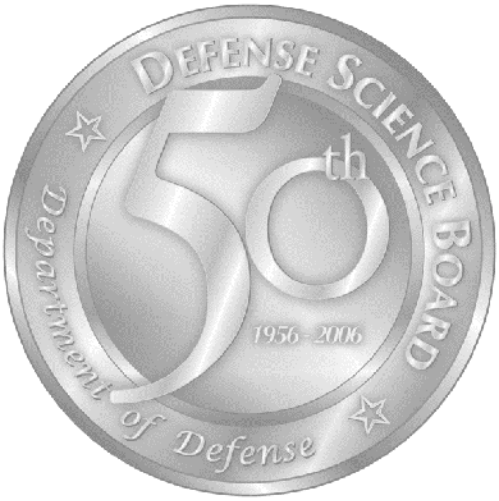
Defense Science Board
2006 Summer Study

on

Information Management for Net-Centric Operations



Volume II
Operations Panel Report

April 2007

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

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Science Board 2006 Summer Study of Information Managment for Net-Centric Operations. Volume II. Operations Panel Report	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Secretary of Defense,Defense Science Board,3140 Defense Pentagon,Washington,DC,20301-3140**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**80**	

This supporting paper of the DSB 2006 Summer Study on Information Management for Net-Centric Operations contains material that was provided as inputs to the volume I report. The findings and recommendations contained herein may not represent the consensus view of the full study.

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.

Table of Contents

Chapter 1. Introduction

Operations Panel

Panel Co-Chairs:
Gen Jim McCarthy, USAF (Ret), U.S. Air Force Academy
LTG Keith Kellogg, USA (Ret), CACI

Members and Government Advisors:
Mr. Scott Fouse, ISX Corp
Mr. Greg Gardner, Oracle
MajGen John Hawley, USAF (Ret), CollaborX
Dr. Richard Ivanetich, IDA
Dr. Jerry McGinn, Northrop Grumman
Mr. F. Michael Ponti, OASD NII
LtGen Harry Raduege, USAF (Ret), Deloitte
Mr. Kevin Woods, IDA

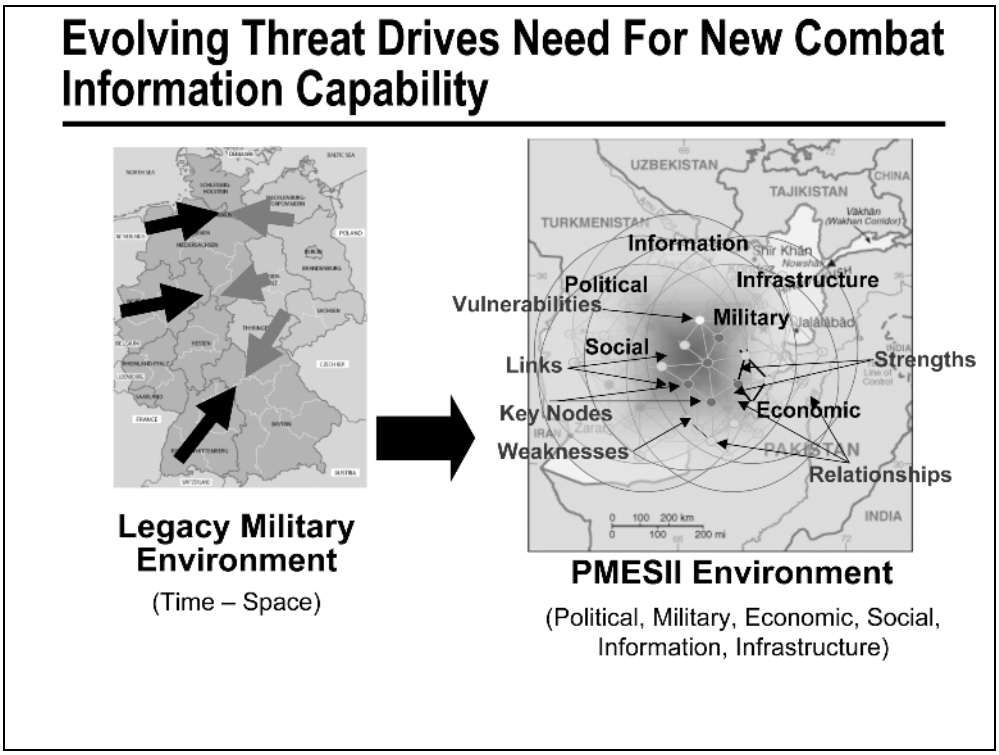
This report of the operations panel of the Information Management summer study served as the basis for the full summer study report sections that included warfighter assessments of needs and suggested improvements to enhance combat capabilities. The panel appreciates the candor and insights that formed the basis for panel recommendations. The panel co-chairs acknowledge the investment of time and the insights that the panel members brought to this study.

The panel contributed primarily to the first and fourth statements in the terms of reference.[1] The panel examined the operational value enabled by information networks. Particular attention was paid to

1. The study's terms of reference is Appendix A.

emerging missions, counterinsurgency, counterterrorism, stabilization and reconstruction, and response to catastrophic disasters. The panel assessed the state of knowledge management for information networks. Additionally the panel focused on information discovery, sharing, collaboration, visualization, and storage for all missions and users. In addition, the elements of a Combat Information Capability (CIC) were developed and described.

The panel's principal focus was on warfighter's needs as viewed through the eyes of those who experienced combat operations in both Iraq and Afghanistan. This perspective helped the study members appreciate the value of a CIC both as kludged in today's combat environment and desired for the future.



There are a number of catalysts for change. These include globalization, the information revolution, and force changes in structure and technology.

In terms of globalization, the environment has evolved from a relatively immature state where, in the industrial age of the 20th century, security meant "defense" and "containment;" to a more mature and integrated environment where "the world is flat," information is shared globally in near real time, and where security means "defense and all else."

The information revolution has moved the world from a place where data moved at about 30 words per minute over field phones and 60 words per minute over radios to one in which data can be moved at roughly 1.5 trillion words per minute over wideband data links. The impacts on the U.S. security environment are enormous.

There are other evolving threat characteristics that the panel considered during the course of the study. Future threats will be:

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

Adversaries have become very skilled at neutralizing U.S. operational advantages. Of primary concern to the study was that U.S. adversaries seemed to not only be using their many skills in information technology to move information rapidly, but also they have a significant capability to attack U.S. information systems. There was also much concern expressed about the trend of commercial-off-the-shelf information technology production moving to Asia and the implications of this trend.

Since Operation Desert Storm, the United States has reduced the size of its warfighting forces by 200 ships, 12 air wings, and 4.5 divisions. At the same time:

- There are more active and potential global hotspots.
- The threat is increasingly using asymmetric tactics.
- Interoperability is still an issue with many coalition and allied participants not to mention inter-service.
- Long-term allied support is not a given.

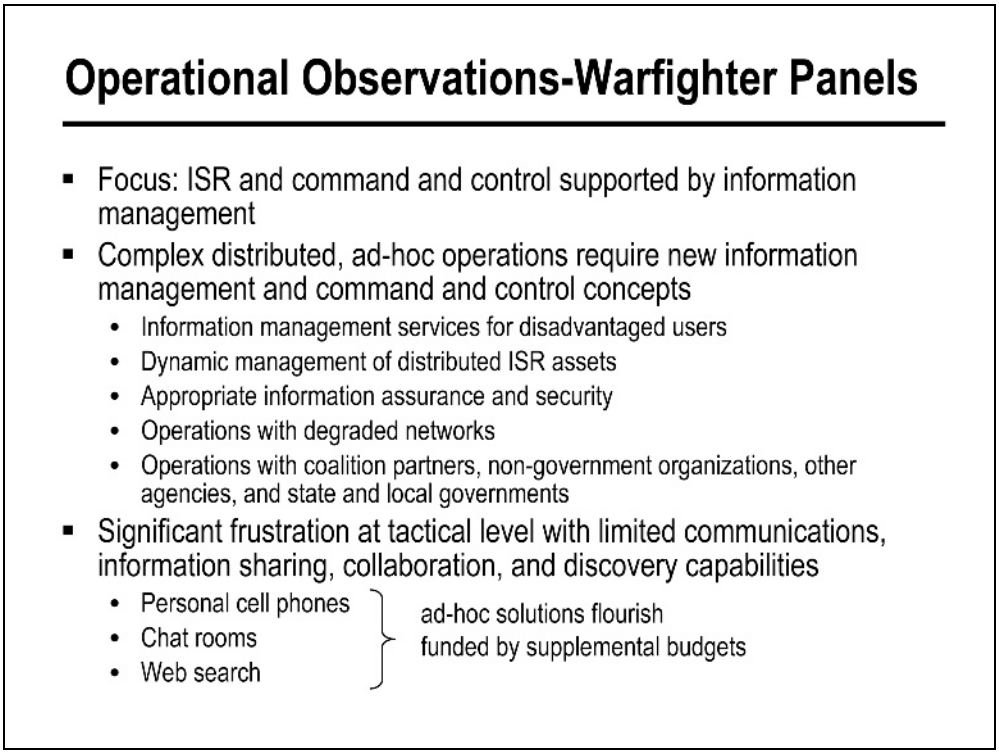
A fundamental trade of massed forces for massed electrons has occurred. The defense budget has remained flat with investments focused more on information technology; precision; command, control, communications, and computers; and intelligence, surveillance, and reconnaissance. Now, there is a need for rebalance so that the investment focuses on making sense of sensor information.

The implication is clear: technological advances and radically improved collaboration and information sharing capabilities with smaller, deployable military forces mandate interdependence across the range of national power (political, military, economic, social, infrastructure, and information). It also places a premium on managing information and making the right decisions at the right time.

In a practical and logical sense, this environment means that the government will have to be more effective at convincing the population of a target country (Iraq, for example) to support their government and refrain from violence in order to promote economic pluralism, restore and improve infrastructure services, and promote legitimate governance within a context of full spectrum information operations rather than just simply training their security forces and conducting military operations against insurgents.

This dynamic frames the outlook on security operations in the information age.

Chapter 2. Deriving Information Needs from Operational Scenarios

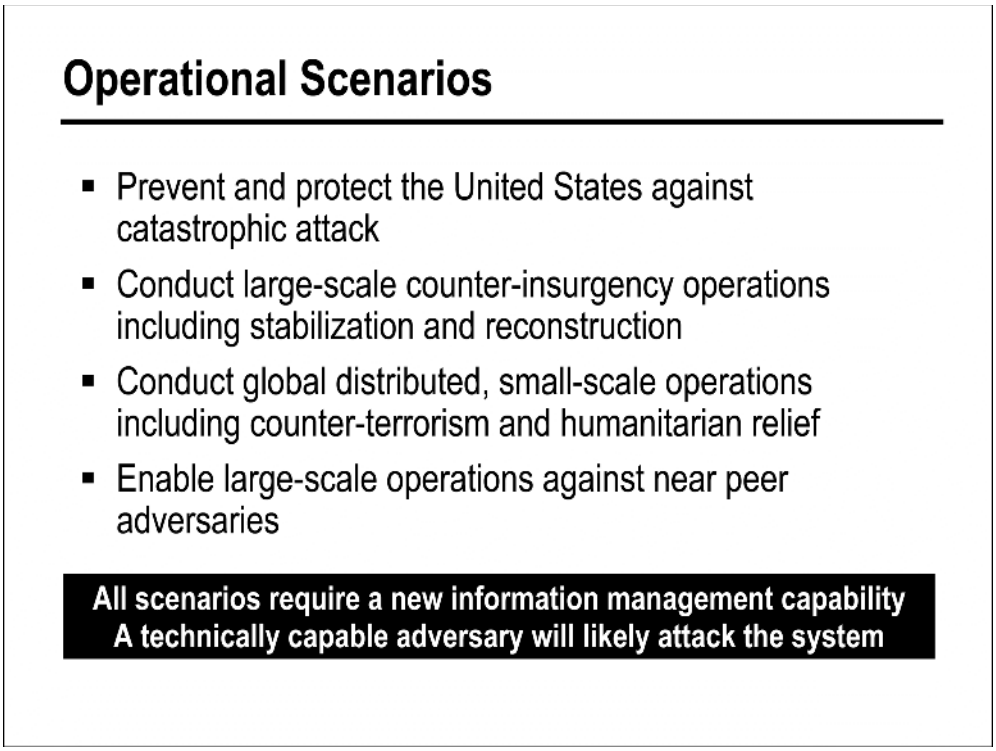


The focus of most combat operations over the past several years has been overwhelmingly in the land domain. The distinguishing characteristic of this domain, with some exceptions, is its people-centric nature. This characteristic is distinct from the platform-centric nature of other domains or even more traditional conventional land combat. The recent experiences of warfighters 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 and networks at the tactical level. The validation of the network-centric operations thrust of current

Department of Defense (DOD) activities should also include a serious look at its risks, vulnerabilities, and challenges.

Warfighters 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 on vast amounts of information is changing the way some commanders organize forces for combat. On the negative side the tactical networking solutions continue to be ad hoc in nature. 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 observations of several warfighter panels varied according to the particular experiences of the participants. Nevertheless, several findings emerged. Information management was the warfighters principal concern. Finding the needed information effectively and in a timely manner was very difficult for both the tactical commander and the staff. The information management challenge at the tactical level was couched in very practical terms: warfighters want information management concepts that support, not restrict, their concepts of operation. Commanders want improved access to intelligence, surveillance, and reconnaissance (ISR) data at all levels. In some cases, this access is desirable without value-added analysis; in other cases, intelligence processing is helpful as long as it meets time requirements. Establishing information sharing and collaboration seamlessly for voice, data, and video without regard to organizational echelon is the desired end state.



