Network Centric Warfare

Department of Defense Report to Congress

27 July 2001

For this report on line go to: www.c3i.osd.mil/NCW/

For more information on NCW go to: www.dodccrp.org/ncw.htm

Table of Contents

List of Figures

List of Tables

Section 1

Introduction and Background

This report completes the Department of Defense's (DoD's) response to the provisions of Section 934 of the Defense Authorization Act for FY01 (Public Law 106-398).[1] This section calls for the Secretary of Defense, in consultation with the Chairman of the Joint Chiefs of Staff, to develop two reports related to Network Centric Warfare (NCW). SEC.934 (c) directs the Secretary, in consultation with the Chairman of the Joint Chiefs of Staff, to submit to the Congress a report on the development and implementation of NCW concepts. SEC. 934(d) directs a study on the use of Joint experimentation for developing NCW concepts and a report on the results of this study.

With respect to the first of these two reports, DoD submitted an interim response to Congress, *Sense of the Report*, in March 2001. This report provided a definition and explanation of terms and an initial perspective on where NCW is today and where it is going in the DoD. With respect to the second of these reports, the U.S. Joint Forces Command prepared and submitted a report on the status of NCW and Joint Experimentation in March 2001. This report is the final submission associated with SEC. 934 (c) and completes DoD's response to Congress pursuant to Section 934 of Public Law 106-398. It provides a thorough explanation of NCW concepts, details relevant DoD activities, assesses DoD progress, and describes the way ahead.

1.1 Congressionally Directed Action

Section 934 of Public Law 106-398 stipulated that areas listed below be addressed:

SEC. 934. NETWORK CENTRIC WARFARE

1. Findings. Congress makes the following findings:

   (a) *Joint Vision 2020* set the goal for the DoD to pursue information superiority in order that joint forces may possess superior knowledge and attain decision superiority during operations across the spectrum of conflict.

   (b) One concept being pursued to attain information superiority is known as NCW. The concept of NCW links sensors, communications systems, and weapons systems in an interconnected grid that allows for a seamless information flow to warfighters, policy makers, and support personnel.

---

1 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ398.106

(c) The Joint Staff, the Defense Agencies, and the military departments are all pursuing various concepts related to NCW.

2. Goal. It shall be the goal of the DoD to fully coordinate various efforts being pursued by the Joint Staff, the Defense Agencies, and the military departments as they develop the concept of NCW.

3. Report on NCW

(a) The Secretary of Defense shall submit to the congressional defense committees a report on the development and implementation of NCW concepts within the DoD. The report shall be prepared in consultation with the Chairman of the Joint Chiefs of Staff.

(b) The report shall include the following:

i. A clear definition and terminology to describe the set of operational concepts referred to as "network centric warfare."

ii. An identification and description of the current planned activities by the Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff, and the United States Joint Forces Command relating to NCW.

iii. A discussion of how the concept of NCW is related to the strategy of transformation as outlined in the document entitled *Joint Vision 2020*, along with the advantages and disadvantages of pursuing that concept.

iv. A discussion on how the Department is implementing the concepts of network centric warfare as it relates to information superiority and decision superiority articulated in *Joint Vision 2020*.

v. An identification and description of the current and planned activities of each of the Armed Forces related to network centric warfare.

vi. A discussion on how the Department plans to attain a fully integrated, joint command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capability.

vii. A description of the joint requirements under development that will lead to the acquisition of technologies for enabling network centric warfare and whether those joint requirements are modifying existing service requirements and vision statements.

viii. A discussion of how DoD activities to establish a joint network centric capability are coordinated with other departments and agencies of the United States and with United States allies.

ix. A discussion of the coordination of the science and technology investments of the military departments and Defense Agencies in the development of future joint network centric warfare capabilities.

x. The methodology being used to measure progress toward stated goals.

4. Study on the Use of Joint Experimentation for Developing NCW Concepts.

   (a) The Secretary of Defense shall conduct a study on the present and future use of the joint experimentation program of the DoD in the development of NCW concepts.

   (b) The Secretary shall submit to the congressional defense committees a report on the results of the study. The report shall include the following:

      i. A survey of and description of how experimentation under the joint experimentation at United States Joint Forces Command is being used for evaluating emerging concepts in network centric warfare.

      ii. A survey of and description of how experimentation under the joint experimentation of each of the armed services are being used for evaluating emerging concepts in network centric warfare.

      iii. A description of any emerging concepts and recommendations developed by those experiments, with special emphasis on force structure implications.

      iv. The Secretary of Defense, acting through the Chairman of the Joint Chiefs of Staff, shall designate the Commander in Chief (CINC) of the United States Joint Forces Command to carry out the study and prepare the report required under this subsection.

5. Time for Submission of Reports. Each report required under this section shall be submitted not later than March 1, 2001.

CONFERENCE REPORT LANGUAGE HR 016-945, pg. 839.

Network Centric Warfare (sec. 934)

The House bill contained a provision (sec. 907) that would require the Secretary of Defense to submit a report to the congressional defense committees outlining the efforts of the Department to define and integrate network centric warfare concepts into its vision for future military operations.

The Senate amendment contained a similar provision (sec. 906) that would require the Secretary of Defense to submit three reports: (1) a report on the implementation of NCW principles; (2) a study on the use of joint experimentation for developing NCW concepts; and (3) a report on science and technology programs to support NCW concepts.

The House recedes with an amendment that would establish a requirement for the Secretary of Defense to submit two reports: (1) a report on implementation of NCW principles; and (2) a study on the use of joint experimentation for developing NCW concepts. The amendment would further clarify specific elements of the information to be included in the reports.

1.2 Mapping From SEC. 934 to Report

The Department recognized that this direction by the Congress provided an opportunity not only to assemble a comprehensive report on its thinking and activities related to NCW, but also to stimulate a continuing dialogue both within DoD and between DoD and the Congress on this subject.

The report maps to the tasking by Congress as follows:

1. **A clear definition and terminology to describe the set of operational concepts referred to as "Network Centric Warfare."**

   These activities are discussed in numerous places throughout the report. The following sections focus upon the strategy and policy elements related to enabling and facilitating the development of NCW concepts and capabilities. Joint Forces Command achievements were discussed in the report submitted on 8 March 2001, included in Appendix H of this report.

   - Section 2.2.3 relates Decision Superiority and Knowledge Superiority to cognitive domain operations.
   - Section 3.2 provides definitions of terms used in describing NCW.
   - Section 3.3 addresses concepts that use different terminology but are related to the goals of network centricity.
   - Section 5.2 defines the term Infostructure.
   - Section 7 describes the Mission Capability Package (MCP) concept.

2. **An identification and description of the current and planned activities by the Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff, and the United States Joint Forces Command relating to NCW.**

   - Section 7.1.1 describes the strategy of Co-Evolution to develop NCW.
   - Section 9.2.2.1 describes the activities of the Combined Communications Electronics Board (CCEB) to coordinate C4ISR planning.
   - Section 9.2.2.2 describes Coalition Interoperability initiatives being conducted under the CCEB.
   - Section 9.3 describes the 1999 recommendations of the Defense Science Board for the establishment of a focal point for coordinating the Global Information Grid (GIG) as a key transformative activity in the DoD.
   - Section 10.3 describes changes in the Acquisition system to expedite development of NCW.

- Section 11 provides a detailed overview of ongoing developments and initiatives relating to NCW within the Office of the Secretary of Defense, the Joint Chiefs of Staff, and the United States Joint Forces Command.
- Appendix H provides the text of the U.S. Joint Forces Command report to Congress about activities related to NCW and Joint Experimentation.

3. **A discussion of how the concept of NCW is related to the strategy of transformation as outlined in the document entitled *Joint Vision 2020*, along with the advantages and disadvantages of pursuing that concept.**
   - Section 2 describes the relationship between NCW and DoD Transformation, including the relationship between NCW and *Joint Vision 2020.*
   - Section 3.4 discusses how Information Superiority and NCW transform the practice of nine fundamental principles of war.
   - Section 10.4.7 describes how science and technology success is dependent upon co-evolution of technology, doctrine, and organization.
   - Section 9.2.2 describes GIG Architecture Development
4. **A discussion of how the Department is implementing the concepts of NCW as it relates to information superiority and decision superiority articulated in *Joint Vision 2020*.**
   - Section 5 describes the Prerequisites that lead to implementation of NCW.
   - Section 7 describes the DoD NCW Implementation Strategy.
   - Section 6 describes the things that are enablers of NCW.
   - Section 9.2 describes Policy and Governance that guide the CINCs, Services, and Agency in development of the Global Information Grid.
5. **An identification and description of the current and planned activities of each of the Armed Forces relating to NCW.**
   - Section 3.3.1 contains examples of Service NCW Concepts that are developing NCW.
   - Section 4 provides an Overview of Service Visions and Concepts and summarizes the individual Service concepts that are stated in detail in Appendix A.
   - Section 8.2 provides a detailed discussion of experimentation conducted by the Services that provides evidence of the value of NCW.

- Section 8.2.1.1 describes U.S. Air Force Air-to-Air Mission experimentation in NCW.
- Section 8.2.1.2 describes U.S. Army Advanced Warfighting Experiment (AWE) Maneuver experimentation activity.
- Section 8.2.1.6 describes U.S. Air Force Split-Based Operations.
- Section 11 summarizes NCW-Related Initiatives and Programs and provides links to detailed descriptions in Appendix E.
- Appendix E provides Service and Agency NCW-related initiatives and programs.

