabilities
- a formal information assurance risk management system, model, and associated metrics
- education and training programs, including information management
- research on advanced information concepts
- lessons learned from current operations

This plan must be considered a living document and periodically updated as the threat, commercial technology, and other factors change that affect its capability and performance.

Because so much of the combat information requirement can be satisfied with existing and planned ISR capability, there is a need to develop a joint requirement for dynamic, integrated command and control of ISR assets. This capability can optimize the allocation of all ISR resources and lead to more robust sharing of tactical combat information. An essential part of building this capability is to incorporate the need for space platform visibility tools and ground segment improvements into this requirement.

Recommendation: Strategic Plan

The Chairman, Joint Chiefs of Staff should develop a CIC strategic plan that provides:

- commanders with the ability to command and control combat information capabilities
- staff capabilities to implement combat information management
- network operation, upgrade, and testing strategies
- experimentation, training, and exercises
- a formal information assurance risk management system, model, and metrics

Recommendation: CIC as a Critical Defense Weapon System

Deputy Secretary of Defense designate the Combat Information Capability as a critical defense weapon system.

Chapter 6. Conclusion

As this study evolved, it became clear that, given the way this system is to be fielded, *the Combat Information Capability must be treated as a critical defense weapon system*. It requires, therefore, a different mindset about how it is used, managed, and protected.

The evolving national security scenarios described earlier in this report demands increasingly distributed, dynamic operations. Whereas the network/COTS approach and strategy certainly enable new paradigms for sharing and using information, this capability also has the potential to significantly *increase* the nation's vulnerability to internal and external threats. It becomes a very attractive target for U.S. adversaries.

Therefore the task force members believe that the system and its capabilities will always be under attack and, as a result, will always be operated in either a degraded or compromised mode. Commanders need to understand this and know how to operate under this scenario. There are significant information assurance issues and risks that this CIC will be attacked, degraded, or compromised, and this risk must be resourced and managed accordingly.

One significant implication is the DOD needs a new, innovative acquisition strategy to take full advantage of the rapidly evolving capabilities of a true-COTS system.

The findings and recommendations of the task force can be distilled to three points:

- **DOD Combat Information Capability must be treated as a critical defense weapon system.**
- **Information assurance for this critical capability is critical and must be resourced and risk-managed accordingly.**
- **An innovative acquisition strategy is required to leverage true COTS information technology.**

Appendix A. Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

MAR 15 2006

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT - Terms of Reference - 2006 Summer Study on Information Management for Net-Centric Operations

The United States military steadily transformed during the latter part of the 20th century by an ever increasing reliance on information networks and their ability to provide wider access to information and to support collaboration. Impressive gains in the usability, usefulness and availability of all forms of information have improved the effectiveness of military operations. Our increasing ability to leverage information and networking will be a critical enabling factor in developing better ways to work with others in the USG and with both coalition and non-traditional partners as we, collectively, undertake the challenging missions of the 21st Century.

Today a Company Commander can control a Division's worth of firepower, tagging and tracking systems promise to significantly improve the logistics chain and the improved availability of intelligence information and greater connectivity between sensors and shooters has increased the effectiveness of our forces and enhanced their security. During the past ten years, we have seen the evolution of military missions driven by adaptive adversaries who recognize our increasing dependence on information networks. Going forward, transformation must focus on addressing the stresses imposed by 21st Century mission challenges associated with stabilization and reconstruction operations in urban and unconventional environments and responses to unforeseen events with catastrophic consequences. Information and the ability that networks provide to make this information available to those who need it, as well as the ability for individuals and organizations to collaborate, are the lifeblood of military and civil-military operations. The quality, reliability, availability, timeliness, discoverability, relevance, and security of information and interactions among individuals and organizations across the enterprise (warfighting, with business and intelligence support) will have profound consequences for successful mission execution.

To date the transformation of the DoD enterprise has focused on improved connectivity, interoperability, and information sharing among disparate joint forces and systems. Future challenges and the need to maintain adequate levels of security, integrity, and reliability will place new demands on our information networks, processes and personnel. As new users demand more information and adaptive information sharing, improved knowledge utilization and better tools for information discovery will become critically important. "Googling" and "blogging" are making their way into military operations at all levels, but the full implications of this revolution are as yet unknown and we have no clear direction and defined doctrine.

You are requested to form a Defense Science Board Summer Study assessing the Department's strategy, scope and progress toward achieving a robust and adaptive Net-Centric DoD Enterprise.

The Summer Study should:

- Examine the operational value enabled by networks and networking and their impact on innovations across the Enterprise. Assess the implications of new and innovative approaches to command and control structures, capabilities, and processes, including interagency, coalition, and non-traditional participants, the need for greater adaptability and the emergence of new missions such as counter-insurgency, stabilization and reconstruction operations, counter-WMD, and catastrophic disaster support.
- Evaluate the underlying framework, architecture, processes and organizational structures that are in place or being pursued to deliver the power of information to the DoD enterprise as well as potential external partners. Explore Enterprise Wide cost/risk trades between bandwidth, quality of service, network availability, network security, information integrity, information sharing, and collaboration.
- Assess the state of the art in knowledge utilization. Particular attention should focus on information discovery, sharing in a secured networked environment, visualization and collaboration. How are emerging techniques being incorporated into operations both in the near and far term. How is information being turned into knowledge and then coordinated action as quickly as possible?