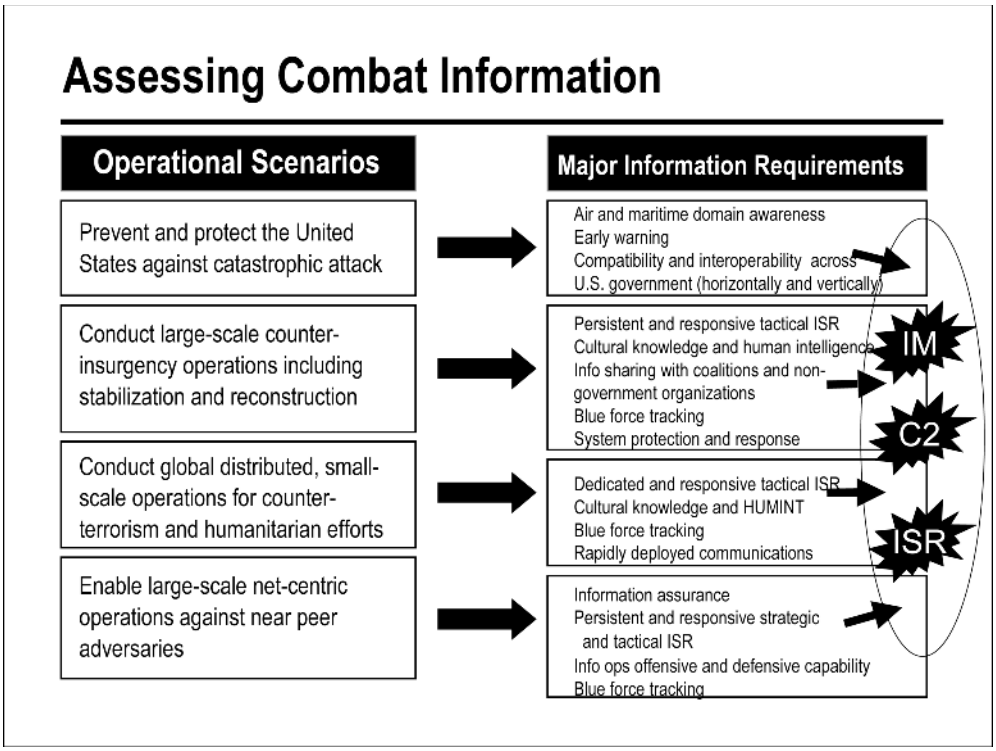
The study assessed the following operational scenarios that were derived from the threat assessment prepared for the most recent Quadrennial Defense Review:

- prevent and protect the United States against catastrophic attack
- conduct large-scale counterinsurgency 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

It was concluded that under all scenarios a sophisticated and state-of-the-art information management capability would be required.

Information systems technology has proliferated across the globe driven primarily by the global economy and the Internet. One could argue that the United States no longer holds a significant advantage in information systems technology. Potential adversaries are technically

very capable in this area and are able to move information rapidly. Adversaries will also clearly understand the importance of information to winning in combat and will therefore commit to attacking U.S. command, control, communications, and information systems. These attacks may be kinetic and/or non-kinetic attacks.



When the four operational scenarios are examined in detail, certain major information requirements become clear for each scenario. These information requirements include data, 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 are illustrative of the respective scenarios and they provide a good sense of the types of information required for today's security challenges.

Homeland Defense

Prevent and protect the U.S. against catastrophic attack

- air and maritime domain awareness
- early warning of potential attacks against the United States
- compatibility and interoperability across the U.S. government, horizontally and vertically (that is, at the federal level among various agencies and departments as well as between federal, state, and local authorities)

Conduct large-scale counter-insurgency operations including stabilization and reconstruction

Iraq
Afghanistan

- persistent and responsive tactical ISR, for example, to track small groups and counter improvised explosive devices
- cultural knowledge and human intelligence to gain an understanding of the local environment
- information sharing with coalitions and non-government organizations to harmonize mutually reinforcing efforts
- blue force tracking to maintain situational awareness and prevent fratricide among U.S. and coalition forces
- system protection and response

Conduct global distributed, small-scale operations for counter-terrorism and humanitarian efforts

Horn of Africa
Philippines

- dedicated and responsive tactical ISR, for example, to track small groups and support deployment of humanitarian assistance
- cultural knowledge and human intelligence to gain an understanding of the local environment
- blue force tracking to maintain situational awareness and prevent fratricide among U.S. and coalition forces
- rapidly deployed communications

Enable large-scale net-centric operations against near peer adversaries

China

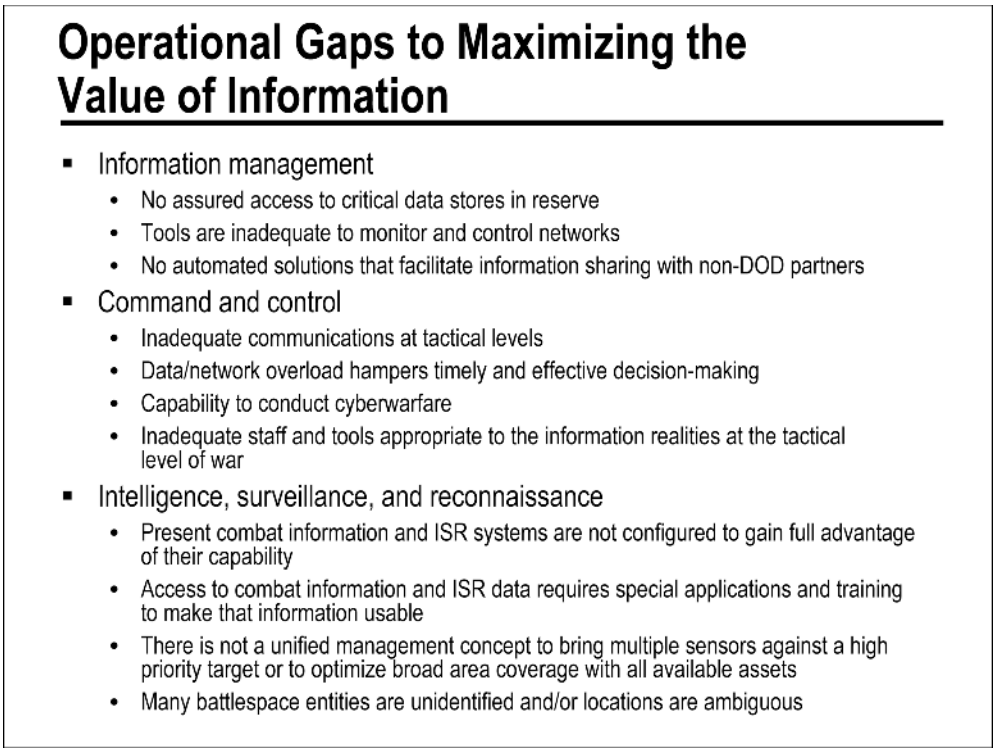
- information assurance
- persistent and responsive strategic and tactical ISR
- information operations offensive and defensive capability
- blue force tracking

This examination shows that, while there is much commonality across the scenarios, the major information requirements have needs that are distinct for each operational scenario. Nonetheless, three major areas emerge as central throughout all of the scenarios:

- information management
- combat information capability command and control
- intelligence, surveillance, and reconnaissance.

Moreover, information management, command and control, and ISR—taken as a whole—combine to form what the panel 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 be discussed on the following pages.



After discussions with a cross-section of warfighters with recent operational experience in Iraq and Afghanistan, as well as insights from panel members, three areas of concern emerged: information management, command and control, and ISR.

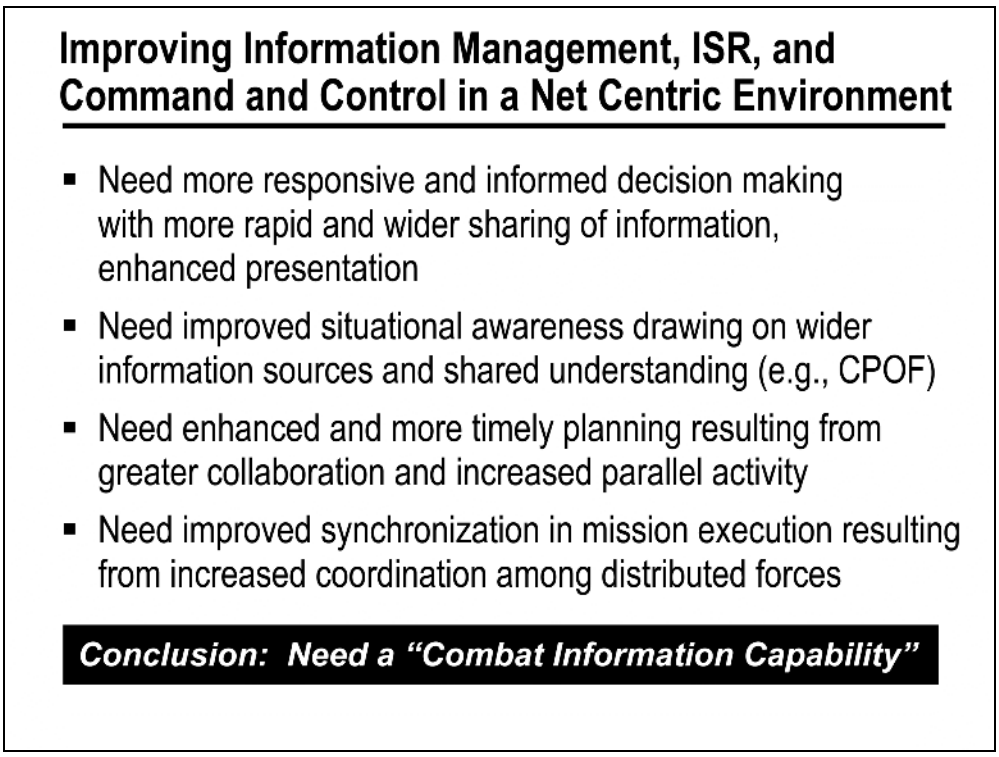
Information management. Recent operations have reinforced the endemic challenge of providing the right information at the right time in the right form. The ability of commanders to organize and manage information and related resources was limited by a host of complex interrelated issues. The most common 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 the quality of, and protecting information for operational use. Information management will provide essential mission functionality for the user to discover (data and services), understand, and use information, and collaborate with other users.

Command and control. In this context command and control is defined within the scope of activities generally associated with information. Commanders at all levels recognize the need to understand the critical capabilities necessary for mission success. Many of the warfighters 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.

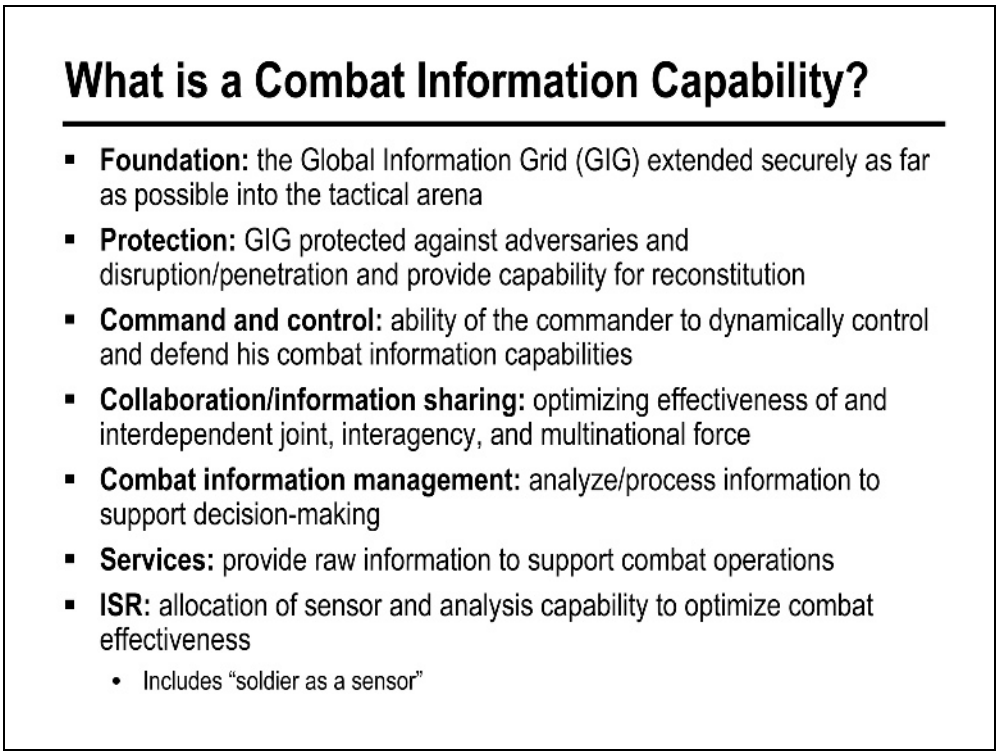
ISR. The tactical warfighter's major concern was the inability to access or fuse ISR data. The ISR data being referred to would include the full range of sensor outputs to include human intelligence reporting.

The often repeated statement "every soldier is a sensor" is meaningless unless the flow of information 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 constraints, and lack of mobility, for example) means that the sensors generally, when compared to those in a platform-centric environment, tell a commander less and then only after more processing.

Chapter 3. Combat Information Capability



To draw the most combat capability from a net-centric environment, information management, ISR, and command and control must be improved. Decision-making must be conducted more rapidly, with wider information sharing and enhanced means for presenting material. Tactical forces need improved situational awareness by drawing on a wider base of information sources and benefiting from improved and shared understanding. An example of this philosophy in action is the Army's Command Post of the Future. Operational planning needs to be improved through greater collaboration among applicable participants. The warfighter needs time-saving benefits derived from increased parallel activity and less reliance on old, slow serial processing. Mission synchronization needs to be improved through increased coordination among distributed forces. In short, different ways of thinking about the criticality of battlefield information are required. Today, DOD needs a Combat Information Capability for modern military operations.



The concept of a CIC becomes the commander's primary enabler for providing command and control of military forces. This includes new ways for maintaining oversight of forces, sensors, networks, and the information flowing to, from, and within the battlespace. It is envisioned to have the seven characteristics shown above.

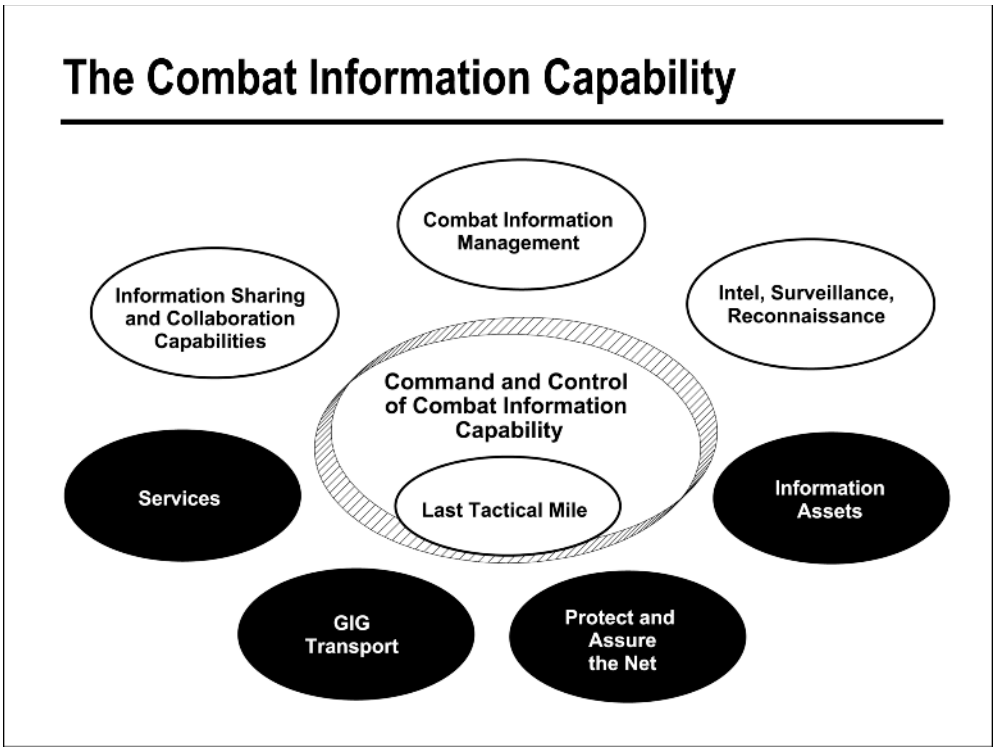
A CIC will collect and disseminate authoritative location and identification information on battlespace entities, targets, and threats; facilitate information sharing and collaboration; support critical operational and logistics planning; and provide improved situational awareness and understanding to decision makers.