6. **A discussion of how DoD plans to attain a fully integrated Joint C4ISR capability.**
   - Section10.3.1 describes how the Defense Acquisition System is emphasizing **Joint** interoperability requirements in development of C4ISR systems.
   - Section 9.2.1 lists Guidance and Policy Memoranda for CINCs, Services, and Agencies, emphasizing integrated **Joint** development of NCW implementation.
   - Section 9.2.2 describes GIG Architecture development.
   - Appendix E, paragraph 6, describes NCW-related initiatives and programs by BMDO to ensure **Joint** integration of Service and Agency efforts in support of the BMDO mission to provide Ballistic Missile Defense.
   - Appendix G lists analysis, experimentation, and Advanced Concept Technology Demonstrations (ACTD) activities that address multiple NCW focus areas.
7. **A discussion of the Joint requirements under development that will lead to the acquisition of technologies for enabling NCW and whether those Joint requirements are modifying existing service requirements and vision statements.**
   - Section 10.2 describes the revised Requirements Generation System of the DoD.
   - Appendix B, paragraphs 2.3 and 2.4, describe how the Navy is developing new warfare requirements processes to achieve NCW goals.
   - Appendix B, paragraph 3, describes how the U.S. Marine Corps is developing new warfighting requirements processes to achieve NCW goals.
   - Appendix E, paragraph 3 (Navy Initiatives and Programs), describes how the Navy is organizing Mission Capability Packages that include: GIG, and Theater Air and Missile Defense (TAMD). All Navy C4ISR programs are connected to one or more MCP, thus giving visibility to the contribution of individual programs to the Joint Mission.

8. **A discussion of how DoD activities to establish a Joint network-centric capability are coordinated with other departments and agencies of the United States and with United States Allies.**

   – Section 8.2.1.2.3 describes UK Exercise Big Picture 1 experimentation with NCW.

   – Section 8.2.1.3 describes U.S. Navy experimentation with Combined Forces Command Korea.

   – Section 8.2.1.5 describes real world operations with Coalition forces during *Operation Allied Force*, the Kosovo air operation.

   – Section 9.2.2.1 describes the activities of the Combined Communications-Electronics Board Coalition Wide Area Network to coordinate C4ISR planning.

   – Section 9.2.2.2 describes Coalition Interoperability initiatives being conducted under the CCEB.

   – Section 11.7 discusses engagement with Allies and Partners and specific initiatives to improve interoperability.

   – Appendix B, paragraph 1.4.3, describes Army concepts for Allied interoperability.

   – Appendix C, paragraph 2.2, describes Navy experimentation with Allied forces to improve Allied interoperability.

   – Appendix C, paragraph 4, explains the U.S. Air Force concept of operations for Allied interoperability.

   – Appendix E, paragraph 3.3.3, describes the Navy initiative for Allied interoperability with Information Technology for the Twenty-first Century.

9. **A discussion of the coordination of the science and technology investments of the military departments and Defense Agencies in the development of future Joint NCW capabilities.**

   – Section 5.4 describes research required to build new capabilities in the cognitive domain.

   – Section 10.4 describes the DoD process of coordination of research and development investments and emphasizes the importance of NCW for DoD Science &Technology.

   – Section 10.4 refers to specific ACTDs that are developing science and technology products for NCW.

- Appendix E, paragraph 3.4.4, details the Navy Knowledge Superiority and Assurance science and technology program.
- Appendix F describes Defense Technology Objectives supporting NCW.

10. The methodology being used to measure progress towards stated goals.

- Section 3.2.8 establishes central NCW Hypotheses.
- Section 8 addresses NCW Assessment, Analysis, and Evaluation, Including Evidence of NCW Impacts.
- Section 8.1.2 discusses Measuring DoD Progress Toward a Network-Centric Force.

1.3 Organization of the Report

This report to the Congress on NCW consists of a stand-alone Executive Summary, a detailed report, and stand-alone unclassified and classified Appendixes.

The unclassified appendixes include descriptions of Service and Agency NCW-related visions, concepts, initiatives, and programs. A classified appendix provides details of evidence to date regarding the mission effectiveness of NCW concepts and capabilities.

The main body of the report is organized around three primary themes. The following roadmap summarizes the focus of these three themes:

About NCW (provides an overview of NCW concepts and theory, discusses the role of NCW in DoD transformation, and provides an overview of Service Visions and Concepts for NCW)

Section 1: Introduction and Background

Section 2: DoD Transformation

Section 3: NCW Concepts and Theory

Section 4: Overview of NCW Service Visions and Concepts

Road to NCW (prerequisites for NCW; enabling NCW; DoD NCW implementation strategy; approaches to NCW assessment, analysis, and evaluation; and evidence compiled to date of the power and promise of NCW)

Section 5: Prerequisites for NCW

Section 6: Enabling NCW

Section 7: DoD NCW Implementation Strategy

Section 8: NCW Assessment, Analysis, and Evaluation, Including Evidence of NCW Impacts

Implementing NCW (the key role of the GIG, DoD's strategy, policies and procedures DoD initiatives and programs designed to make NCW a reality, an assessment of progress to date, and recommendations for accelerating our rate of progress)

Section 9: Global Information Grid

Section 10: NCW and DoD—Policies and Processes

Section 11: Current and Planned NCW-Related Initiatives and Programs

Section 12: Findings and Conclusions

1.4 Relationship to the Quadrennial Defense Review (QDR)

The drafting of this report preceded the start of the QDR currently in progress, and will be completed prior to its conclusion. A draft of this report and other material related to NCW, have been made available to those engaged in the QDR. As a result, QDR discussions have been informed with respect to network-centric concepts, their relationship to transformation, and the potential of NCW to dramatically increase combat power.

The QDR terms of reference direct that plans and programs take full account of the transition of Space, Information, and Intelligence assets from enablers of current U.S. military activities to core capabilities of the future force. This clearly would pave the way for Network Centric Operations (NCO). Furthermore, plans and programs under consideration in the areas of C4ISR, IO, and space are being assessed with respect to their potential contributions to network-centric capabilities. Since QDR deliberations are ongoing, it would be premature to include specifics in this NCW report.

Section 2

DoD Transformation

DoD is fully committed to creating a 21st century military by taking advantage of Information Age concepts and technologies, particularly new "business models" and information technologies.

2.1 What is DoD Transformation?

Information technology (IT) provided the building blocks for the Internet, radically restructured the economics of information, and enabled new ways of doing business that have created a "new economy." These same dynamics can help DoD transform its primarily platform-centric force to a network-centric force—a force with the capability to create and leverage an information advantage and dramatically increase combat power, a force that will enhance the Department's capability to preserve global peace and dominate across the spectrum of military operations if required to restore tranquility.

The Commander in Chief, President Bush, amplified this commitment to transformation and highlighted the enabling role of IT during his remarks at the U.S. Naval Academy Commencement on May 25, 2001, when he stated:

> *…We must build forces that draw upon the revolutionary advances in the technology of war that will allow us to keep the peace by redefining war on our terms. I'm committed to building a future force that is defined less by size and more by mobility and swiftness, one that is easier to deploy and sustain, one that relies more heavily on stealth, precision weaponry and information technologies.*

Few within the DoD will dispute the importance of the need for transformation. However, transformation clearly means different things to different people. For some, it is synonymous with modernization and focused on material acquisition. For others, transformation goes beyond normal modernization, which is evolutionary in nature ('bigger, faster, further'), to embrace innovative and fundamental changes in the way the armed forces operate.[2]

Recently, the Secretary of Defense has approved definitions of **transformation** and **modernization** for use in the QDR. These definitions are provided in the box on the next page.

---

2 Joint Staff Whitepaper on "Transforming to *Joint Vision 2020*," February 2001.

Transformation: the evolution and deployment of combat capabilities that provide revolutionary or asymmetric advantages to our forces.

Modernization: the replacement of equipment, weapons systems, and facilities in order to maintain or improve combat capability, upgrade facilities, or reduce operating costs.

Even those who agree on the importance and necessity of transformation may disagree on the risks associated with transformation. Complicating matters further, some critics of transformation argue that the current security environment does not justify the cost and risk that transformation would entail.[3]

This report takes the position that the appropriate application of IT, in conjunction with other technologies (such as stealth and precision weaponry), can both modernize the force ***and*** enable changes in the way the armed forces operate. With this premise, it is clear that a DoD transformation that leverages IT, by necessity, must involve not only adapting to new systems capabilities but also developing new paradigms for their use.