The study will be sponsored by me as the Under Secretary of Defense (Acquisition, Technology and Logistics) and the Assistant Secretary of Defense (Networks and Information Integration). Mr. Vincent Vitto and Dr. Ronald Kerber will serve as the Summer Study Task Force Co-Chairmen. Mr. John Mills, OASD (NII), will serve as the Executive Secretary. LTC Scott Dolgoff will serve as the Defense Science Board Secretariat representative.

The Task force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

Kenneth J. Krieg

Appendix B. Task Force Membership

CHAIRMEN

Name	Affiliation
Dr. Ronald Kerber	Private Consultant
Mr. Vincent Vitto	Draper Laboratory

TASK FORCE MEMBERS

Dr. Milton Adams	Draper Laboratory
Dr. Shawn Butler	MSB Associates
Mr. Edward Carney	Cisco Systems, Inc.
Mr. John Dahms	Lockheed Martin
Dr. Craig Fields	Private Consultant
Mr. Scott Fouse	ISX Corporation
Mr. Greg Gardner	Oracle
Mr. James Gosler	Sandia National Laboratory
Ms. Carol Haave	Private Consultant
Mr. Richard Haver	Northrop Grumman
MajGen John Hawley, USAF (Ret)	CollaborX
Dr. George Heilmeier	Private Consultant
Dr. Richard Ivanetich	Institute for Defense Analyses
LTG Keith Kellogg, USA (Ret)	CACI
Dr. William LaPlante	Johns Hopkins Applied Physics Laboratory
Dr. Robert Lucky	Private Consultant
Dr. Joseph Markowitz	Private Consultant
Dr. Mark Maybury	MITRE Corporation
Gen James McCarthy, USAF (Ret)	U.S. Air Force Academy
Dr. Jerry McGinn	Northrop Grumman
Dr. Dawn Meyerriecks	America Online, Inc.
Hon. Art Money	Private Consultant

Mr. Robert Nesbit	MITRE Corporation
Dr. Robert Popp	Aptima, Inc.
Mr. Lawrence Prior III	SAIC
Mr. John Quilty	Private Consultant
LtGen Harry Raduege, USAF (Ret)	Deloitte & Touche, LLP
Mr. Rocky Roccanova	Rock and Nova, Inc.
Mr. Larry Sampler	Institute for Defense Analyses
Hon. John Stenbit	Private Consultant
ADM William Studeman, USN (Ret)	Private Consultant
Mr. Alan Wade	Private Consultant
Mr. Kevin Woods	Institute for Defense Analyses

EXECUTIVE SECRETARY

Mr. John Mills	OASD-NII

DEFENSE SCIENCE BOARD REPRESENTATIVE

LTC Scott Dolgoff, USA	Defense Science Board Secretariat

GOVERNMENT ADVISORS

LtGen Bruce Brown, USAF (Ret)	ODoD CIO
Ms. Ann Carbonell	National Geospatial Intelligence Agency
Mr. Tom Gaetjen	JS J-6
Mr. Richard Hale	DISA
Mr. Mike Krieger	ODoD CIO
Mr. Robert Lentz	ODoD CIO
Mr. David Mihelcic	DISA
Ms. Cecilia Phan	JS J-6
Mr. Michael Ponti	OASD NII
Mr. Tony Sager	NSA
Mr. Thomas Scruggs	ODoD CIO

STAFF

Dr. Heather Davies	Strategic Analysis Inc.
Ms. Julie Evans	Strategic Analysis Inc.
Mr. Anthony Johnson	Strategic Analysis Inc.
Mr. Theodore Johnson	Strategic Analysis Inc.
Dr. Philippe Loustaunau	Strategic Analysis Inc.
Dr. Adrian Smith	Directed Technologies, Inc

Appendix C. Presentations to the Task Force

Name	Topic
MARCH 20–21, 2006	
Operator's Panel Group 1: COL Ralph Baker, Col Jagusch, MAJ Lynne Schneider, MSG Larry Riddle, Col Tucker, LTC Dave DesRoches Operator's Panel Group 2: LTC RD Douthit, LTC Sean Corrigan, MAJ Bob Castro, SGM Mike Hoover	Operators discussion panels
Mr. Ryan Paterson	Command Post of the Future
RDML Arther Brooks, NORTHCOM	Net-Centric Operations in Defending the Homeland and perspectives from Hurricane Katrina/Rita
Maj Gen Rajczak, JFCOM	Joint Command and Control
Mr. Mike Krieger, ODoD CIO	DOD Support for the Warfighter
LtGen Harry Raduege Jr., USAF (Ret)	Combat Librarian
Mr. Larry Huffman	DISA Support to the Warfighter
APRIL 20–21, 2006	
Honorable John Grimes, Assistant Secretary of Defense for Networks and Information Integration	NII Overview
LtCol Joe Bessleman, Global Combat Support System (GCSS), Air Force MAJ Kurtis Warner, FusionNet Lorraine Wilson, Distributed Common Ground Systems (DCGS), Navy	Program of Record Perspective on Information Sharing Panel