The bottom line is that soldiers walking through the Shia-Kot Valley in Afghanistan during Operation ANACONDA who took fire from Taliban forces hidden in a cave want net-centric operation and self-synchronization capabilities, and want it right here, right now to make the adversary go away.

If they are networked, they can share their situational awareness and their very high fidelity perspective of the battlespace with those that may not have the same perspective, such as the low flyers who have a moderate fidelity perspective, or the high flyers who have a low fidelity perspective. If the situational awareness and perspective across participants and platforms can be shared, then those participants will be able to quickly collaborate on the desired effects needed and decide on the best capability in which to engage. Commanders don't want tens of bombs from a B-52 if, for example, friendly forces are only hundreds of meters away.

On the other hand, if the ground forward air controller and F-16 pilot share a picture of the situation (shared situational awareness) they are able to quickly collaborate and decide on what to do when the situation dynamically changes. In other words, they self-synchronize to best engage the enemy and avoid fratricide.

There is, however, a quality aspect to information in this net-centric environment. Consider, for example, the video clip used by insurgents in Iraq to demonstrate that Americans were indiscriminately bombing civilian crowds. Information was taken from a sensor, manipulated, and broadcast as truth. This example emphasizes that higher quality information needs to be rigorously cross-checked for accuracy.



The CIC can be described by referring to the chart above. The foundation is the global information grid (GIG) transport extended to the High Assurance Internet Protocol Encryptors (HAIPE) that are to be moved as far forward as possible and include information assurance elements of the network. This design is intended to provide wideband capability with robust defenses. The elements that will "protect and assure the network" assume that adversaries will attempt to deny this important capability.

"Information assets" refer to data that is generally stored in data sources available to the warfighter. Sensor data, track data, and analyzed information would fit into this characterization. "Services" are the tools that permit discovery and exploitation of the data, applications, displays, and persistent collaboration capability to satisfy combat information needs. Depending on the scenario, the GIG, information assets, services, and the protect/assure functions 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.

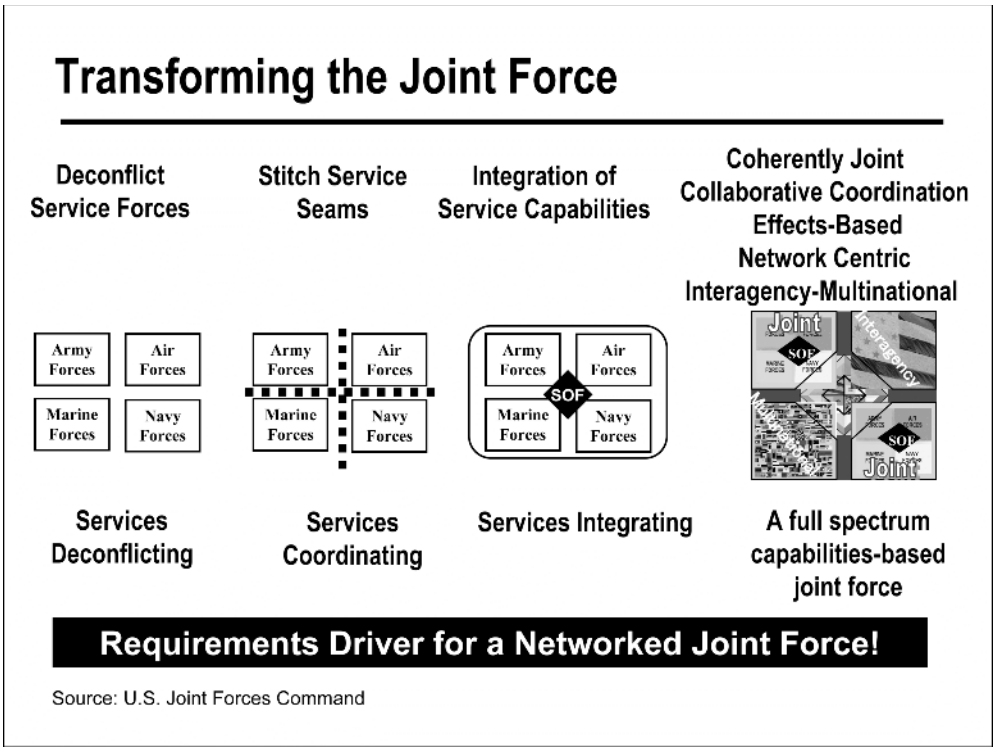
The gray areas on the chart are focused on the operational and tactical level of operations and the recommendations to improve capabilities over the last tactical mile. "Combat information management" refers to strengthening the structure to provide commanders and individual warfighters with educated and trained assistants who understand and support combat information requirements. An "information sharing and collaboration" capability refers to the tools and communications that provide the ability to share information dynamically and to collaborate for planning and execution.

Command Post of the Future (CPOF) capabilities in Iraq are an excellent illustration of the value of collaboration that is explained later in the report. "Intelligence, surveillance, reconnaissance" refers to the ability to treat operational and tactical ISR assets as an ISR "system" to obtain the most effective, responsive coverage by limited 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 warfighting capability as is done with other essential elements of combat power. This report describes aspects of the CIC that permit the commander to exercise command and control.

The "last tactical mile" generally lies outside the HAIPE, may have limited communications bandwidth, has unique security and assurance requirements, and warrants particular focus in this study. The panel outlines particular requirements to support the "disadvantaged" warfighter.

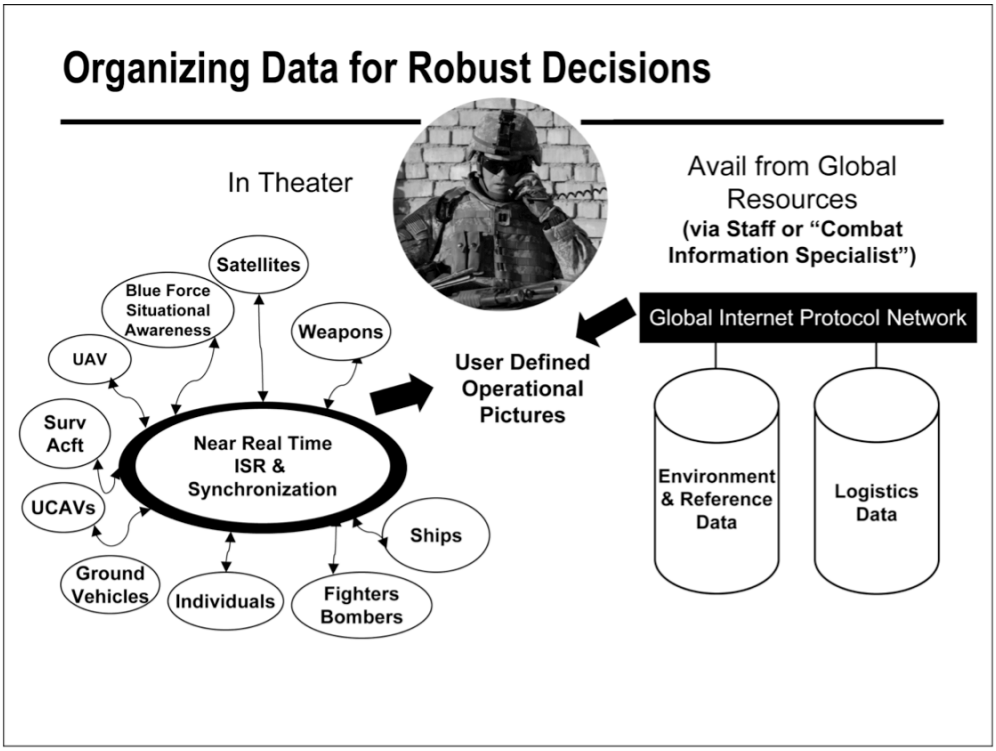
Taken together, these elements comprise a CIC that the report will outline as its principal finding.



It is important to understand how joint forces will be employed before the design of the CIC is finalized. The figure above is an illustration that was created by Joint Forces Command to show the history and future of joint force operations. In the not too distant past, joint force commanders could only reliably disseminate written orders to subordinates and, thus, had to employ procedural means of de-confliction such as lines on the battlefield and/or time de-confliction to insure safe separation of component forces. For example, in the Vietnam era, Air Force units were employed in the Hanoi region by day but by night Navy forces were used in order to prevent the potential for fratricide. Gradually, as battlefield communications began to improve, joint force commanders were able to start employing component forces in closer proximity to one another. New concepts such as joint engagement zones were developed to more closely integrate the joint force. The Joint Fires Initiative was a key part of Millennium Challenge 04, a recent major joint force experiment.

The operational goal for the future is to be able to conduct interdependent joint operations where any sensor under the control of any joint component commander can sense any other components' targets. This sensor would provide target quality information to that component so that the best available weapon from any component or service can be employed against almost any target on the battlefield within range. Sometimes this is referred to as the "any sensor, any weapon" concept. Thus, joint interdependent operations is a concept that allows the joint force commander to achieve an effect against an adversary using the best system (or sensor) available irrespective of operational command of assignment. Under joint interdependent operations, when a time-sensitive target emerges on the battlefield, the commander in charge of joint force employment will be able to attack the target with, for example, an aircraft, naval gunfire, and/or ground artillery, depending on which asset can be brought to bear in a timely manner and have the desired effect on the target.

The key enabler to being able to operate in the manner described above is creation of an unambiguous track data environment of all battlespace entities (friendly, enemy, and neutral) that can be simultaneously shared at all levels (strategic, operational, and tactical) via user-definable operational displays. This capability is sometimes referred to as a single integrated picture of the battlespace. The figure on the next page is an illustration of how the single integrated picture, as a key element of the CIC, will be created and disseminated.



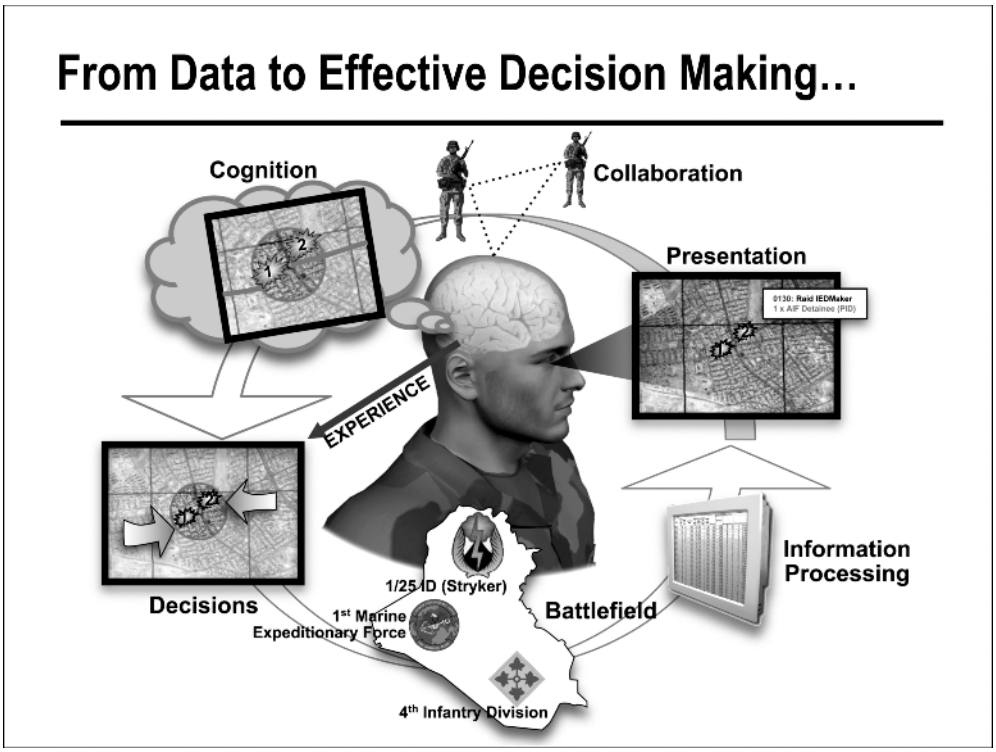
Command centers at both the strategic and operational levels, as well as tactical joint force elements, must have a common understanding of the location and identification of all battlespace entities (people, air vehicles, ground vehicles, ships, subsurface vehicles, space vehicles, buildings, bridges, critical infrastructure components). This information comes from a variety of sources, many of which are represented in the ovals on the left side of the figure above. 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 battlespace 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 (such as land, maritime,

space, and, perhaps, cyberspace) thereby creating an unambiguous track data environment for all domains.

This unambiguous track data environment created primarily via a well-synchronized, near-real-time ISR tracking network (illustrated in the figure above) 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 user-defined operational displays needed at the tactical level may vary significantly from those required in a command center. However, the important premise is that all user displays use common data sources so that the information is consistent and authoritative across the entire joint force.

The net effect is that the warfighter will have near real-time data and the user-defined operational display to carry out the assigned mission.

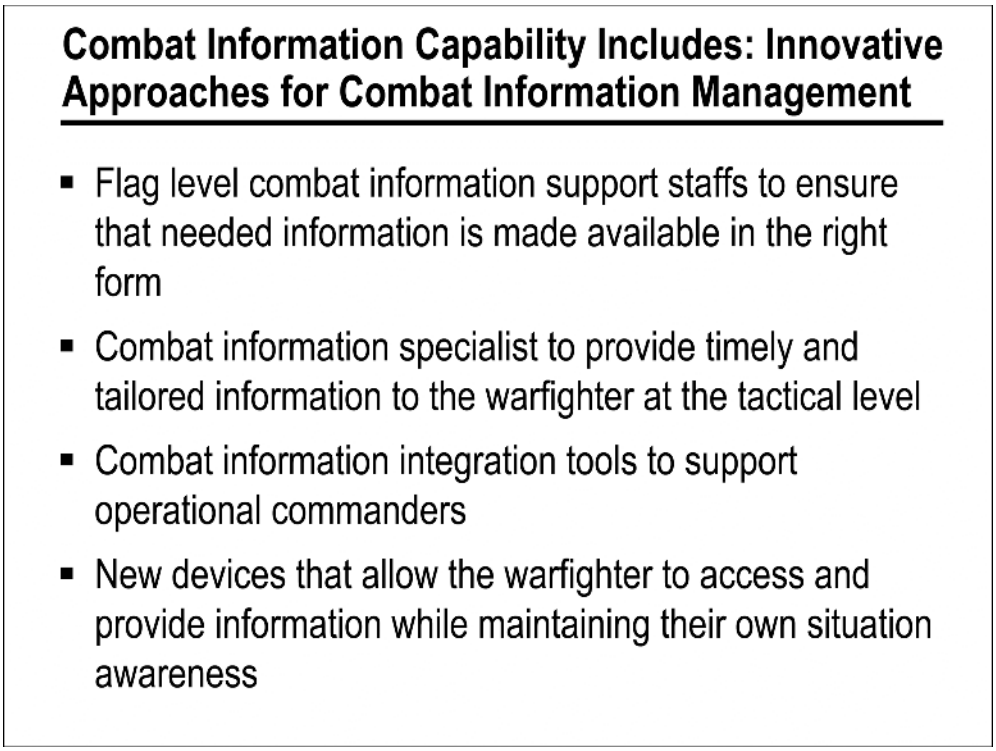


Once the information is made available to the user, the next major problem to address is how to support that user in making sense of that information.