The challenge for DoD is to harness the power of information technologies to develop concepts of operation and command and control approaches that will be information-driven rather than uncertainty-driven. Our ability to integrate across a number of dimensions will determine how successful we are in bringing all of the available information and all of our available assets to bear in any given situation or circumstance. These dimensions include time, echelons, functions, geography, agencies, and coalitions. DoD needs to assemble "systems of systems" (SoS) (with co-evolved organizations, doctrines, processes, and information flows) that will enable this integration to occur. For example, temporal integration (such as getting the commander's intent to all relevant subordinates at the same time) promises to result in less confusion and to reduce the fog of war while at the same time enabling a greater degree of simultaneity. The same Information Age technologies will also enable *continuous* Command and Control (C2) processes, to replace the cyclical processes of the Industrial Age. Integration across echelon and function can also reduce the fog of war and help ensure coordination of activities such as logistics, operations, and intelligence. Integration across space or geography is key to the ability to mass effects without the need to mass forces. Finally, integration of coalition operations and interagency efforts is essential to achieve a unified effort, one of our most urgent challenges. The ultimate goal of DoD transformation must be the development of a force that provides the warfighting commander in chief (CINC) with the capability to dominate across the spectrum of operations within the context of the future security environment.

---

3 Steven Metz, *American Strategy: Issues and Alternatives for the Quadrennial Defense Review,* p. vii.

2.2 *Joint Vision 2020* and NCW

2.2.1 *Joint Vision 2020*

Joint Vision 2020 builds upon and extends the conceptual template established by *Joint Vision 2010* to guide the continuing transformation of America's Armed Forces. The primary purpose of those forces has been, and will be, to fight and win the Nation's wars. The overall goal of the transformation described in *Joint Vision 2020* is the creation of a force that is dominant across the full spectrum of military operations—persuasive in peace, decisive in war, preeminent in any form of conflict.[4]

If the U.S. Armed Forces are to be faster, more lethal, and more precise in 2020 than they are today, the United States must continue to invest in and develop new military capabilities. *Joint Vision 2020* describes the ongoing transformation to those new capabilities. As first explained in *Joint Vision 2010*, and dependent upon realizing the potential of the information revolution, today's capabilities for maneuver, strike, logistics, and protection will become dominant maneuver, precision engagement, focused logistics, and full dimensional protection.[5]

The Joint Force, because of its flexibility and responsiveness, will remain the key to operational success in the future. The integration of core competencies provided by the individual Services is essential to the Joint team, and the employment of the capabilities of the Total Force (active, Reserve, Guard, and civilian members) increases the options for the commander and complicates the choices of our opponents. To build the most effective force for 2020, U.S. Armed Forces must be fully Joint: intellectually, operationally, organizationally, doctrinally, and technically.[6] The overarching focus of *Joint Vision 2020* is full spectrum dominance—achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection. Improved capabilities for Joint C2 are key to achieving this goal.

Joint Vision 2020 also highlights the key role that multinational operations and interagency operations must play in enabling full spectrum dominance. In addition, *Joint Vision 2020* describes the key role that organizational and conceptual innovation must play in conjunction with technological innovation to enable transformation.

---

4 *Joint Vision 2020*. Office of Primary Responsibility; Director for Strategic Plans and Policy, Joint Staff/J5; Strategy Division, Published by: U.S. Government Printing Office, Washington, DC, June 2000, p. 1. www.dtic.mil/JV2020.

5 *Ibid*, p. 1-2

6 *Ibid.*, p. 2.

2.2.2 *Joint Vision 2020* and Network Centric Warfare

Network Centric Warfare is a warfighting concept that allows us to achieve *Joint Vision 2020* operational capabilities. It is a maturing approach to warfare that is specifically designed to achieve the multi-dimensional integration and synergies necessary to realize DoD transformation goals.

Network Centric Warfare allows the force to achieve an ***asymmetric information advantage.*** This information advantage is achieved, to a large extent, by allowing the force access to a previously unreachable region of the information domain—the network-centric region—that is broadly characterized by both increased information richness and increased information reach, as portrayed in Figure 2-1.[7] NCW is predicated upon dramatically improved capabilities for information sharing. When paired with enhanced capabilities for sensing, information sharing can enable a force to realize the full potential of dominant maneuver, precision engagement, full dimensional protection, and focused logistics.

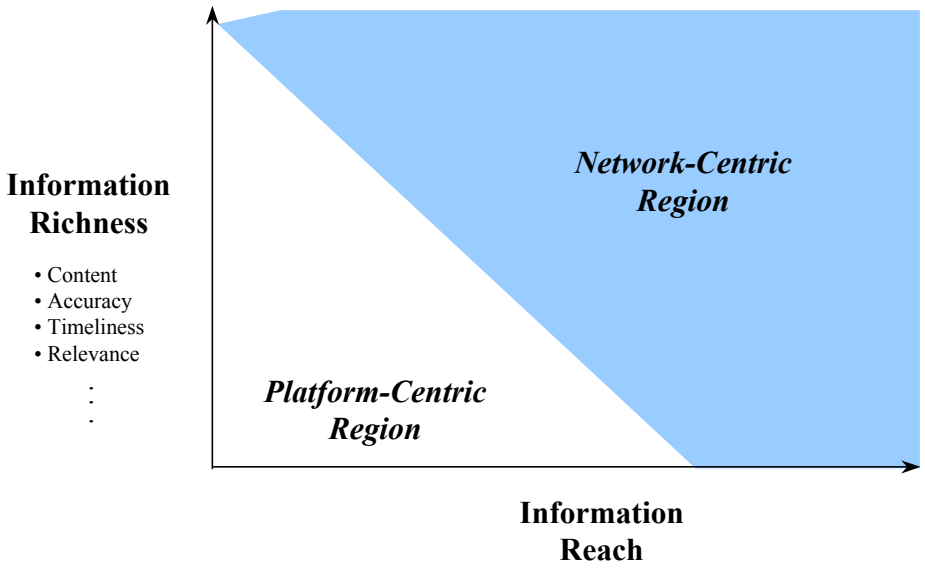


Figure 2-1. Network-Centric Region of the Information Domain

---

[7] John J. Garstka, "Network Centric Warfare: An Overview of Emerging Theory," *PHALANX,* December 2000, Vol. 33, No. 4, p. 1, 28-33.

▲ Network-centric capabilities allow the force to attain an improved information position that can partially "lift the fog of war" and enable commanders to improve their decision making and fight in ways that were not previously possible.

Realization of the full potential of Network Centric Warfare requires not only technological improvements, but the continued evolution of organizations and doctrine and the development of relevant training that will enable U.S., Allied, and coalition forces to develop and sustain an asymmetric advantage in the information domain.

The relationship between NCW and *Joint Vision 2020* operational concepts is discussed below, starting with relationship between NCW and Information Superiority. A much broader discussion of the collection of concepts and underlying assumptions that are associated with Network Centric Warfare is provided in Section 3 and amplified in greater depth in the remainder of the report.

2.2.3 Information Superiority and Decision Superiority

2.2.3.1 Information Superiority

Joint Vision 2020 states that information superiority is fundamental to the transformation of the operational capabilities of the Joint force. Central to this premise is the explicit acknowledgement of the ongoing "information revolution" and its impact in creating a qualitative change in the information environment that will result in profound changes in the conduct of military operations. *Joint Vision 2020* characterizes information superiority as having the following attributes:[8]

- A state of imbalance in one's favor in the information domain
- State of imbalance is potentially transitory in nature
- State of imbalance is enabled, in part, by information operations
- Information contributing to this state is not perfect—the "fog of war" is reduced—but not eliminated

These and other attributes of information superiority are explored in greater depth in Section 3.

The ability of the Joint force to achieve an asymmetric information advantage will be dependent upon its ability to get accurate and timely information for all aspects of the battlespace, analyze it, and disseminate militarily exploitable information to the commanders

---

8 *Ibid*, p. 8-10, 28-30.

of space, air, land, and undersea forces while denying adversaries access to that information.[9] The impact of this degree of information advantage is emerging from Joint and Service experimentation. One of the key insights that has been gained to date is that networking enables a force to share information to a degree unprecedented in military operations. This previously unachievable capability, currently manifested in information constructs such as the common operational picture (COP), will be a principal enabler of the increased combat power that will be generated by the 2020 operational concepts.

2.2.3.2 Decision Superiority

Joint Vision 2020 recognizes that an information advantage can be effectively translated into a competitive advantage when it enables commanders and their forces to arrive at better decisions and implement them faster than an opponent can react. In a noncombat situation, this translates to the capability to make decisions at a tempo that allows the force to shape the situation or react to changes and accomplish its mission. These collective capabilities are referred to as "decision superiority."[10] Decision superiority results from superior information filtered through a warfighter's experience, knowledge, training, and judgement. A commander's capability to achieve decision superiority is enhanced through the expertise of supporting staffs and the efficiency of associated processes.

Joint Vision 2020 also states that decision superiority does not automatically result from information superiority, that organizational and doctrinal adaptation, relevant training and experience, and the proper command and control mechanisms and tools are equally necessary. In addition, it is important to note that decision superiority does not refer solely to the capability of commanders to make decisions, but rather to an improved capability of a warfighting force to make decisions.

A real world example of the power of decision superiority exists at the tactical level in the air-to-air mission. In this mission area, dramatic increases in information sharing enabled by networking provide warfighters with significantly enhanced shared situational awareness. This enhanced situational awareness enables aircrews to fight smarter and make better decisions faster by employing new tactics, techniques, and procedures. As a result, they are able to fight smarter and win more decisively. An operational special project conducted by the USAF in the 1990s demonstrated how pilots flying F-15Cs equipped with tactical data links could increase mission effectiveness (measured in kill ratios) by over 100%. Across a broad spectrum of engagement scenarios, from one-on-one engagements to eight vs. sixteen

---

9 Transformation Study Report, "Transforming Military Operational Capabilities," Executive Summary, p. 20.

10 *Joint Vision 2020,* p. 8-10.

engagements in day and night conditions, the combination of information advantage and a decision-making advantage resulted in a 2.6-fold increase in kill ratios. An in-depth discussion of this powerful example of the power of NCW is provided in Section 8.2.