Marian Cherry, Horizontal Fusion Edward Siomacco, Net-Centric Enterprise Services (NCES) Bernal Allen, Net-Enabled Command Capability (NECC)	Delivering Core Enterprise Services to Best Enhance Programs of Record
LtCol Steve Starks, USAF LTC Chuck Gabrielson, Army LTC Jim Garrison, Army Major Robert Wagner, Army CDR John Hearne, Navy	Technical Operators Panel
COL Ed Payne, Army, CIO-G6 LTC Harborth William, USA	Army Knowledge Online (AKO)
Kerim Tumay, VP Engineering Programs and Project Management	Convera
Tony Hall, Director, Factiva Global Government Sector Kirk Donval Hornburg, Director of Service, Factiva Global Government Sector	Factiva
Kevin Laudano	Accenture

MAY 18–19, 2006

Craig Harber and Chris Kubic, NSA	Information Assurance Architecture
Gen James Cartwright, CDR USSTRATCOM	Discussion
Mr. Mike Krieger, OSD/NII	Data Strategy
Dr. Ron Jost, OSD/NII	Communications Architecture

JUNE 13–14, 2006

Dr. Linton Wells	Information Sharing with Non-Traditional Partners
Mr. Randy Cieslak, PACOM	TPIAS Phase III Data Flows
RDML Betsy Hight, USN	Joint Task Force-Global Network Operations
Terry Oxford-Scientific Advisor, NSA	Vulnerabilities to U.S. Critical Infrastructure

Mr. Paul Pittelli, NSA	Multi-Level Security
Mr. Ken Aull-Senior Technologist, ISD Office of Technology, Northrop Grumman Mission Systems	Identity Management
Will Kelchner- DIA	Defense Intelligence Multi-level Capability via MDDS
Mr. Donovan Lewis-Chief, Threat Analysis Division and Mr. Taylor Scott, DIA	Threats to the Network
Mr. Jim Gosler	The Digital Dimension
Sean O'Keeffe-Technical Director, Security and Evaluation, Office of Networks Solutions Engineering (C4),NSA/CSS Commercial Solutions Center	HAIPE Overview and MCEB—HAIPE Request for Joint Staff Assistance

JULY 18–19, 2006

MAJ Neil Khatod, USA-Chief of Concepts, TRADOC Program Integration Office — Networks and COL Jim Henderson, USA-Chief, Battle Command and Awareness Division, Army Capabilities Integration Center, TRADOC	Single Integrated Transport System
Dr. Larry Stotts	DARPA Tactical Communications
Mr. Mike Kern, Mr. Tony DeSimone, and Mr. Tony Modelfino, Assistant's to the Deputy to the ASD(NII)/DOD CIO, for Enterprise Wide System Engineering	Enterprise engineering issues and performance assessment approach example for quality of service
Dr. Robert Popp and Dr. Craig Haimson	Last Tactical Foot
Mr. John Landon	NII Acquisition

AUGUST 9, 2006—INDUSTRY PRESPECTIVES

Mr. Bill Clingempeel	Qualcomm
Mr. George Spix	Microsoft
Mr. Bob Shrimp	Oracle
Mr. Rafat Alvi	Sun
Mr. Greg Akers	CISCO

Appendix D. Glossary

ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration
C2	command and control
CIC	Combat Information Capability
CIO	chief information officer
CONUS	continental United States
COTS	commercial off the shelf
DDR&E	Director, Defense Research and Engineering
DISA	Defense Information Services Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DSB	Defense Science Board
EWSE	Enterprise-Wide System Engineering
GIG	Global Information Grid
GIG/BE	Global Information Grid/Bandwidth Expansion
HAIPE	High Assurance Internet Protocol Encryption
HUMINT	human intelligence
IM	information management
IP	Internet Protocol
ISR	intelligence, surveillance and reconnaissance
JCIDS	Joint Capabilities Integration and Development System
JFCOM	Joint Forces Command
JTRS	Joint Tactical Radio System
JWICS	Joint Worldwide Intelligence Communications System
NCES	Net-centric Enterprise Services
NCO	network-centric operations
NECC	Net-enabled Command and Control
NIPRNET	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
POP	point-of-presence
R&D	research and development
SIGINT	signals intelligence
SIPRNET	Secret Internet Protocol Router Network
SRW	soldier radio waveform
STRATCOM	United States Strategic Command

TMOS	TSAT Mission Operations System
TSAT	Transformational Satellite Communication
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
WIN-T	Warfighter Information Network-Tactical
WNW	wideband networking waveform