The answer lies in net-centric operations theory as articulated by, among others, Garstka and Alberts. This theory addresses physical, information, cognitive, and social domains. The physical is where strike, protect, and maneuver take place across the environments of ground, sea, air, and space. The information domain is where information is created, manipulated, added value to, and shared. It can be considered the "cyberspace" of military operations. The cognitive domain is 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 is 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.

Chapter 4. CIC Functions and Staff

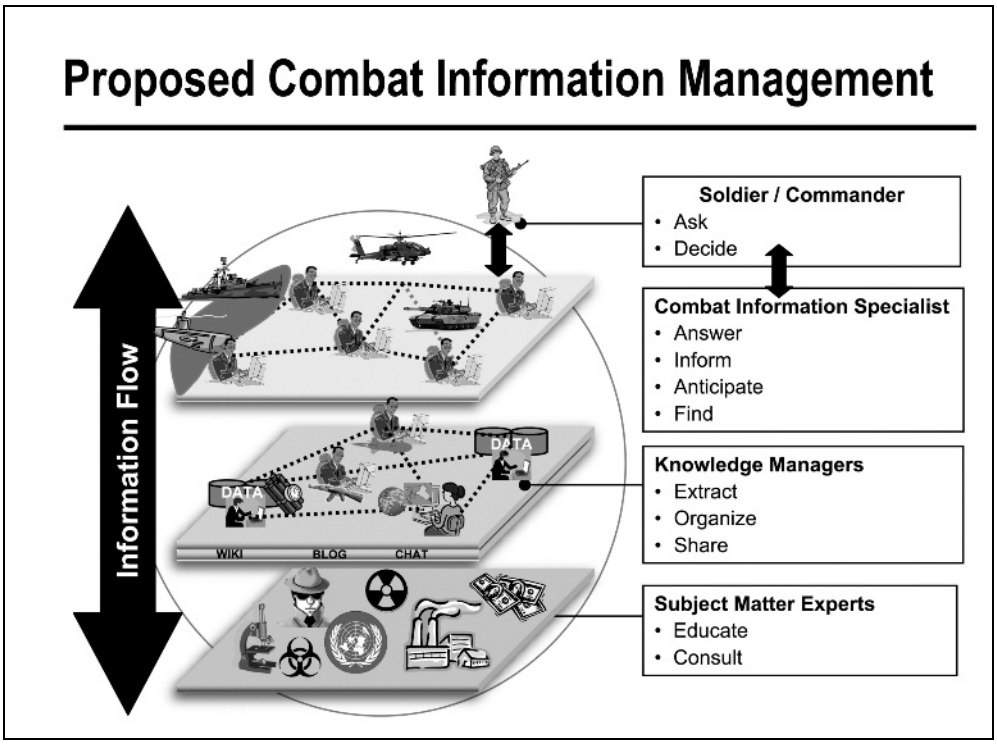


Getting information to the commander or warfighter is necessary and challenging, but by itself insufficient to enable making the best possible decisions and employing forces to the best effect. To achieve that end, the commander needs focused practical assistance in processing information. At the brigade level and above, commanders need a specific, focused staff to process information into a form that enables better decision-making.

Importantly, the panel believes that commanders in the rank of O-9 and above (those who serve as joint force commanders) need a dedicated combat information integrator to optimize their ability to make effective, timely decisions. The combat information integrator facilitates collaboration and information sharing; ensures disciplined information

management; facilitates interdependence among diplomatic, information, military, and economic partners; blends the art and science of information management; and leverages best practices. This individual has a number of key attributes: significant and relevant operational experience, commander's trust, exceptional intellectual curiosity, and technological sophistication, and undergoes continual training. The combat information integrator is appropriately empowered to interact with commanders and is managed via a unique career management path.

The following pages describe a new management approach to information which includes staff functions, tools and training to assist commanders in assessing situational awareness, system operating mode, force allocation, and ultimately making better decisions.



Combat information management involves the seamless, timely flow of information between and among a globally connected set of players. At the tactical level, individual soldiers and commanders, who are often bandwidth-constrained, rely on organic combat information specialists to help them access, analyze, and process information for decisions. Those specialists are connected with specially trained and experienced knowledge managers, probably operating from a geographically distant location, who provide additionally refined and detailed information, upon which decisions can be made. Importantly, these knowledge managers are content experts, not staff officers.

In turn, knowledge managers access national or international level subject matter experts, who provide deep expertise in designated fields. When appropriate, subject matter experts work directly with combat information specialists to provide timely, refined information to combat commanders to make better informed decisions. This system is fully interconnected and "flat," and global information flows horizontally and vertically among these experts who focus solely on this function. Information flows up as well as down—subject matter experts are

informed by the latest tactical developments as much as they help combat information specialists.

To date there has been an overall lack of focus and effort on managing information in the GIG, including its creation, quality assurance, access control, and timely and appropriate dissemination. Commercial industry, 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 disseminate 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 their field 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.

Current DOD doctrine does not explicitly recognize the management of combat information as a critical military resource. Accordingly, the military services and combatant commanders need to establish combat information positions and associated concepts of operations. The figure above 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 to longer-term substantive analysis.

In particular, the panel recommends the creation of three distinct levels. 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

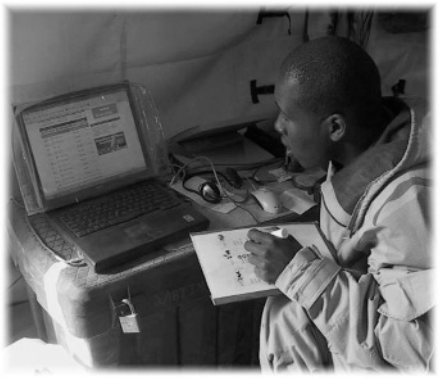
developing answers to those questions, they may collaborate with combat information specialists supporting other units and commanders and/or they may work with knowledge managers who identify, discover, extract, organize, catalog, and maintain information about a selected set of topics. Knowledge managers, and others, utilize 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.

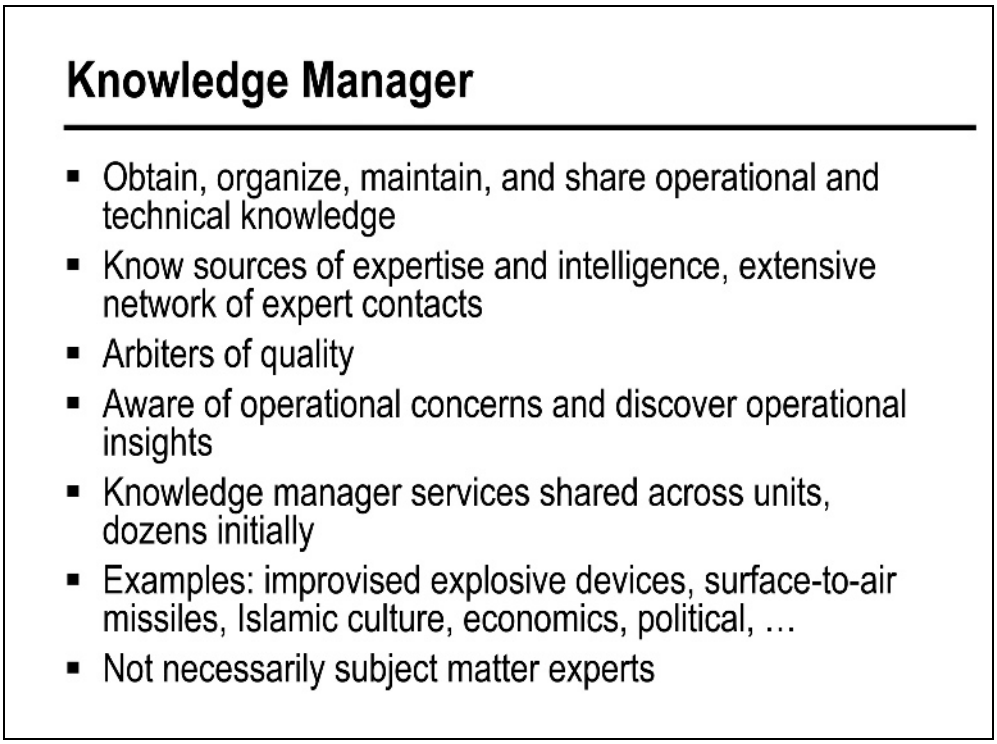
While it is clear that advanced information discovery technology will support these specialists, a primary finding is that technology alone will not solve the problem. Several existing technologies can support each of these roles. This can include wikis, blogs, and collaboration tools (see: http://en.wikipedia.org/wiki/Military_Occupational_Specialty). In fact, the Air Force has defined an Information Manager specialty (http://usmilitary.about.com/od/airforceenlistedjobs/a/afjob3a0x1.htm).

Combat Information Specialist

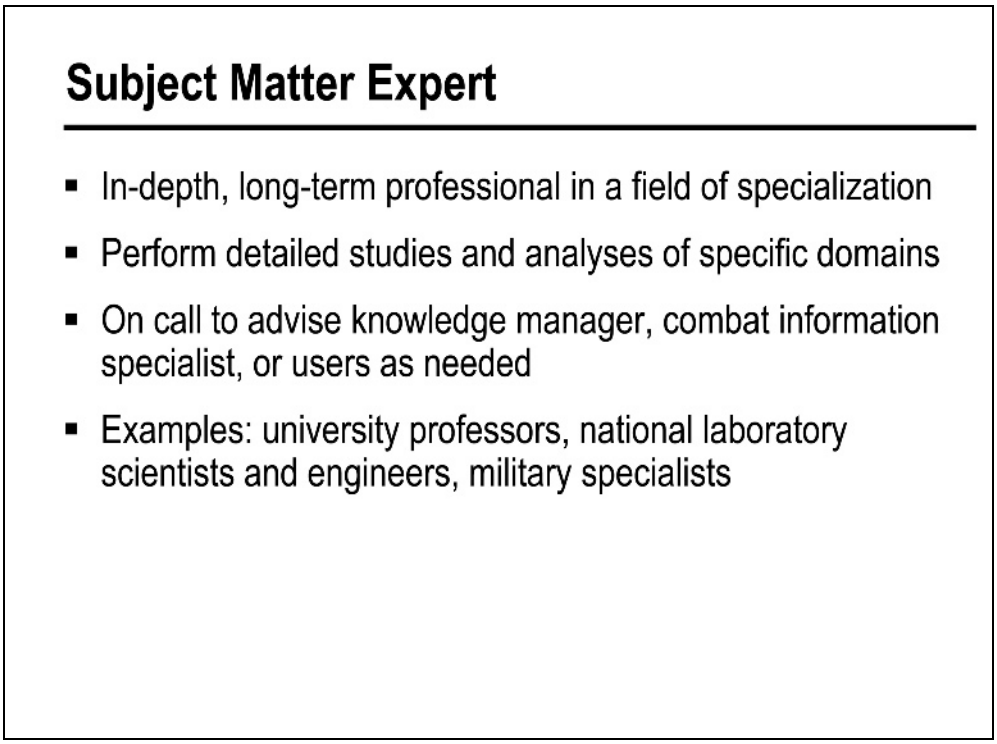
- Anticipate and track operational information needs
- Extensive network of contacts for information and intelligence
- Answer operational requests
- Disseminate to combatants and share with peers
- Provide knowledge managers with after-action reviews
- Integrated into units at all echelons
- Have access to classified information at SECRET level



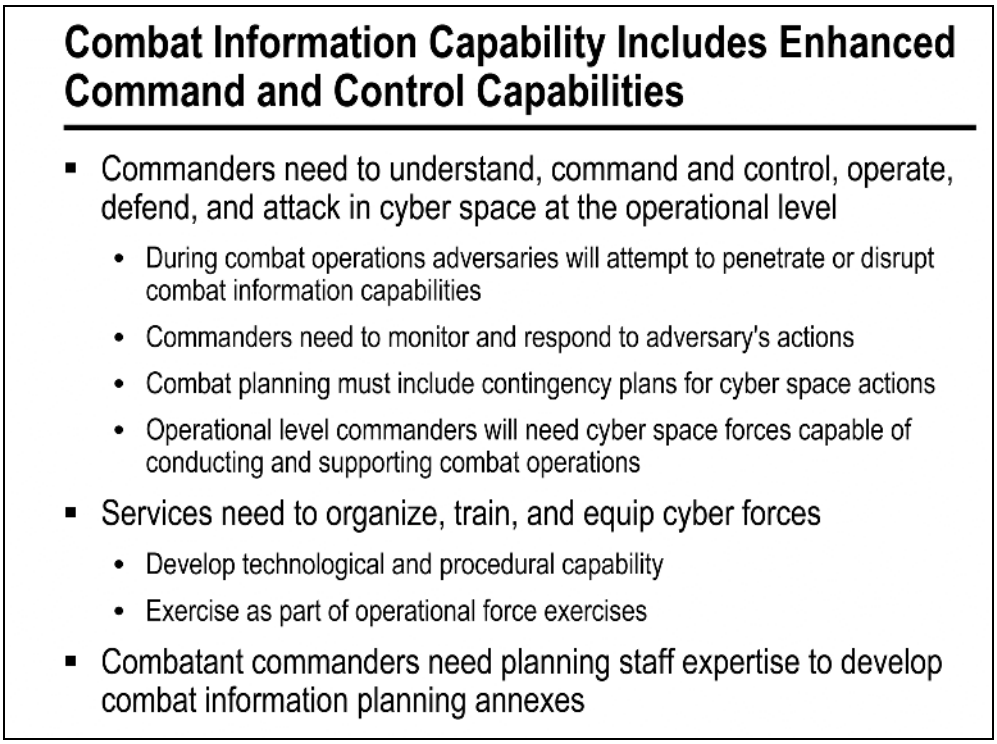
Combat information specialists answer operational requests, anticipate and track operational information needs, and disseminate critical information to combatants—both in mission rehearsal and preparation and in real-time support of mission execution. They are integrated into units at all echelons and have an intimate understanding of the unit's missions and objectives. As such, they 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 that knowledge managers assimilate into their individual domains as appropriate.