2.2.4 Dominant Maneuver

Dominant Maneuver is the ability of Joint forces to gain positional advantage with decisive speed and overwhelming operational tempo in the achievement of assigned military tasks. Widely dispersed Joint air, land, sea, amphibious, special operations, and space forces, capable of scaling and massing force or forces and the effects of fires as required for either combat or noncombat operations, will secure advantage across the range of military operations through the application of information, deception, engagement, mobility, and counter-mobility capabilities.

The Joint force capable of dominant maneuver will possess unmatched speed and agility in positioning and repositioning tailored forces from widely dispersed locations to achieve operational objectives quickly and decisively. The employment of dominant maneuver may lead to achieving objectives directly, but can also facilitate employment of the other operational concepts. For example, dominant maneuver may be employed to dislodge enemy forces so they can be destroyed through precision engagement. At times, achieving positional advantage will be a function of operational maneuver over strategic distances. Overseas or US-based units will mass forces or effects directly to the operational theater. [11]

Network Centric Warfare capabilities will support the conduct of dominant maneuver by enabling:

- Adaptive and concurrent planning
- Coordination of widely dispersed units
- Gathering of timely feedback on the status, location, and activities of subordinate units
- Anticipation of the course of events leading to mission accomplishment

The Joint force will also be capable of planning and conducting dominant maneuver in cooperation with interagency and multinational partners with varying levels of commitment and capability.

The capability to rapidly mass force or forces and the effects of dispersed forces allows the Joint force commander to establish control of the battlespace at the proper time and place. In a conflict, this ability to attain positional advantage allows the commander to employ

---

11 *Ibid.,* p. 20.

decisive combat power that will compel an adversary to react from a position of disadvantage, or quit. In other situations, it allows the force to occupy key positions to shape the course of events and minimize hostilities or react decisively if hostilities erupt. And in peacetime, it constitutes a credible capability that inhibits potential adversaries while reassuring friends and Allies.[12]

Beyond the actual physical presence of the force, dominant maneuver creates an impact in the minds of opponents and others in the operational area. That impact is a tool available to the Joint force commander across the full range of military operations. In a conflict, for example, the presence or anticipated presence of a decisive force might well cause an enemy to surrender after minimal resistance. During a peacekeeping mission, it may provide motivation for good-faith negotiations or prevent the instigation of civil disturbances. In order to achieve such an impact, the commander will use information operations as a force multiplier by making the available combat power apparent without the need to physically move elements of the force. The Joint force commander will be able to take advantage of the potential and actual effects of dominant maneuver to gain the greatest benefit.[13]

Insight into the relationship between information superiority and decision superiority and its capability to enable dominant maneuver can be gained from the following concrete example from the recently completed Division Capstone Exercise (DCX)—Phase I (described at length in Section 8.2.1.2.5). The following quote from LTC "Ric" Rierra, a battalion commander who participated in this exercise, highlights how a common operational picture can provide commanders at the tactical level with the capability to make better decisions, and in some cases, fight in ways that were not previously possible. During this exercise, the OPFOR had planned a trap for LTC Riera's battalion, which consisted of two companies of M2A3s Bradley fighting vehicles reinforced by a company of M1A2-SEP tanks. The OPFOR let his battalion proceed with an attack up a valley as the OPFOR pulled back, and then launched a rear attack, making wide hooks around both of his flanks.

> *As a battalion commander, I need to see platoons. I need to see what platoons are doing. I don't need to see all the things on the battlefield, just the things that are important to me. That makes* ***decisions*** *easier.*
>
> *I had to fight in one direction and then turn and fight in another. Two things enabled me to do that: the soldiers with their level of training, and this command*

---

12 *Ibid.,* p. 20.

13 *Ibid.,* p. 21.

*and control system that **allowed me to make better decisions**. It's not perfect, but it's a lot better than I've ever had. It's powerful stuff.*[14]

LTC "Ric" Riera, USA
2nd Battalion, 8th Infantry, 4th ID

2.2.5 Precision Engagement

Precision Engagement is the ability of Joint forces to locate, survey, discern, and track objectives or targets; select, organize, and use the correct systems; generate desired effects; assess results; and reengage with decisive speed and overwhelming operational tempo as required, throughout the full range of military operations.

Simply put, precision engagement is effects-based engagement that is relevant to all types of operations. Its success depends on in-depth analysis to identify and locate critical nodes and targets. ***The pivotal characteristic of precision engagement is the linking of sensors, delivery systems, and effects. NCW concepts and capabilities effectively network sensors, command and control, and shooters to engage with precision across the depth and breadth of the battlespace.***

In the Joint force of the future, this linkage will take place across Services and will incorporate the applicable capabilities of multinational and interagency partners when appropriate. The resulting system of systems will provide the commander the broadest possible range of capabilities in responding to any situation, including both kinetic and nonkinetic weapons capable of creating the desired lethal or nonlethal effects.[15]

The concept of precision engagement extends beyond precisely striking a target with explosive ordnance. ***Network Centric Warfare capabilities will enhance the capability of the Joint force commander to understand the situation, determine the effects desired, select a course of action and the forces to execute it, accurately assess the effects of that action, and reengage as necessary while minimizing collateral damage.***

For example, Fleet Battle Experiment (FBE)-Foxtrot, which was conducted in conjunction with Joint and combined exercise in the Arabian Gulf in November—December 1999, demonstrated the potentially dramatic impact that robust Joint command and control can have in enabling precision engagement and achieving CINC warfighting objectives. FBE-Foxtrot employed a Joint Fires Element in conjunction with improved capabilities for information sharing to engage a broad class of targets across the depth and breadth of the battlespace. This improved capability for precision engagement enabled the Maritime

---

14 Dennis Steele, "Dust, Digits, and Steel: Launching Warfare's Future," *Army*, June 2001, p. 36.

15 *Joint Vision 2020*, p. 22.

Component Commander to employ parallel operations to coordinate the protection for in-stride anti-submarine warfare and mine warfare efforts and open a key choke point on a timeline not previously possible. (An overview of the Fleet Battle Experiment series is provided in Appendix C, paragraph C.2.3).

During conflict, the commander will use precision engagement to obtain lethal and nonlethal effects in support of the objectives of the campaign. This action could include destroying a target using conventional forces, inserting a special operations team, or even the execution of a comprehensive psychological operations mission. In other cases, precision engagement may be used to facilitate dominant maneuver and decisive close combat. The commander may also employ nonkinetic weapons, particularly in the arena of information operations where the targets might be key enemy leaders or troop formations, or the opinion of an adversary population.[16]

In noncombat situations, precision engagement activities will focus on nonlethal actions that shape the perception and, therefore, the actions of participants. These actions will be capable of defusing volatile situations, overcoming misinformation campaigns, or directing a flow of refugees to relief stations, for example. Regardless of its application in combat or noncombat operations, the capability to engage precisely allows the commander to shape the situation or battle space in order to achieve the desired effects while minimizing risk to friendly forces and contributing to the most effective use of resources.[17]

2.2.6 Focused Logistics

Focused Logistics is the ability to provide the Joint force the right personnel, equipment, and supplies in the right place, at the right time, and in the right quantity, across the full range of military operations. This will be made possible through a real-time, web-based information system providing total asset visibility as part of a common relevant operational picture, effectively linking the operator and logistician across Services and support agencies. Through transformational innovations to organizations and processes, focused logistics will provide the Joint warfighter with support for all functions.

Focused logistics will provide military capability by ensuring delivery of the right equipment, supplies, and personnel in the right quantities, to the right place, at the right time to support operational objectives**. It will result from revolutionary improvements in information systems, innovation in organizational structures, reengineered processes, and advances in transportation technologies.** The transformation that will facilitate the

---

16 *Ibid.,* p. 22-23.

17 *Ibid.,* p. 23.

ultimate realization of the full potential of focused logistics is ongoing and significant progress has been made.[18]

Focused logistics will effectively link all logistics functions and units through advanced information systems that integrate real-time total asset visibility with a common operational picture. These systems will incorporate enhanced decision-support tools that will improve analysis, planning, and anticipation of warfighter requirements. They will also provide a more seamless connection to the commercial sector to take advantage of applicable advanced business practices and commercial economies. Combining these capabilities with innovative organizational structures and processes will result in dramatically improved end-to-end management of the entire logistics system and provide precise real-time control of the logistics pipeline to support the Joint force commander's priorities. The increased speed, capacity, and efficiency of advanced transportation systems will further improve deployment, distribution, and sustainment. Mutual support relationships and collaborative planning will enable optimum cooperation with multinational and interagency partners.[19]

The result for the Joint force of the future will be an improved link between operations and logistics resulting in precise time-definite delivery of assets to the warfighter. This substantially improved operational effectiveness and efficiency, combined with increasing warfighter confidence in these new capabilities, will concurrently reduce sustainment requirements and the vulnerability of logistics lines of communication, while appropriately sizing and potentially reducing the logistics footprint. The capability for focused logistics will effectively support the Joint force in combat and provide the primary operational element in the delivery of humanitarian or disaster relief, or other activities across the range of military operations.[20]

2.2.7 Full Dimensional Protection

Full Dimensional Protection is the ability of the Joint force to protect its personnel and other assets required to decisively execute assigned tasks. Full dimensional protection is achieved through the tailored selection and application of multilayered active and passive measures, within the domains of air, land, sea, space, and information across the range of military operations with an acceptable level of risk.