Knowledge managers are responsible for obtaining, organizing, maintaining, and sharing operational and technical knowledge in a specific area of focus. 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 there is no need to physically be collocated with operators, they are intimately aware of operational concerns and discover operational insights via their interactions with combat information specialists and operators. One key role they play is as arbiters of quality. Services provided by knowledge managers are shared across units, with dozens initially deployed, growing to thousands at steady state, dynamically altering according to changing information needs.



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 managers, combat information specialists, or users as needed. They may come from any sector, including university professors, national laboratory scientists and engineers, 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 (such as Tacit.com or AskMe.com).



Today, commanders take the command and control of a functional area of combat capability as a given. In terms of combat information, they manage their command and control staff to get the right information in the right form at the right time. To fully realize the potential of network-centric operation, commanders need to take control of their information and the associated infrastructure (the CIC). This ultimately involves two major elements. First, the commander needs to recognize that this is one of the critical tasks. Second, the commander will need the staff, tools, and processes to gain situational awareness of the CIC.

As much as a fully capable information system is needed throughout a mission, adversaries are well aware of U.S. dependence on that capability, and have capabilities of their own 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 be able to relate the current status to mission capability. The

commander must also be aware of enemy efforts to disrupt operations, so that an attack can be anticipated and countered with a response.

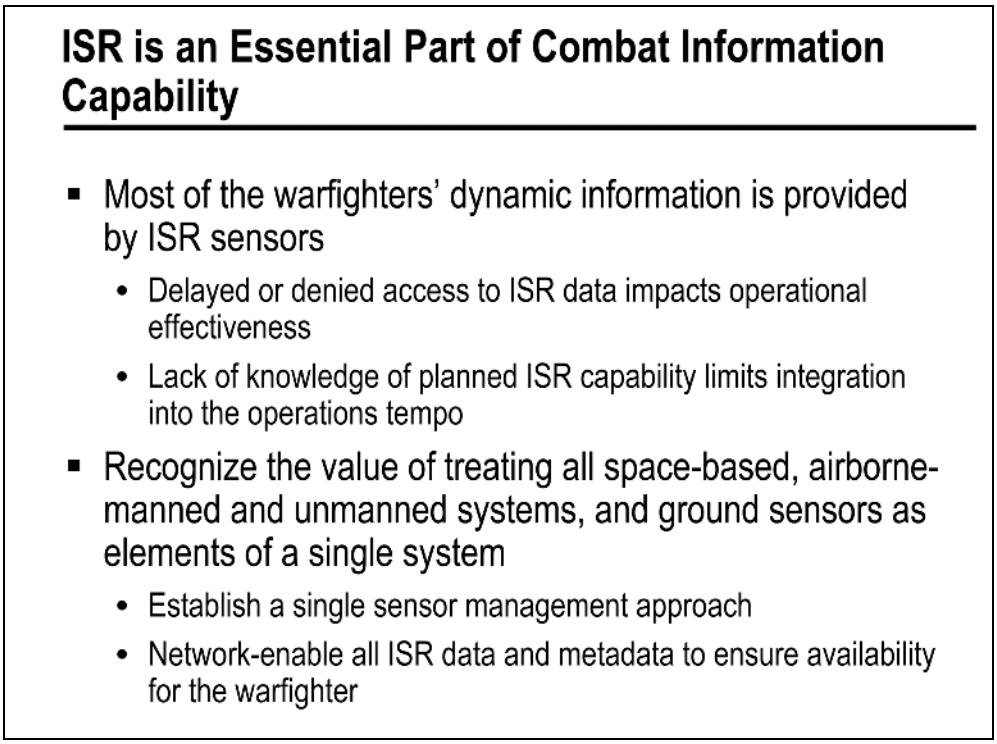
As the commander and his or her staff develop mission plans, contingency plans are necessary for degraded operations. The degradation could be in a variety of areas, such as bandwidth, latency, corrupt data, coverage, or protection. Sometimes, contingency planning may result in a different operating approach to offset adversaries' actions.

A 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 CIC into the overall command and control function. Commanders need to be able to have command and control of critical information. This will bring together both kinetic and non-kinetic attack elements into a unified system and as a step toward providing a unified approach to the world of the cyber command and control, which historically has been treated in separate systems. This unification of command and control processes will allow commanders to have a tool set that manages cyber actions and also allows 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 forces. This will need to address more than just the network. It must also include the information management functions that have been discussed in this report. New tools and processes need to be developed for each of the three major information management staff positions: combat information specialist, knowledge manager, and subject matter expert. These staff elements will need to be trained on the tools and procedures. This training will need to extend to exercises such as division mission rehearsal exercises, where command and control of the CIC is exercised along with other joint warfighting capabilities.

Finally, information management staff expertise should be leveraged to develop a new 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.

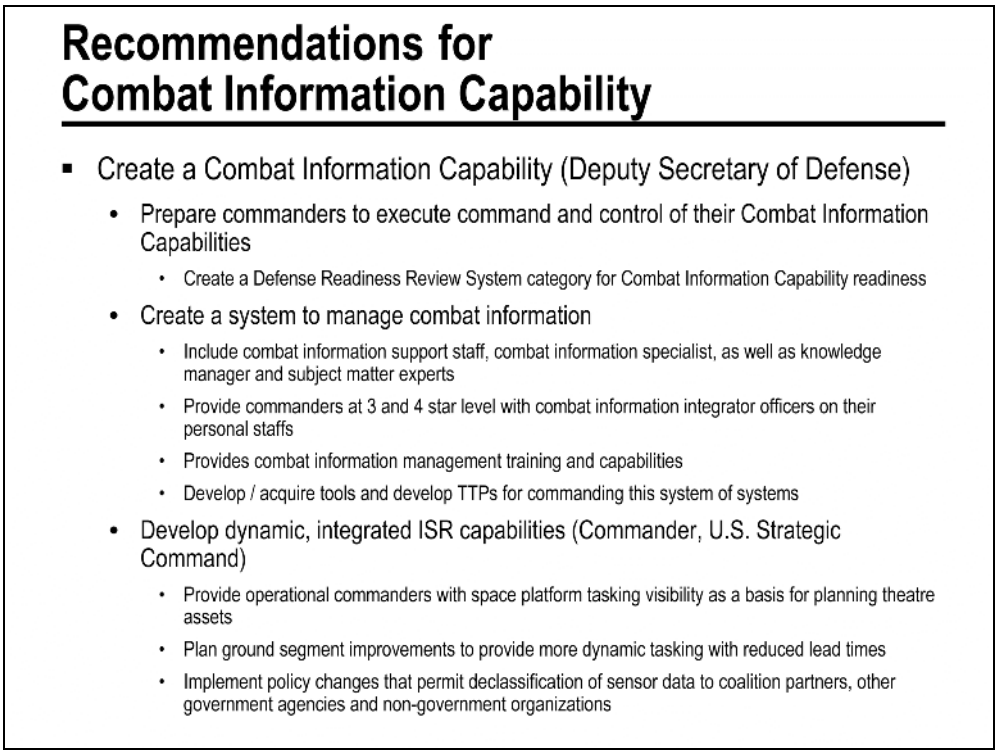


The warfighter is dependent on ISR sensors for most dynamic combat information. While some part of sensor data is usable only when analyzed, much of the reconnaissance data requires immediate access because of the time-critical nature of combat operations. Thus, limiting access to ISR information has a significant impact on combat operations. Currently, combat information requirements 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 limits the ability of commanders to integrate ISR into their operations tempo at all levels 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 its metadata to ensure timely availability to the warfighter.

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.



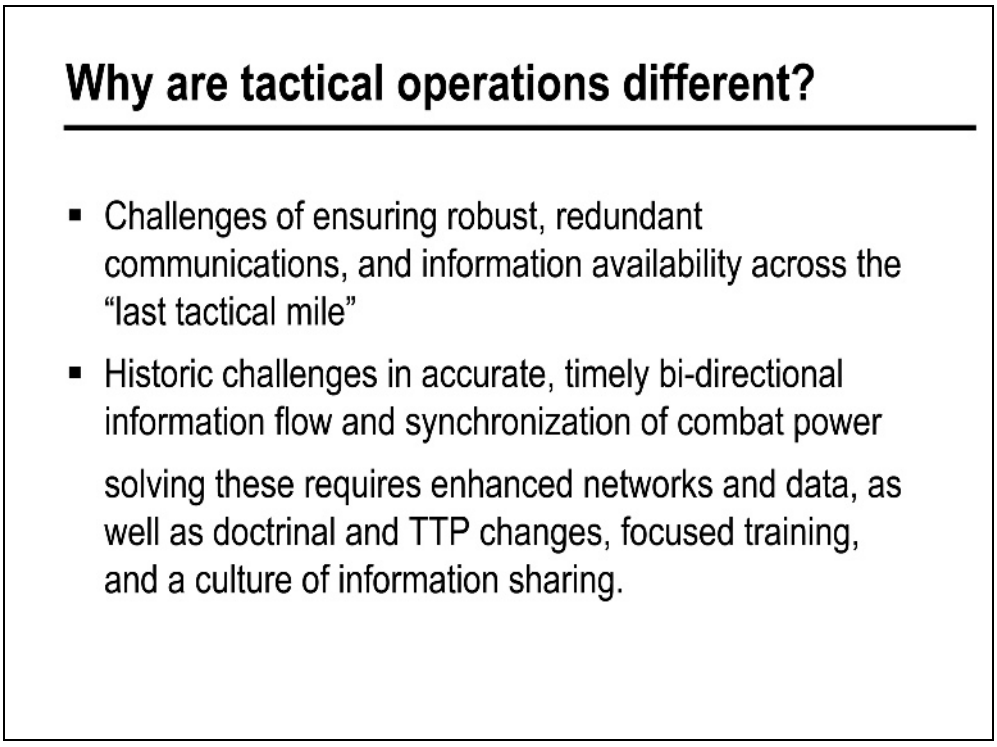
The panel recommends the Deputy Secretary of Defense direct creation of, and allocate resources for, a Combat Information Capability across the department, since all military commanders must undertake new ways to execute command and control of their combat information resources and capabilities. In order to maintain oversight, the panel recommends that these new capabilities be monitored by creating a Defense Readiness Review System category for CIC readiness. In addition, Joint Forces Command needs to prepare commanders to effectively command and control this capability.

A CIC must contain the following capabilities:

- It must include execution elements of a combat information support staff: combat information specialists, knowledge managers, and subject matter experts.
- The CIC must include robust combat information management training and education, and the capabilities to support such activity.

- The CIC must acquire the proper tools and develop tactics, techniques, and procedures (TTP) 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.

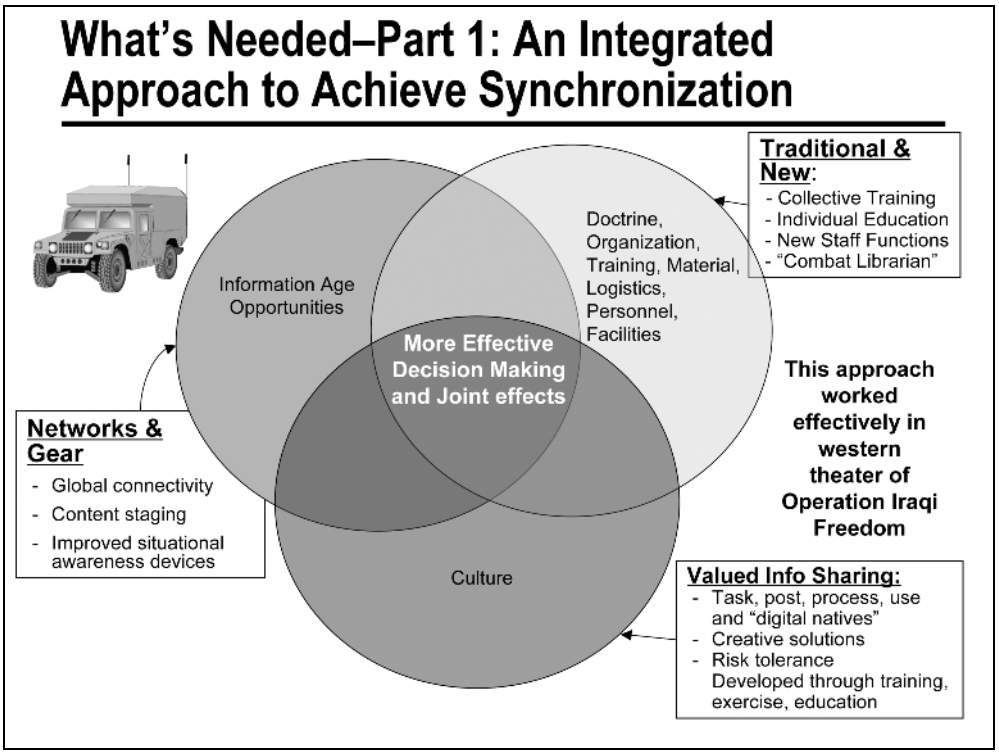
Chapter 5. Tactical Operations



The domains of warfare have been defined as physical, informational, cognitive, and social. The distinctions between and interaction of each domain are generally consistent down to the tactical edge. A generally held belief for net-centric proponents is that solving the "last-tactical mile" communications challenges completes the promise of net-centric capabilities. While better communications at the tactical level closes the gap between the promise of net-centric operations and the state of the art, it is not enough.

Improving net-centric operations in the cognitive and social domains is the area that, in addition to better communications, will begin to close the performance-promise gap. Notwithstanding the current array of physical and informational challenges in net-centric operations at all levels, most practitioners operate in a nearly homogeneous command and control environment. Headquarters staffs

with varying degrees of net-centric capabilities are managing information, facilitating decisions, and communicating to other staffs or platforms. It is at the tactical level that the Clausewitz warning "everything is very simple in war, but the simplest thing is difficult" is most pronounced.



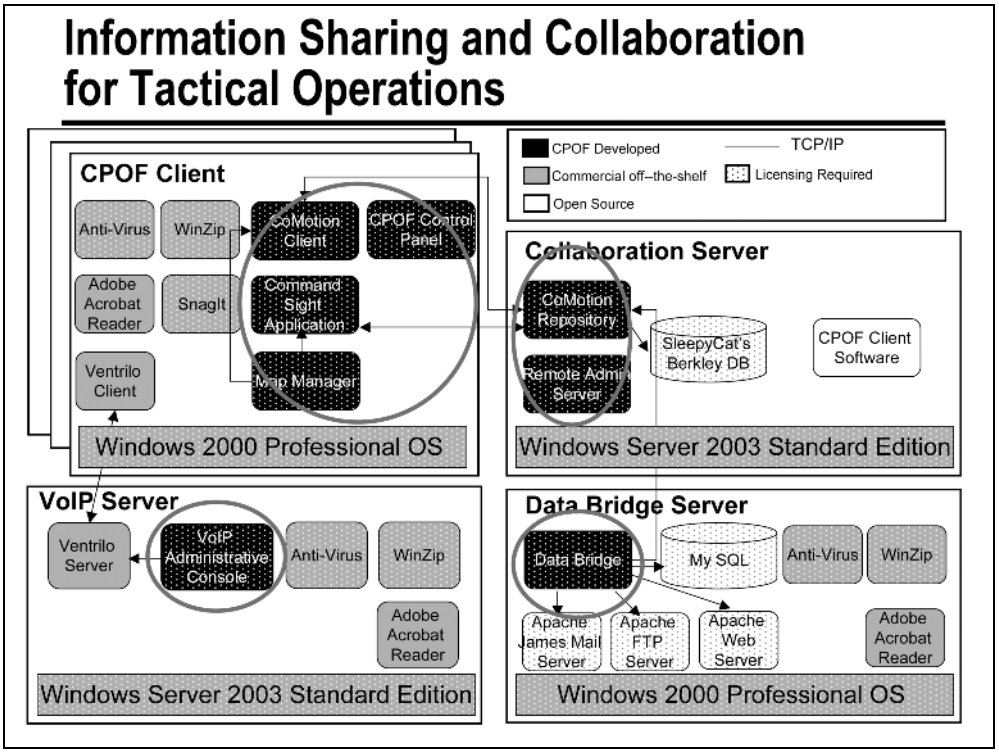
The true success of information management in net-centric operations depends on the successful integration of technology across disparate systems combined with the willingness of organizations to gain experience and adapt both culturally and organizationally.

An excellent example of this combination is reflected in operations in the western theater in Operation Iraqi Freedom. In what was arguably the most networked battlespace in history, commanders created combat power through network-centric systems, doctrine, organization, training, materiel, logistics, personnel, and facilities, and organizational culture.

During Operation Iraqi Freedom Phase One, coalition forces in the western theater accomplished all of their assigned missions, including prevention of all Scud launches, while operating at a 500:1 ground-force disadvantage. The integration of existing command and control systems allowed more rapid response (nine minute response times) to time-

sensitive targets while avoiding *any* air-to-ground fratricide during hundreds of engagements.

MITRE conducted a detailed study of these operations including in-depth interviews with warfighters throughout the kill and command and control chains. This study led to further investigation of particular systems, associated TTPs, and organizations. MITRE concluded that the loose coupling of networks that provided situational awareness from ground-to-air and air-to-ground enabled the coordination necessary to support lightly equipped ground forces. This enhanced communications infrastructure and collaborative tools enabled robust command and control networking that expanded both reach and richness of the information. The MITRE case study demonstrates that successful combat integration and decision-making depends not only on the successful integration of technology across disparate systems but also the vital importance of an organization being adaptive both culturally and organizationally.



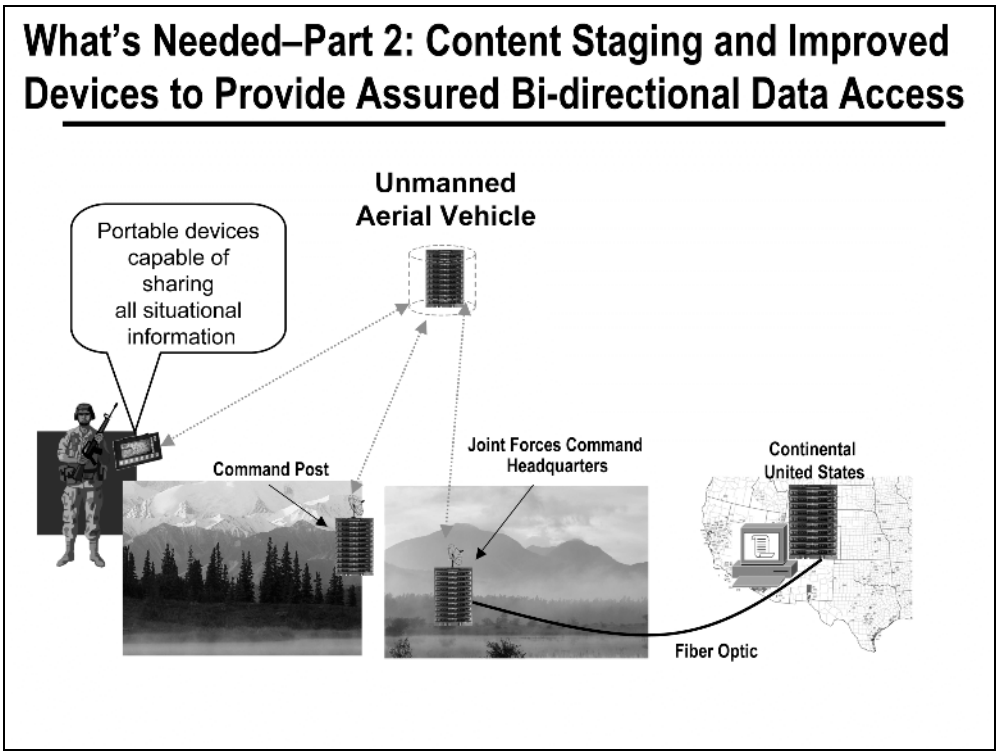
A critical aspect of successful military missions is having a deep, shared understanding of the current situation and the mission objectives, not simply to have a plan. One of President Eisenhower's quotes captures this quite well, "In preparing for battle I have always found that plans are useless, but planning is indispensable." One way, and perhaps the only way, to achieve this deep, shared understanding is to provide the team with a collaborative visualization environment that allows team members to capture their understanding of the situation, share it with others, and collaboratively develop plans to achieve mission objectives.

This is how Command Post of the Future is being used by forces in Iraq today. Distributed, collaborative planning became popular in the early 1990s when networks and video teleconferences were becoming available at the higher echelons. What is different today is the fact that

with systems like CPOF, rather than dedicating bandwidth to share a picture of someone's face, the bandwidth is being used to share thoughts, and thus supporting true collaboration, rather than simply distributed planning. Since the focus is on sharing data, and doing so in a bandwidth efficient manner, CPOF has demonstrated the need and high value of information sharing and collaboration at the tactical levels.

An interesting perspective is how this capability was developed. The CPOF system is built on three core commercial products. One is the database system, which in this case is Berkeley DB, a very popular and powerful database system now owned by Oracle (owned by Sleepy Cat Software when CPOF was first developed). Another commercial component is the 3D visualization package called 3DJava, a high performance tool set developed by Oculus Software. The final commercial component is a collaboration and visualization environment called CoMotion, originally developed by Maya Viz.

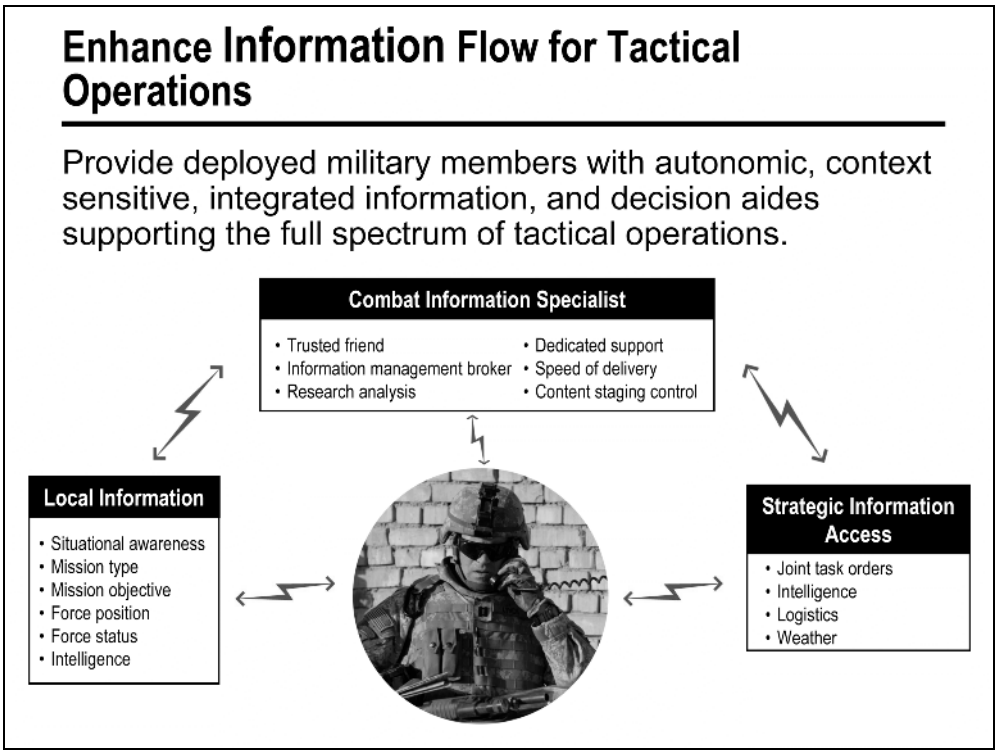
Working closely with users, the developers from Oculus and Maya, as well as other small companies, discovered ways that users wanted to use this collaborative, visualization capability. Those same developers then tailored, augmented, and extended the core commercial products to provide military capability. Initially this was done in the context of a tactical user, but without full understanding of the issues of the tactical environment. Once the system was deployed, other modifications were made to deal with the disadvantaged communications, which had frequent drop outs, high packet loss, and high latency. This experience demonstrates that commercial technology can be adopted and successfully adapted to military use.



The CIC described in this report will constantly be subject to attack by an adversary, both via non-lethal and lethal means. Therefore, the system-of-systems must be capable of degrading gracefully when attacked. Currently most combat data and information content is stored in data storage repositories far to the rear and/or in the continental United States. From the commanders' perspective, this creates a huge vulnerability that may lead to catastrophic failure of their command and control information systems in the event of an attack on various communications systems and nodes.

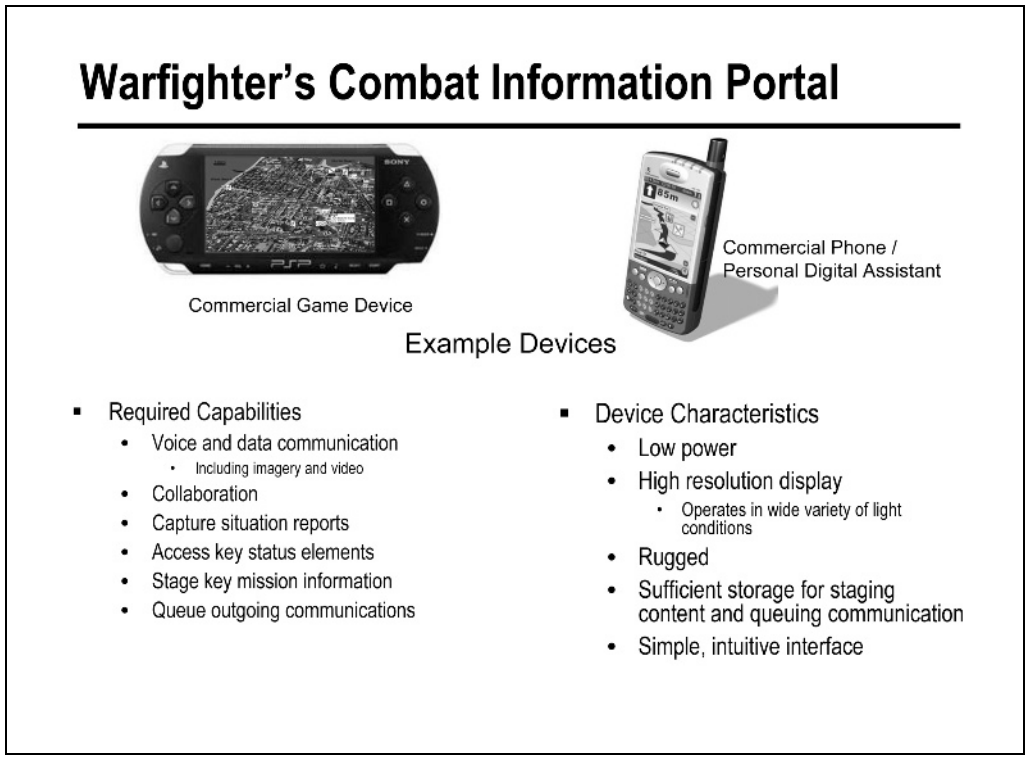
In order to greatly reduce the vulnerability of the CIC to attack, the panel determined that critical battlefield information should be staged in the area of responsibility and/or perhaps even stored in an unmanned aerial vehicle over the area of operations and within direct line of sight of sensors and ground forces. This operational concept is depicted in the figure above. In essence, critical battlefield data would be well protected (firewalled) and staged forward in several servers distributed throughout both the forward and rear areas. Such architecture would not only provide a means to isolate and secure various data sources against an

adversary's attack, but it would also allow data to be replicated between data sources whenever available bandwidth allows. Staging content in theater would not only reduce system vulnerability to attack, but it would also potentially reduce information query response times. Thus, the advantages to all would be reduced system vulnerability to attack, better use of available bandwidth for data transfers, and greatly reduced query response times for warfighters.



The tactical warfighter can clearly benefit from improved access to time-sensitive information and decision aids. The challenge is how to provide that information given the communication and time constraints of the tactical environment. The solution involves three key components. First is the combat information specialist, who can ensure that the warfighter will get the information needed in the right context. Second is a prepared set of information that comes from the local environment, and is very specific to the mission at hand. This information will be staged forward so that the warfighter will have access to it even if there are communication outages. Third is the reach-back to more strategic information assets and general reference information. Due to the harsh nature of the tactical environment, these three components need to be able to provide value to the warfighter separately, but combined will provide a complete capability to access the full range of information required for tactical operations.

The need, then, is to provide a device that the warfighter can use to access this information.



Providing combat information to the edge will require innovative devices that will be low power, rugged, operate in a variety of climactic conditions, integrate voice and data communication, and essentially serve as the single portal to the tactical fighter for combat information, communication, and collaboration. This device needs to address the realities of the tactical environment, and thus be simple and intuitive to operate.

This portal device could potentially be derived from commercial technology. Cell phones, PDAs, and portable game devices should all be explored as candidates to meet this important operational need.

The operational device should provide warfighters 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, or non-government organizations

- collaboration in support of situational awareness, planning, mission rehearsal, and execution
- situation reports such as SALUTE reports
- blue force positional information
- 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.