---

18 *Ibid.,* p. 24.

19 *Ibid.,* p. 24-25.

20 *Ibid.,* p. 25.

U.S. military forces must be capable of conducting decisive operations despite our adversaries' use of a wide range of weapons (including weapons of mass destruction), the conduct of information operations or terrorist attacks, or the presence of asymmetric threats during any phase of these operations. Our people and the other military and nonmilitary assets needed for the successful conduct of operations must be protected wherever they are located—from deployment, to theater combat, to redeployment. Full dimensional protection exists when the Joint force can decisively achieve its mission with an acceptable degree of risk in both the physical and information domains.[21]

The capability for full dimensional protection incorporates a complete array of both combat and noncombat actions in offensive and defensive operations, enabled by information superiority. It will be based upon active and passive defensive measures, including theater missile defenses and possibly limited missile defense of the United States; offensive countermeasures; security procedures; antiterrorism measures; enhanced intelligence collection and assessments; emergency preparedness; heightened security awareness; and proactive engagement strategies. Additionally, it will extend beyond the immediate theater of operations to protect our reach-back, logistics, and key capabilities in other locations.

An example of the significant contributions that Network Centric Warfare capabilities will make to mature full dimensional protection capabilities is provided by the U.S. Navy's Cooperative Engagement Capability (CEC), a bedrock capability for Theater Air and Missile Defense (TAMD). CEC provides a compelling existence proof of the power of Network Centric Warfare. By robustly networking air-, sea-, and land-based sensing capabilities, CEC enables commanders to significantly enhance shared situational awareness and dramatically increase mission effectiveness in the TAMD mission. Operational tests to date have demonstrated CEC operational effectiveness against the most challenging air defense threats. CEC is nearing Initial Operational Capability and is currently being pursued by the British Royal Navy. This breakthrough Network Centric Warfare capability is discussed in detail in Section 8.2.1.4 and Appendix E, paragraph 3.8.6

There is a critical need for protection of the information content and systems vital for operational success, including increased vigilance in counterintelligence and information security. The Joint force of 2020 will integrate protective capabilities from multinational and interagency partners when available and will respond to their requirements when possible. Commanders will thoroughly assess and manage risk as they apply protective measures to specific operations, ensuring an appropriate level of safety, compatible with other mission objectives, is provided for all assets.[22]

---

21 *Ibid.,* p. 26.

22 *Ibid.,* p. 27.

The Joint force commander will thereby be provided an integrated architecture for protection, which will effectively manage risk to the Joint force and other assets, and leverage the contributions of all echelons of our forces and those of our multinational and interagency partners. The result will be improved freedom of action for friendly forces and better protection at all echelons.[23]

2.2.8 The Global Information Grid (GIG)

Joint Vision 2020 highlights the importance of U.S., Allied, and coalition forces achieving dramatically improved capabilities for operating in the information domain. The concept for achieving this capability to operate in the information domain is the GIG. It is described in *Joint Vision 2020* as "…the globally interconnected, end to end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters, policy makers, and support personnel."[24]

The GIG will help enable Network Centric Warfare and Network Centric Operations by improving information sharing among all elements of a Joint force, and with Allied and coalition partners. This improved information sharing provides the basis for shared situational awareness. The success of the GIG will depend in large part on how well it helps achieve fully interoperable forces by connecting today's islands of interoperability to allow ***force-wide information sharing***.

The improved capabilities for information sharing enabled by the GIG will provide commanders with improved capabilities for ***Joint command and control***. Improved information sharing will dramatically improves commanders' capabilities for formulating and disseminating intent based on up-to-date knowledge of the situation that exists in the battlespace. In addition, the capabilities provided by the GIG will enable Joint force headquarters to be more dispersed and survivable and subordinate unit headquarters to be smaller, more agile, mobile, and dispersed. Furthermore, the GIG will provide the infostructure for advanced command and control applications that will enable flexible and adaptive coordination of forces and sensors.[25]

The GIG will also help facilitate information exchange with the diplomatic and law enforcement communities as well as with non-governmental and private organizations. DoD needs to be able to work with these organizations across the spectrum of conflict, during planning, execution, and post-execution phases in support of a variety of missions.

---

23 *Ibid.,* p. 27.

24 *Ibid.,* p. 9.

25 *Ibid*., p. 31-33.

In addition, improved GIG capabilities for Network Operations (NetOps) will provide enhanced, shared situational awareness of the network. This awareness is critical to preparing and reacting to adversary information operations and will enhance the effectiveness and execution of NCO/NCW.

The role of the GIG in enabling NCW, Information Superiority, and ultimately full spectrum dominance is portrayed in Figure 2-2. An in-depth discussion of the GIG is provided in Section 9 and Appendix D, where service and agency contributions to the GIG are discussed.

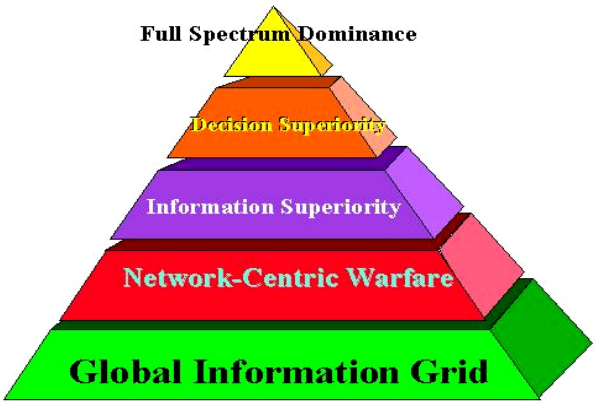


Figure 2-2. The GIG as an Enabler

The GIG will dramatically improve capabilities for force and enterprise-wide information sharing by leveraging rapidly advancing information technology to create a network-centric information environment. In addition to providing the building blocks of the GIG, information technology will increasingly permit Joint forces to integrate the traditional forms of information operations with sophisticated all-source intelligence, surveillance, and reconnaissance in a fully synchronized information campaign. Central to this information campaign will be improved capabilities for information operations.

2.2.9 Information Operations

Information operations—those actions taken to affect an adversary's information and information systems while defending one's own information and information systems. (JP1-02) Information operations also include actions taken in a noncombat or ambiguous situation to protect one's own information and information systems as well as those taken to influence target information and information systems.

Information operations are essential to achieving full spectrum dominance. The Joint force must be capable of conducting information operations, the purpose of which is to

facilitate and protect U.S. decision-making processes, and in a conflict, degrade those of an adversary. While activities and capabilities employed to conduct information operations are traditional functions of military forces, the pace of change in the information environment dictates that we expand this view and explore broader information operations strategies and concepts.[26]

We must recognize that "nontraditional" adversaries who engage in "nontraditional" conflict are of particular importance in the information domain. The United States itself and U.S. forces around the world are subject to information attacks on a continuous basis regardless of the level and degree of engagement in other domains of operation. The perpetrators of such attacks are not limited to the traditional concept of a uniformed military adversary. Additionally, the actions associated with information operations are wide-ranging—from physical destruction to psychological operations to computer network defense. The task of integrating information operations with other Joint force operations is complicated by the need to understand the many variables involved (summarized in the following box).[27]

The Variables of Information Operations

- Multidimensional definition and meaning of "information"—target, weapon, resource, or domain of operations
- Level of action and desired effect—tactical, operational, strategic, or combination
- Objective of operations—providing information, perception management, battlefield dominance, command and control warfare, systemic disruption, or systemic destruction
- Nature of situation—peace, crisis, or conflict

Our understanding of the interrelationships of these variables and their impact on military operations will determine the nature of information operations in 2020. The Joint force commander will conduct information operations whether facing an adversary during a conflict or engaged in humanitarian relief operations. Such operations will be synchronized with those of multinational and interagency partners as the situation dictates. New offensive capabilities such as computer network attack techniques are evolving. Activities such as information assurance, computer network defense, and counter deception will defend

---

26 *Ibid.,* p. 28-30.