Recommendations for Improving Information Flow to and from Tactical Commanders to Enable Decision-making

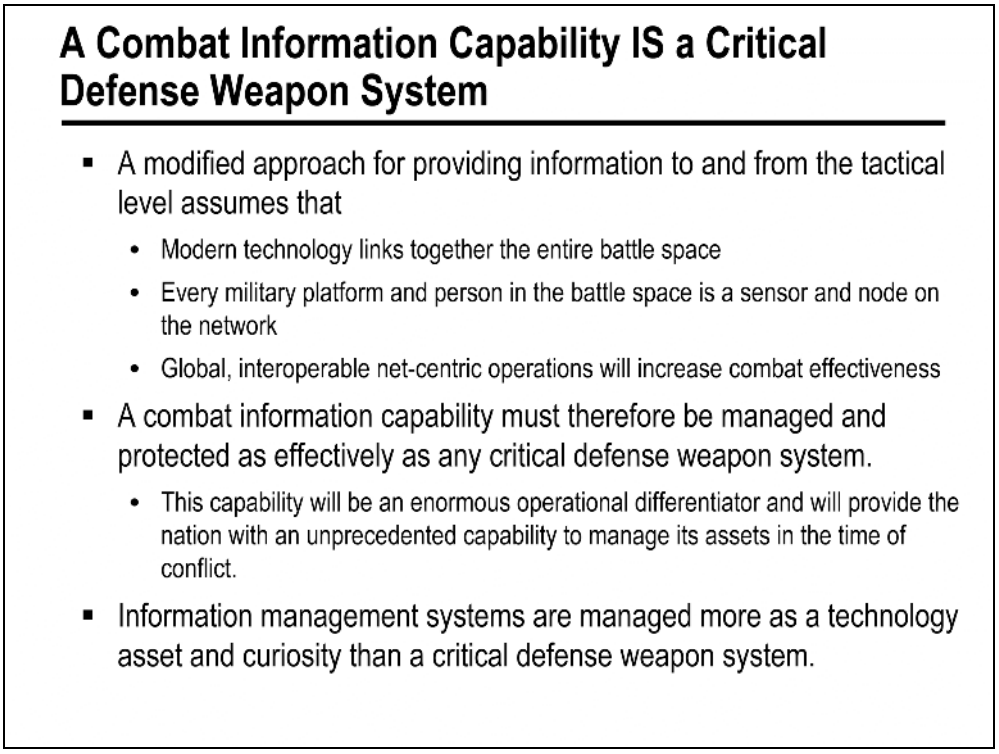
- Introduce the concept of into the GIG architecture in an effort to protect the network against communications failures or attack (ASD/NII)
- Focus additional resources on fielding improved voice and data systems at the tactical level (ASD/NII)
- Provide commanders with rigorous, focused training on the art and science of combat operations integration and information / network management (CJCS)
- Formalize the requirement for an "exercise and training network" linking all echelons (CJCS)
- Adopt a doctrinal joint staff function for combat information management (CJCS)
- Adopt a doctrinal "combat librarian" global reach capability for tactical commanders (CJCS)

The operations panel reinforces the view that cultural characteristics occasionally prevented realization of net-centric operations tenets. A net-centric culture revolves around the belief that the information one element produces may be useful to another element for unforeseen reasons. Thus, the information solution that enables better decision-making is based on the faith that information made available to the enterprise will increase combat power in unspecified forces. Decision makers must turn from the "hunt" for combat power toward the "farming" of combat effects through better combat information management processes like the use of combat information specialists. This cultural change requires leaders and soldiers to take risks in developing new solutions, and an organization that tolerates individuals willing to take risks.

The following recommendations are needed to improve the ability of commanders at all levels to make decisions and win:

- First, develop a forward content staging base to enable bandwith-disadvantaged tactical users timely access to information posted by individuals from across the enterprise.
- Second, provide warfighters—particularly at the last tactical mile—technologically better tools (e.g., the Joint Relay Extension and Battle Universal Gateway Extension at the unit level, and soldier handheld devices operating on the soldier radio waveform) to help them access, share, and manage information.
- Third, improve command and control by implementing a tough, rigorous training system for commanders and units on the best ways to employ and manage combat information capability.
- Finally, create a focused staff function and organic combat information specialist, to enable both soldiers and commanders to optimize information management and make the best possible decisions.

Chapter 6. A CIC is a Critical Defense Weapon System



As discussed in the preceding pages, tactical operations require enhanced networks and data, as well as doctrinal and TTP changes; rigorously, focused training; and a culture of information sharing. This culture assumes that:

- Modern technology links together the entire battlespace, from the strategic to the tactical.
- Every military platform and person in the battlespace is a sensor and node on the network.
- Global, interoperable net-centric operations will increase the combat effectiveness of U.S. military forces.

The preceding section illustrated the power of staging critical combat information forward, a combat information specialist, and doctrinal joint staff functions for combat information management for the tactical commander. Because these attributes of the CIC are so critical to the current and future success of U.S. forces, it is imperative that the CIC is treated not as a force enabler or a mere staff function, but instead as a critical defense weapons system. This capability will be an enormous operational differentiator for U.S. forces and will provide the nation with an unprecedented capability to manage its assets during combat, stabilization and reconstruction, and peacetime contingencies.

The implications of treating this CIC as a critical defense weapon system are significant.

Treating Combat Information Capability as a Defense Weapon System

- Fielding and operating a Combat Information Capability requires, for example:
  - Commanders that are trained and empowered
  - Effective leader development
  - Robust training and exercises
  - The ability to operating effectively with military and non-military partners
  - Equipment and tools
  - System operational management
  - Innovative governance and acquisition
  - A review process to assess progress and adjust trajectory

Commanders need to have the responsibility and authority that 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 information age leaders—that is, they need to understand all aspects of how information can be used to provide their forces a competitive advantage. One of the interesting aspects of unleashing information in an organization is that it will have the effect of flattening the organization, thus enabling a more rapid and effective collaboration.

Effective and robust training is essential to this critical weapon system. 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

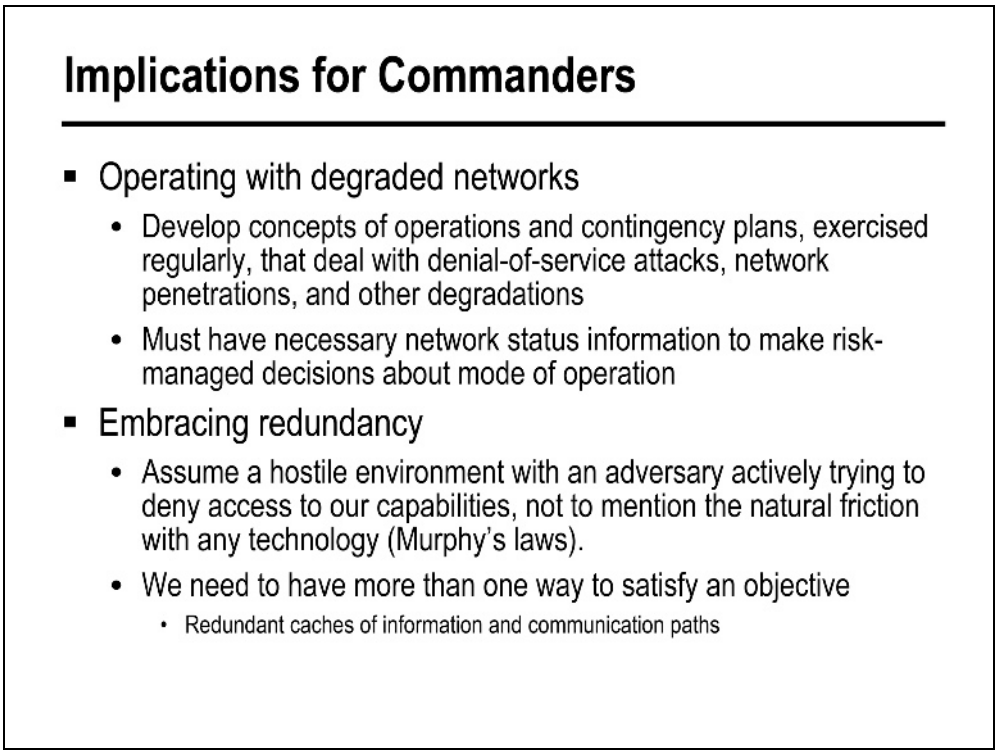
with realistic exercises; therefore this is not simply an academic activity but one that will prepare the warfighters for combat.

In addition to preparing personnel, another aspect of a critical weapon system is the operation of that system. One very important aspect of the operation is ability to interact with other systems and other, non-DOD participants. This includes coalition partners, other government agencies, and non-government organizations. This will certainly require technology to enable information sharing, but it will also require procedures to guide users through the process of sharing information with people you might not ordinarily trust.

Another element of this critical weapon system is the identification and development of the set of the tools necessary for daily operation. This includes tools such as a help desk to support a wide range of users, tools for backup and restoration of the database, and network diagnostics. The combination of these tools, with staff and procedures, will complete the system operational management.

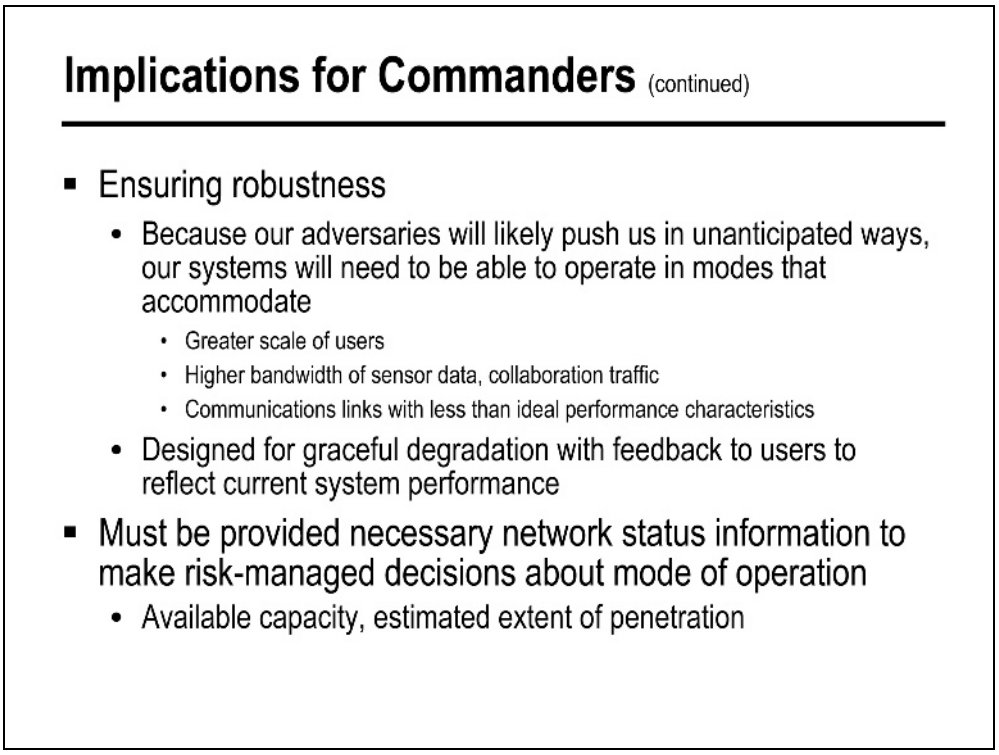
Part of the day-to-day management of the system is the collection of new requirements that emerge from innovative uses of the tools. Many of these requirements can be satisfied with the development of new techniques and procedures, but others may require developmental activities as well. To be able to deal with both the emergent and new development requirements, an innovative governance and acquisition process will be essential to allow the CIC to keep pace with commercial technology.

Finally, in addition to a day-to-day systems management process, a longer term review process to assess progress and adjust trajectory needs to be put in place. One thing that would facilitate this and other processes is the right instrumentation to provide analysts with the opportunity to understand how the system is being used and determine the impediments to reaching its full potential.

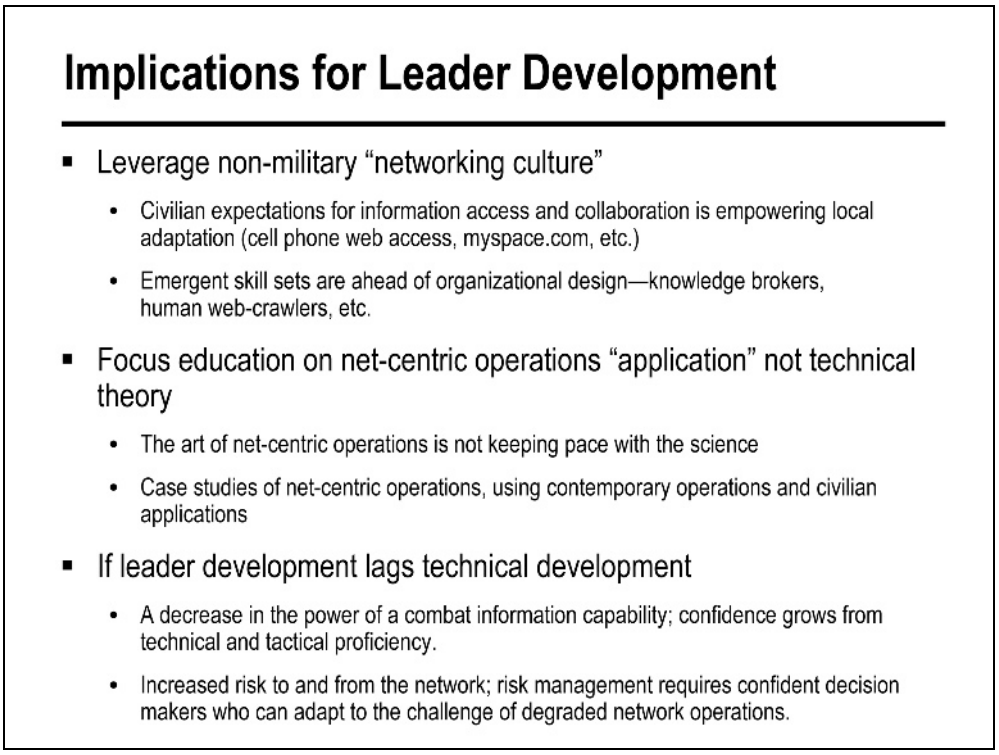


For the tactical commander, operating with degraded systems (weapons, communications, logistics, maneuver) is the norm, not an anomaly. It is this defining quality of the tactical environment that requires modifications to the current deployment of net-centric capabilities. Any solution to challenges at the tactical level must start with the nature of the tactical environment, not the nature of the technical challenge. Two significant concerns voiced by tactical commanders regarding the ability to leverage the power of information are redundancy and robustness.

The redundancy of the network and the critical data on the network is a key attribute given the immediacy of enemy actions, the environment, and even unintentional errors. A practical knowledge of how the various networks work together and what options exist to restore or work around failures are key requirements for commanders in a net-centric battlefield.



Robustness of the information system 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.



Tactical leaders must learn to leverage a nonmilitary "networking culture" to accelerate tactical applications of information networks.

A long standing truism is that all war takes on the attributes of its age. To the extent that this statement is true, network-centric is more a description of the condition of age than it is an operational concept. In the frenzy to develop and deploy information networks it is easy to lose sight of the fact that humans have always created and expanded social and physical networks. The recent phenomenon of creating and expanding into the information domain is a logical progression. The resulting culture[2] is a determining factor of how military operations are organized, as much if not more than any forward-leaning doctrine. The cultural drivers of the military application of networks are uniquely civilian.

2. Culture is defined as "The system of shared beliefs, values, customs, behaviors, and artifacts that the members of society use to cope with their world and with one another, and that are transmitted from generation to generation through learning."