27 *Ibid.,* p. 28-30.

decision-making processes by neutralizing an adversary's perception management and intelligence collection efforts, as well as direct attacks on our information systems. Because the ultimate target of information operations is the human decision maker, the Joint force commander will have difficulty accurately assessing the effects of those operations. This problem of "battle damage assessment" for information operations is difficult and must be explored through exercises and rigorous experimentation.[28]

The continuing evolution of information operations and the global information environment holds two significant implications. First, operations within the information domain will become as important as those conducted in the domains of sea, land, air, and space. Such operations will be inextricably linked to focused logistics, full dimensional protection, precision engagement, and dominant maneuver, as well as Joint command and control. At the same time, information operations may evolve into a separate mission area requiring the Services to maintain appropriately designed organizations and trained specialists. Improvements in doctrine, organization, and technology may lead to decisive outcomes resulting primarily from information operations. As information operations continue to evolve, they, like other military operations, will be conducted consistent with the norms of our society, our alliances with other democratic states, and full respect for the laws of armed conflict. Second, there is significant potential for asymmetric engagements in the information domain. The United States has enjoyed a distinct technological advantage in the information environment and will likely continue to do so. However, as potential adversaries reap the benefits of the information revolution, the comparative advantage for the US and its partners will become more difficult to maintain.[29]

NCW offers the potential for dramatic advantages, but carries the risk of a major loss of capability if our networks are penetrated or significantly disrupted.[30] As NCW capabilities increase in maturity and warfighters effectively exploit enhanced shared situational awareness enabled by information sharing, the ability to defend networks that enable this information sharing becomes increasingly important. Consequently, progress in implementing Network Centric Warfare is closely linked to improvements in information operations and information assurance capabilities.

---

28 *Ibid.,* p. 28-30.

29 *Ibid.,* p. 28-30.

30 Transformation Study Report, *Transforming Military Operational Capabilities*, Executive Summary, p. 20.

Section 3

Network Centric Warfare Concepts and Theory

3.1 Evolution of Warfare

Warfare takes on the characteristics of its Age. NCW continues this trend—it is the military response to both the challenges and the opportunities created by the Information Age. The term, NCW, provides a useful shorthand for describing a broad class of approaches to military operations that are enabled by the networking of the force. "Networking the Force" entails much more than providing connectivity among force components in the physical domain. It involves the development of doctrine and associated tactics, techniques, and procedures that enable a force to develop and leverage an information advantage to increase combat power.

Consequently, the terms "Network Centric Operations" and "NCW" are used to describe various types of military operations in the same way that the terms "e-business" and "e-commerce" are used to describe a broad class of business activities that are enabled by the Internet.[31] Scott McNealy, chairman and CEO of Sun Microsystems, recently stated, "The "e" in e-business is redundant."[32] His basic point is that e-business has to be about creating value and making a profit or it is not going to be relevant. In a similar sense, NCW is very much about warfare—about employing Information Age concepts to increase combat power in war and mission effectiveness in operations other than war.

The competitors who were first able to correctly identify the opportunity space provided by the Internet and e-business have been able to reap disproportionate rewards. The DoD seeks similar disproportionate advantages in future conflicts as we develop and implement a strategy for a network-centric transformation.

3.2 Definitions

The term Information Superiority,[33] despite its introduction several years ago, still lacks precision in its predominant popular usage. Similarly, the term NCW is, as yet, not

---

31 Amir Hartman, John Sifonis, John Kador, *Net Ready: Strategies for Success in the E-conomy*, McGraw Hill, 2000, p. xvii-xviii.

32 Scott McNealy, "It's like…Businesses Built on Metaphors Still Need Value," *Forbes ASAP*, October 2, 2000, p. 47.

33 JP 1-02 *Department of Defense Dictionary of Military and Associated Terms:* "The degree of dominance in the information domain which permits the conduct of operations without effective opposition."

universally accepted in the Defense community nor are NCW concepts universally understood. The term NCW was first introduced to a wide audience in 1998 in the article "Network Centric Warfare: Its Origins and Future," in *Proceedings of the Naval Institute*.[34] This article described a new way of thinking about military operations in the Information Age and highlighted the relationship between information advantage and competitive advantage. Given the short period of time that has transpired since then, there has been an enormous amount of progress in getting the fundamental tenets of Network Centric Operations understood.

There is an emerging understanding within the DoD and the international defense community of the power of Network Centric Operations. This understanding is the cumulative effect of the publication of tens of articles, the presentation of hundreds of briefings, and the distribution of tens of thousands of copies of the book *Network Centric Warfare: Developing and Leveraging Information Superiority*.[35] Additional factors that have contributed to this understanding include the reprinting and distribution of the book by leading IT and defense companies (Sun Microsystems, EMC, and Boeing), its translation into the Japanese and Korean languages, and the worldwide downloading of the book in PDF format via the Internet at http://www.dodccrp.org/publicat.htm.

There is a growing appreciation of the fact that it is far more important to get the basic ideas of Network Centric Operations across than it is to force people to adopt a particular label or term. Human nature and the sheer size and diversity of DoD and its supporting community make it inevitable that different enclaves have and will continue to coin their own terms to express the fundamental ideas that lie at the heart of NCW.

DoDI 5000.2, "Operation of the Defense A quisition System," Section 4.6.2.2 (October 23, 2000): Information Superiority is defined as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information Superiority is achieved in a non-combat situation or in one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives.
OASD(C3I) characterization of Information Superiority as the right information, to the right people, at the right times, in the right form, secure and assured, while denying adversaries the ability to do the same.

34 VADM Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124:1 (January 1998), p. 28-35.

35 David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Rev.), Washington, D.C., CCRP Press, 1999. www.dodccrp.org/publicat.htm

Therefore, this report goes beyond the labels to the ideas behind them, pulling together those DoD activities and initiatives that reflect the central hypothesis of NCW whether or not the term NCW is used.

This section provides definitions of Information Superiority and NCW. These definitions provide a context for the detailed discussions found in this report.

3.2.1 Fundamentals of Information Superiority

Information Superiority is a state of imbalance in one's favor in the information domain.[36] [37] Information Superiority has also been described in terms of what is needed to achieve it; e.g., the ability to get the right information to the right people, at the right times, in the right forms, while denying an adversary the ability to do the same.

Information Superiority derives from the ability to create a relative information advantage vis-a-vis an adversary. The concept of an information advantage is not new. Commanders have always sought—and sometimes gained—a decisive information advantage over their adversaries. Indeed surprise, one of the immutable principles of war, can be viewed as a type of information advantage that one force is able to establish over another.

An information advantage can:

- Be persistent or it can be transitory
- Exist in some areas of the battlespace but not others
- Be measured in the context of a task or set of tasks
- Be created by taking actions to reduce our information needs and /or increase the information needs of an adversary
- Be achieved through the synergistic conduct of information operations, information assurance (IA), and information gain and exploitation[38]

During World War II, a key contributor to the success of *Operation Overlord*, the Allied invasion of Europe in June of 1944, was the ability of Allied Forces to establish and maintain

---

36 *Joint Vision 2020.*

37 Office of the Assistant Secretary of Defense (Command, Control, Communications, & Intelligence), "Information Superiority Making the Joint Vision Happen," Pentagon, Washington, D.C., November 2000. www.c3i.osd.mil/infosuper/

38 *Ibid.*

an information advantage at the operational level of war. The ability of the Allied intelligence apparatus to break German codes and keep Allied codes secure gave Senior Allied Commanders confidence that the vast deception operation preceding *Operation Overlord* had succeeded.[39] Furthermore, at the time of the invasion, Allied Forces were aware of the geographic positions of all but two of the forty plus divisions of German Army Groups B and G.[40] [41] This significant information advantage, combined with aggressive deception operations, enabled Allied Forces to achieve surprise and a decisive force advantage on the beaches at Normandy and the surrounding countryside.[42] Nevertheless, at the tactical level, there were several instances during the invasion where Allied Forces did not have an information advantage, where landing craft attacked the wrong beaches, paratroops from the 82nd and 101st Airborne Divisions were dropped or landed in the wrong places, and attack aircraft bombed the wrong targets.[43]

Some have mistakenly thought of an information advantage simply in terms of the information and communications capabilities that one force has in comparison to an adversary. This idea leads to an over emphasis on information processes—collection, analysis, dissemination, and so forth. But this is not what information advantage is all about. It is important to assess a force's information capabilities relative to their needs. Concepts of operation; command approaches; organizational forms; doctrine; tactics, techniques, and procedures (TTPs); rules of engagement (ROEs); level of education and training; and the characteristics of weapons systems (taken together these all form a mission capability package) determine a force's information-related needs. The ability of a force to successfully carry out a military operation depends in large part on the degree to which its information needs are met.

Information needs can vary considerably. Throughout history military organizations, doctrine, command concepts, and TTP (subset of mission capability packages) were designed to minimize the amount of information and communications required because capabilities in these areas were very limited. The information-related capabilities we currently have allow

---

39 Anthony Cave Brown, *Body Guard of Lies*, Bantam Books, New York, NY, 1976, p. 1-10, 647-687.

40 *Ibid.*, p. 664.

41 John Keegan, *Six Armies in Normandy: From D-Day to the Liberation of Paris,* Penguin Books, 1982, p. 335-340.

42 Brown, p. 647-687.

43 Keegan, *Six Armies in Normandy: From D-Day to the Liberation of Paris*, Penguin Books, 1982, p. 69-114, 131-132.

us to develop TTP for C2 that can take advantage of our advanced information capabilities, but do not force our adversaries to mirror us in this regard. Therefore, there is no information "gap" or "information arms race" that we can force. Consequently we will face adversaries whose information-related needs will be asymmetrical to ours. What will matter is which force does a better job satisfying their respective information needs, not which side has better information-related capabilities. Thus the advantage is determined by comparing each side's information capabilities relative to their needs.