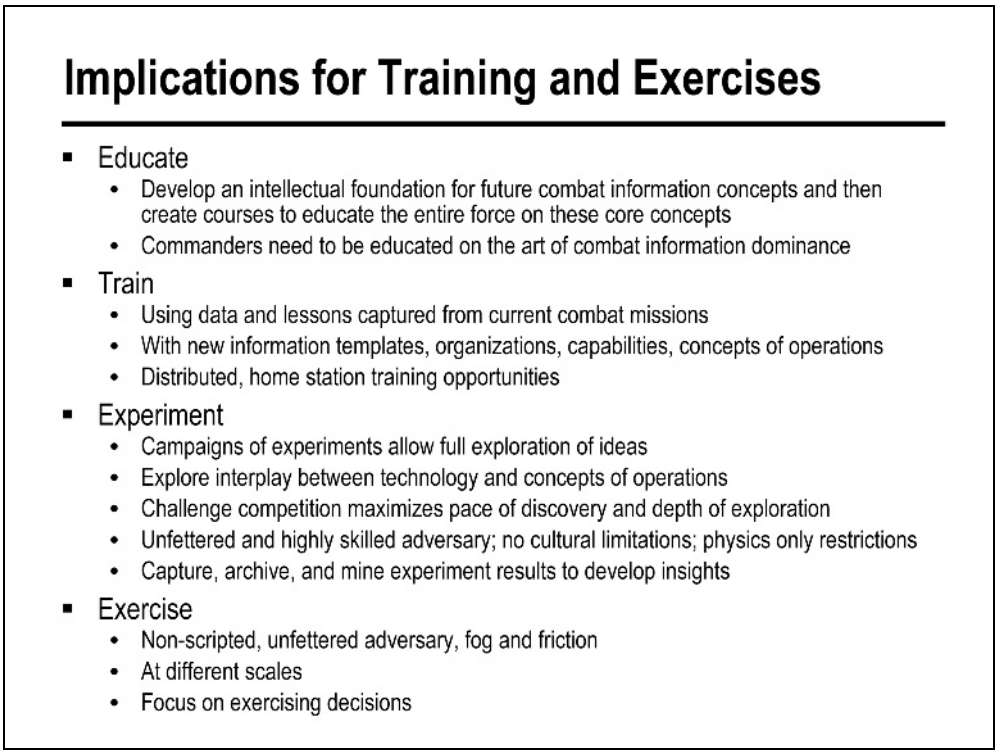
Leveraging the civilian "networking culture" means recognizing solutions that come up from the bottom (the edge) of the system. Solutions applicable to the tactical battlefield are being discovered by the tactical practitioners who are conditioned, in many cases, to solve information challenges in their civilian lives.

The CIC must focus education on net-centric "application," not technical theory. The art of war and the science of war have always been an interactive dynamic. They are two sides of the same coin and often used interchangeably. As net-centric operations have matured into a real, albeit not fully realized or understood capability, the relationship between the science (technology) and the art (commander's realized intent) has become unbalanced. Bringing the world of commercially driven hardware and software into the realm of military operations is occurring at a dizzying pace and is obscuring the distinction. In fact, many of the most virulent critiques of the role and potential of networks in warfare are railing against the tendency to let the science of war overwhelm the art.

The current generation of U.S. military personnel could arguably be counted as the most experienced cohort in the nation's history. The number and variety of military operations during the past 20 years range across all but the highest end of the spectrum of conflict. During this same period of time the impact of information systems and networks on tactical military operations began to play a more dominant role. The tacit knowledge of the current cohort in the application of information networks to the problems of warfare is a national asset. This same generation is living with the exponential changes in the civilian world. It is the combination of living with the most leading-edge and fungible technologies in the civilian world and their operational experiences (good and bad) that makes bottom-up case studies so critical to institutionalizing net-centric operations.

The implications for leader development are critical. There is a cost to allowing combat leaders and network developers to evolve on parallel but divergent paths. Combat leaders need to be trained on net-centric processes and technologies, while network developers need to better understand the challenges of conducting operations in a net-centric environment.

Well-trained and creative leaders can adapt to the challenge of degraded network operations. Operational risk management is a creative, not technical, process.



To realize the full potential of network-centric operations, a full training and education system will need to be established. The first order of business is to develop the intellectual foundation of combat information management. This foundation will become the basis for enhancing and extending the core capabilities, and will also provide commanders the basic tools needed to flourish in this new era to achieve information dominance over the adversary. Once commanders have the freedom to "maneuver" in information space, additional advantages over the adversary will become apparent.

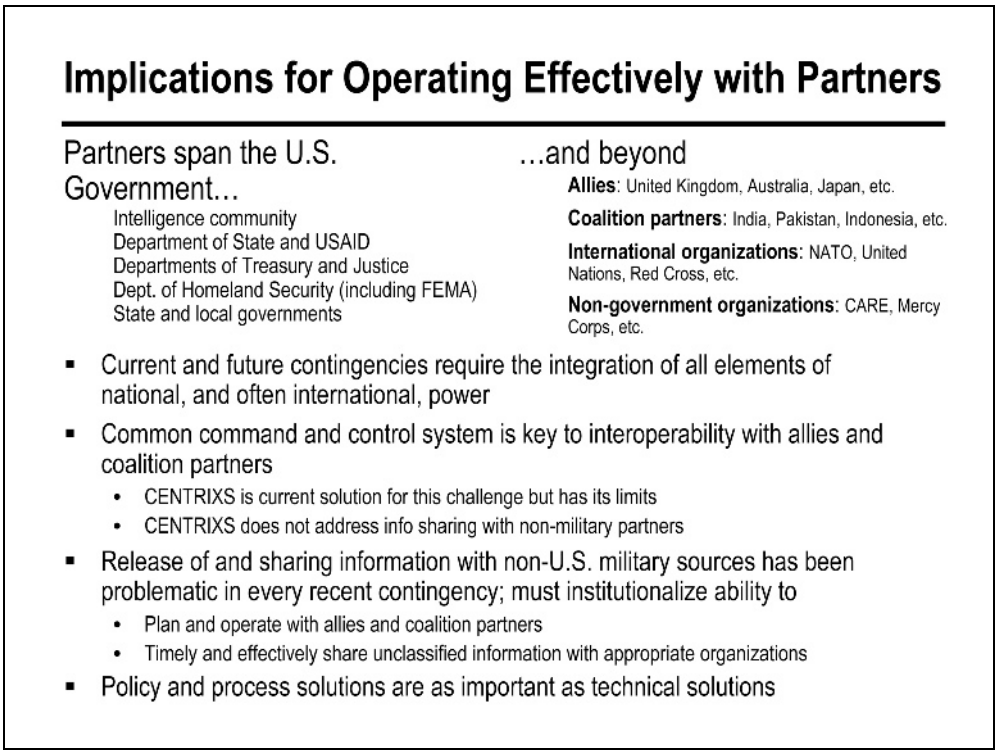
A key component of any major weapons system is the training program. An effective training program will take the results of the education program and make it intuitive. It is important to train with information that is close to what commanders will deal with in combat. The CIC should be developed to allow easy capture of information to support training programs. One aspect of the training should include the ability to develop new information templates on the fly, as well as enabling new organizations and concepts of operations. By including these aspects in the training program, the warfighters will be able to

tune their CIC in combat. The CIC is naturally distributed, providing an opportunity to leverage home station training. The result is the ability to deliver more training at a drastically lower cost.

An important aspect of the CIC is that it will always be evolving. The experience with CPOF has shown that users will develop new information templates and new procedures in order to quickly tune the CIC to the situation at hand. There is a great opportunity to build facilities into this weapon system to allow for continuous experimentation, to maintain dominance in the information domain. Much of the experimentation will explore evolutionary extensions to the capability, but there also needs to be some experimentation devoted to more revolutionary ideas.

To get the most out of experimentation, it should be conducted in a challenge-competitive environment, with unfettered adversaries. Such an approach will ultimately prepare commanders and staff to deal with a degraded CIC capability, and allow them to develop intuition on the elements of the system they can count on. This experimentation process will tune new capabilities that should greatly enhance the core capabilities. Many of the experiments performed may not provide the immediate answers but, over time, a series of experiments should provide users, developers, and technologists key insights into where the high value capabilities are. Many of these experiments can take place in both the training and exercise venues.

The final piece of the training and education element of this critical weapon system is the exercise. Commanders need to be given the time and resources to exercise staff and forces, in as realistic environment as possible. The CIC needs to be exercised at every echelon, and at each level, and the focus needs to be on using the information for making decisions. Decision exercises are a very effective means for bringing education and training together.



One of the defining aspects of today's military environment is that the Untied States has moved well beyond joint operations. Today's operations are fully integrated with key interagency, state and local government, alliance, coalition, host nation, international, and non-governmental organizations and actors. Each of these actors generally operates on its own distinct network, although sustained operations during the past decade in the Balkans and now in Iraq and Afghanistan have led to the development of tools and arrangements for information sharing and collaboration. These efforts, however, have often 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 collaboration of U.S. forces with interagency, coalition, and non-governmental 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. It does address information sharing with non-military partners, because 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 (with the partial exception of the United Kingdom and Australia) 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.

A Combat Information Capability Strategic Plan

- A strategic plan to guide the development of a combat information capability

- This plan should
  - Identify required resources
  - Establish a timeline and identify key milestones for plan implementation

- This plan must address the major actions required to develop a combat information capability:
  - Train commanders to effectively utilize information management infrastructure
  - Concepts for information organization and access
  - Doctrine for combat information capabilities
  - Education and training programs including information management
  - Command and control of combat information capabilities
  - Education in the art of combat information dominance
  - Exercises and experiments for realistic operational scenarios
  - Research on advanced information concepts
  - Lessons learned from current operations

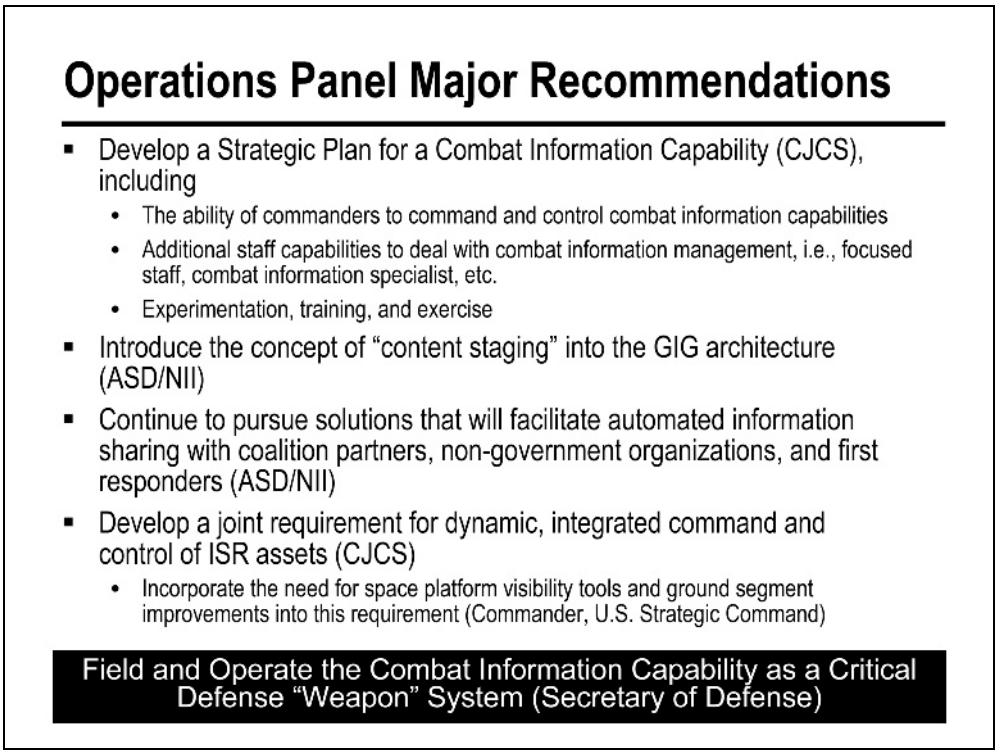
The best way to articulate and develop a CIC across DOD is to create a strategic plan drafted under the authority of the Chairman of the Joint Chiefs of Staff (CJCS). This plan must address the major actions required to develop a true CIC, including:

- concepts for information organization and access
- doctrine for combat information capabilities
- education and training programs including information management
- training for commanders to effectively utilize combat information management infrastructure
- command and control of combat information capabilities
- education in the art of combat information dominance
- exercises and experiments for realistic operational scenarios
- research on advanced information concepts
- lessons learned from current operations

This plan also should

- identify required resources
- establish a timeline for key actions
- identify key milestones for plan implementation

Chapter 7. Major Recommendations



The most significant recommendation of the panel is for the Secretary of Defense to recognize the importance of the CIC as an essential combat capability and declare it a critical defense "weapon system." This recognition means that the essential elements of the CIC will be planned, programmed, and resourced as a weapons system. The assumption is that the GIG and the network operations to the HAIPE will be provided as planned and the weapon system, including support of the warfighter in the theater, will be provided in a single portfolio.

The proposal is similar to the Air Force decision to recognize the Combined Air Operations Center and its extended elements as a weapon system. In doing so, the manning, equipment, training, exercise, research and development, 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 plan.

A significant challenge will be to decide what programs will make up the weapon system elements. Those communications and information management capabilities 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, as well as support for the warfighter outside the HAIPE.

This operational focus requires a strategic plan to lay out the required elements and build them into a CIC. The Chairman of the Joint Chiefs of Staff should develop such a plan with the services as the basis for parts of a program element. The development of the capability and the experimentation, education, training, and exercise of the capability should all be part of the plan.

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 sharing. An essential part of building this capability is to incorporate the need for space platform visibility tools and ground segment improvements into this requirement.

The fragility of present and planned tactical communications requires the concept of a forward content staging base at the tactical level. As an example, the warfighter will load the combat information device with the most current information for the mission. The updates will flow to the device if connectivity is maintained. If communication is lost, the information is still available to the warfighter. When communication is restored, new information again flows. It also reduces the amount of information that must be accessed over narrow bandwidth.

The need to share information with coalition partners, non-government organizations, and first responders still requires more

effective solutions. The Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) needs to pursue solutions that will facilitate automated information sharing. Manual manipulation delays information, making it ineffective in combat and some emergency response operations.

The bottom line is to field and operate the Combat Information Capability as a critical defense weapon system.

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. Glossary

ASD/NII	Assistant Secretary of Defense for Networks and Information Integration
CIC	combat information capability
CJCS	Chairman, Joint Chiefs of Staff
CPOF	Command Post of the Future
DOD	Department of Defense
DSB	Defense Science Board
FEMA	Federal Emergency Management Agency
GIG	global information grid
HAIPE	High Assurance Internet Protocol Encryptors
ISR	intelligence, surveillance, and reconnaissance
NATO	North Atlantic Treaty Organization
OUSD (P)	Office of the Under Secretary of Defense for Policy
SOF	special operations forces
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
UCAV	unmanned combat air vehicle
USAID	United States Agency for International Development