Simply minimizing one's information-related needs is not a winning strategy. Success will instead depend upon the ability to match concepts of operations (CONOPS) with information-related capabilities. Competitive advantages accrue to organizations that successfully master the art of creating and leveraging an information advantage.[44] Using Information Age technologies, organizations can put Information Age concepts to work moving information not people, conducting distributed operations, and substituting information for mass. The key is to find the right balance in which information-related capabilities are matched with a CONOPS, organization, approach to command and control, and the capabilities of the people and the weapons systems.

3.2.2 New Type of Information Advantage

Since the concept of a relative information advantage is clearly not new, two questions come to mind:

1. Can Information Technology help a force develop a new type of information advantage?
2. If so, how?

The answer to the first question is *yes* and the answer to the second question is *networking*. In this context, networking is being used in its broadest sense to include the networking of information-related processes and all forms of collaboration among a better-informed set of participants. Since some of the most significant benefits of networking are not immediately apparent, they are worth highlighting.

First and foremost, networking changes the topology of the information domain and as a consequence, changes the economics of information. This allows individuals and organizations to operate in a different part of the information domain. The information domain can be characterized in terms of the broad attributes of information richness and

---

44 Alberts, Garstka, and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority,* 2nd Ed. (Rev). Washington, D.C., CCRP Press, 1999, p. 28-51.

information reach.[45] Broadly speaking, information richness is a measure of the quality of information and information reach is a measure of the degree to which information can be shared (this is discussed in detail in the soon to be released C4ISR Cooperative Research Program (CCRP) book).[46]

In other words, networking provides access to a new part of the information domain—the network-centric region.[47] Constructs such as common operational pictures (COPs) and collaborative planning environments reside within this region of the information domain.

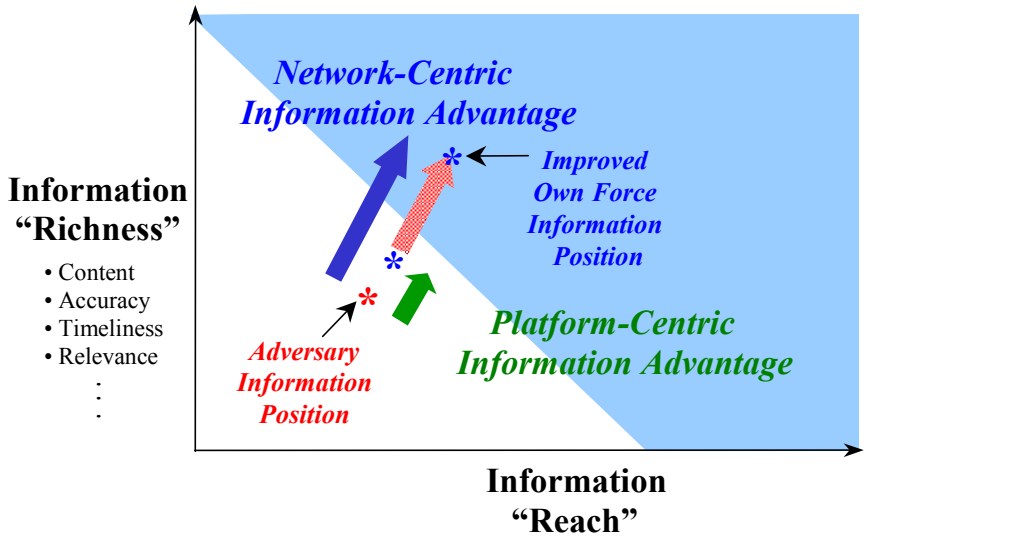
Operating in this network-centric region of the information domain allows warfighters to achieve information positions not previously feasible and, as a result, to develop a *new type of information advantage* previously unattainable. This new "network-centric information advantage" is portrayed in Figure 3-1 in comparison to a "platform-centric" information advantage.

---

45 Philip Evans and Thomas Wurster, *Blown to Bits: How the New Economics of Information Transforms Strategy*, Harvard Business School Press, 2000, p. 23-38.

46 David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori, *Understanding Information Age Warfare*, Washington, DC, CCRP Publication Series, August 2001. http://www.dodccrp.org/publicat.htm

47 John J. Garstka, "Network Centric Warfare: An Overview of Emerging Theory," *PHALANX,* December 2000, Vol. 33, No. 4, p. 1, 28-33.



Networking the Force Enables the Warfighter to Develop a New Type of Information Advantage

Figure 3-1 New Type of Information Advantage

The ability to develop and leverage this new type of information advantage is at the core of the increased combat power enabled by Network Centric Operations and inherent in the warfighting concepts of *Joint Vision 2020*.

3.2.3 Fundamentals of Network Centric Warfare

NCW is warfare. To understand what is different about NCW, as well as to understand the source of increased combat power associated with NCW, one has to simultaneously focus on the three domains of warfare and the interactions among them. These domains, the physical domain, the information domain, and the cognitive domain, are depicted in Figure 3-2.[48] [49]

---

48 *Ibid.*

49 Information Superiority Metrics Working Group White Paper.

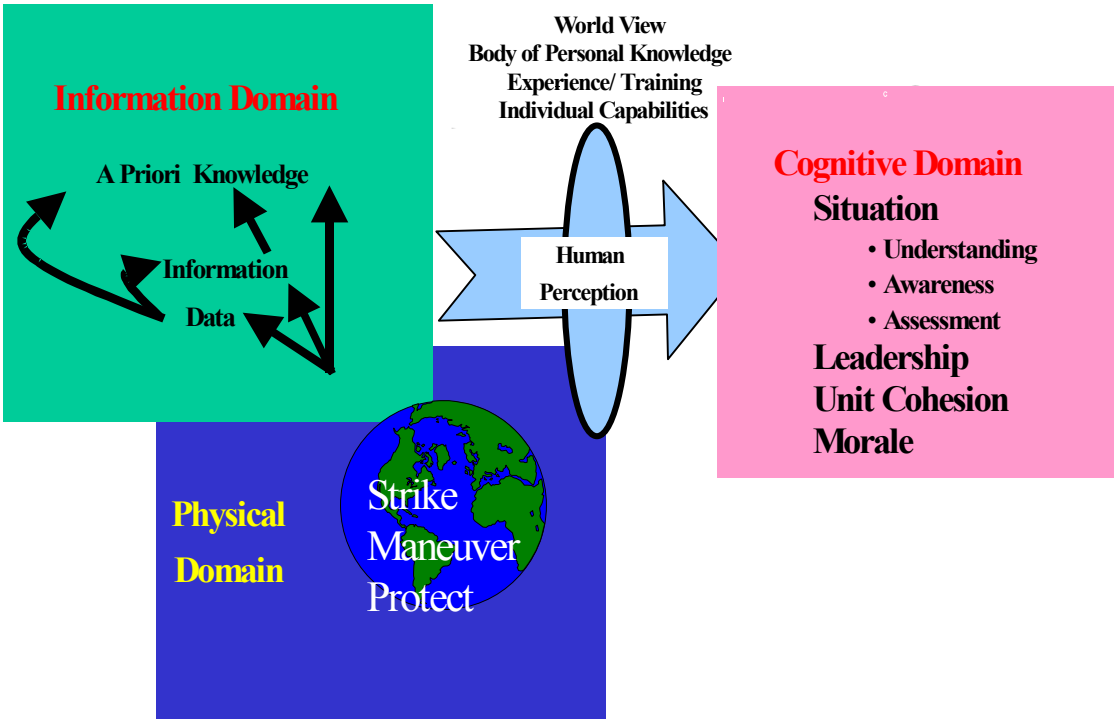


Figure 3-2. Domains of Warfare

3.2.4 The Physical Domain

The physical domain is the place where the situation the military seeks to influence exists. It is the domain where strike, protect, and maneuver take place across the environments of ground, sea, air, and space. It is the domain where physical platforms and the communications networks that connect them reside. Comparatively, the elements of this domain are the easiest to measure, and consequently, combat power has traditionally been measured primarily in this domain. In our analyses and models, the physical domain is characterized as reality, or ground truth. Important metrics for measuring combat power in this domain include lethality and survivability.

3.2.5 The Information Domain

The information domain is where information is created, manipulated, and shared. It is the domain that facilitates the communication of information among warfighters. It is the domain where the command and control of modern military forces is communicated, where commander's intent is conveyed. The information that exists in the information domain may or may not truly reflect ground truth. For example, a sensor observes the real world and

produces an output (data) which exists in the information domain. With the exception of direct sensory observation, all of our information about the world comes through and is affected by our interaction with the information domain. And it is through the information domain that we communicate with others.

Consequently, it is increasingly the information domain that must be protected and defended to enable a force to generate combat power in the face of offensive actions taken by an adversary. And, in the all-important battle for Information Superiority, the information domain is ground zero.

3.2.6 The Cognitive Domain

The cognitive domain is in the minds of the participants. This is the place where perceptions, awareness, understanding, beliefs, and values reside and where, as a result of sensemaking, decisions are made. This is the domain where many battles and wars are actually won and lost. This is the domain of intangibles: leadership, morale, unit cohesion, level of training and experience, situational awareness, and public opinion. This is the domain where an understanding of a commander's intent, doctrine, tactics, techniques, and procedures reside. Much has been written about this domain, and key attributes of this domain have remained relatively constant since Sun Tzu wrote *The Art of War*. The attributes of this domain are extremely difficult to measure, and each sub-domain (each individual mind) is unique.

Note that *all* of the contents of the cognitive domain pass through a filter or lens we have labeled human perception. This filter consists of the individual's worldview, the body of personal knowledge the person brings to the situation, their experience, training, values, and individual capabilities (intelligence, personal style, perceptual capabilities, etc.). Since these human perceptual lenses are unique to each individual, we know that individual cognition (understandings, etc.) is also unique. There is one reality, or physical domain. This is converted into selected data, information, and knowledge by the systems in the information domain. By training and shared experience we try to make the cognitive activities of military decision makers similar, but they nevertheless remain unique to each individual, with differences being more significant among individuals from different Services, generations, and countries than they are among individuals from the same unit or Service.

3.2.7 NCW Defined

NCW involves "networking" in all three of these domains. In its fully mature form, NCW possesses the following characteristics:

Physical Domain:

- All elements of the force are robustly networked achieving secure and seamless connectivity.

Information Domain:

- The force has the capability to collect, share, access, and protect information.
- The force has the capability to collaborate in the information domain, which enables a force to improve its information position through processes of correlation, fusion, and analysis.
- A force can achieve information advantage over an adversary in the Information Domain.

Cognitive Domain:

- The force has the capability to develop and share high quality situational awareness.
- The force has the capability to develop a shared knowledge of commanders' intent.
- The force has the capability to self-synchronize its operations.

In addition, the force must be able to conduct information operations across these domains to achieve synchronized effects in each of these domains.

The central tenet of NCW is that a force with these attributes and capabilities will be able to generate increased combat power by:

- Better synchronizing effects in the battlespace
- Achieving greater speed of command
- Increasing lethality, survivability, and responsiveness

This description of NCW characteristics relates to its fully mature form. In fact this maturity may take years if not decades to be achieved. It is important therefore to be able to understand NCW at various levels of maturity. The level of maturity achieved at any given point in time can be expressed in terms of each of the domains. For example, in the physical domain, one measure of maturity is the extent to which the force is networked. This notion of NCW maturity will form the basis for measuring progress toward NCW implementation. A detailed treatment is provided in Section 8.

To date, thinking about and experimenting with NCW concepts have tended to focus on the tactical and operational levels of warfare, but they are applicable to not only all levels of warfare but to all types of military activity from the tactical to the strategic. When network-centric concepts are applied to operations other than war, we use the term Network Centric Operations. At the operational level, Network Centric Operations provide commanders with the capability to generate precise warfighting effects at an unprecedented operational tempo, creating conditions for the rapid lockout of adversary courses of action.

3.2.8 NCW Hypotheses

The fundamental characteristics of NCW can be described with a set of integrated linkage hypotheses that can be organized into three classes:

1. Hypotheses of the first class deal with the relationships among *degree of networking*, *information sharing*, *improved awareness, improved information quality*, and *shared situational awareness.*
2. Hypotheses in the second class include those that involve the relationship between *shared situational awareness* and *synchronization,* for example, the effect of different degrees of *shared situational awareness and/*or *collaboration* or *synchronization.*
3. The third class of hypotheses involves the link between *synchronization* and *mission effectiveness.*

Figure 3-3 is a graphical representation of an NCW value chain,[50] which depicts these linkage hypotheses. This figure places the NCW value chain in the context of the domains of warfare and relates Information Superiority, Decision Superiority, and Full Spectrum Dominance.

---

50 Office of the Assistant Secretary of Defense, (Command, Control, Communications, and Intelligence), *Information Superiority: Making the Joint Vision Happen,* November 2000, p. 11-12.

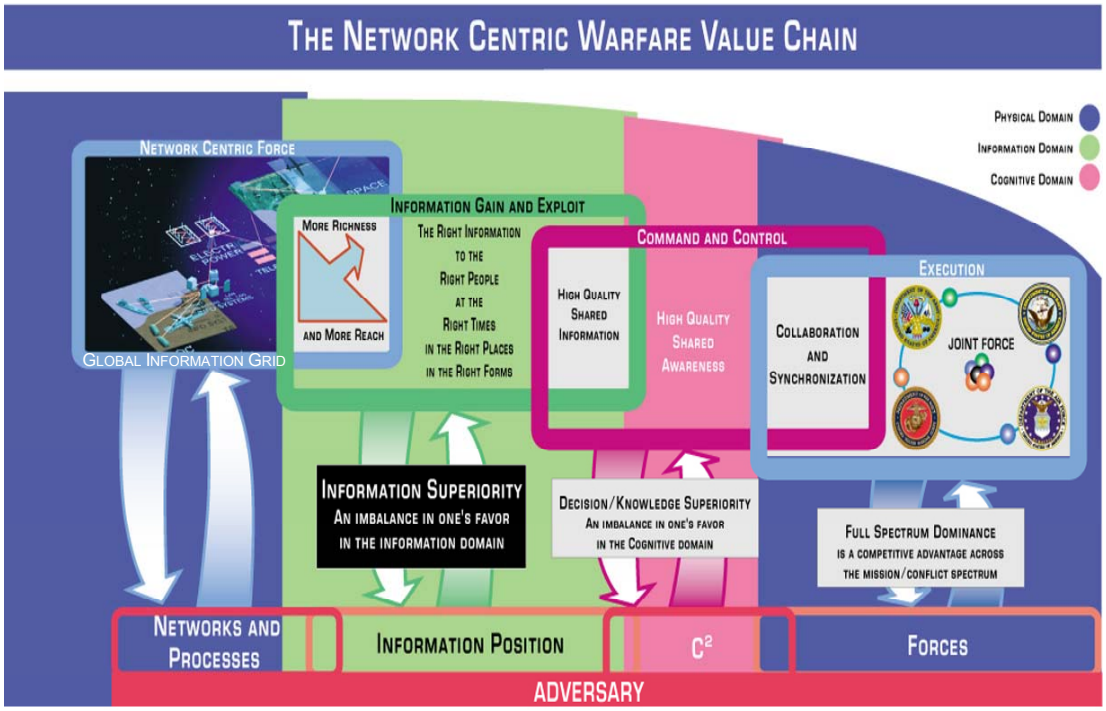


Figure 3-3. NCW Value Chain with Linkage Hypotheses

While at a high level of abstraction, these NCW-related hypotheses may seem obvious, (e.g., that improved sharing of information will result in more shared situational awareness) there are a host of specifics that need to be better understood before NCW concepts can be translated into real operational capabilities on a large scale. For example, it is important to understand:

- The specific conditions under which the shared information—shared situational awareness hypotheses are true
- The shape of the transfer function between information sharing and shared situational awareness
- The variables that influence this relationship (e.g., nature of the information exchange, quality of the information, degree of shared knowledge among the participants)
- Barriers, such as information overload, that prevent shared information from becoming shared situational awareness
- Approaches for overcoming these barriers

The central NCW hypotheses and questions such as those listed above provide a useful organizing logic for both Service and Joint Warfighting experiments.

3.3 Network-Centric Concepts—The Network as a Source of Value Creation

All network-centric concepts share the same simple, yet powerful idea—the idea that information sharing is a source of potential value. In the commercial sector, this value can be measured in terms of four principal competitive attributes: functionality, reliability, convenience, and cost.[51] In combat operations, this value can be measured in terms of key attributes of combat power, such as survivability, lethality, speed, timeliness, and responsiveness.

Over the past few years of Internet growth, an important insight that has emerged from the commercial sector is that the particular combination of factors that contributed to the success of e-business concepts were not *a priori* intuitive. It is now clear in retrospect that billions of dollars were invested in e-business concepts that were fundamentally flawed.[52] In some cases, intuition was correct, and in other cases, it wasn't.

For example, in the case of eBay, one of the most successful e-businesses to date, the initial intuition of its founder and chairman, Pierre Omidyar, was borne out in eBay's subsequent success.[53] According to Pierre Omidyar, when he initially started the eBay Web site on Labor Day in 1995, he had an intuitive appreciation of the value of the information richness and information reach that eBay would provide, but he was unprepared for the overwhelming response by the market.

Similarly, in the fall of 1998 during Fleet Battle Experiment (FBE) Delta, when the U.S. Navy networked elements of the Joint force in ways that had not been previously attempted, they were experimenting with increased information richness and increased information reach. Just as the founder of eBay was following his intuition, VADM Doran, then Commander of the U.S. Navy's 7th Fleet, and his staff were following their intuition when they collaborated with Navy Warfare Development Command and experimented with

---

51 Christensen, et al., *After the Gold Rush: Patterns of Success and Failure on the Internet,* p. 22-24. www.innosight.com.

52 *Loc. cit.*

53 David Bunnel and Richard A. Luecke*, The eBay Phenomenon: Business Secrets behind the World's Hottest Internet Company*, Wiley, Johnson, & Sons, Inc., 2000.

network-centric concepts in the counter special operations forces (CSOF) mission and validated the power of NCW.[54]

3.3.1 NCW Concepts

All NCW concepts share a common attribute: they are enabled by the networking of various elements of the force. The network alone is not sufficient to generate increased combat power, but it is the primary entry fee for enabling NCW concepts.

NCW concepts can be characterized by employing the multi-domain definition introduced previously. However, there is not yet a generally agreed taxonomy for NCW concepts. To a large extent, what has occurred to date is that initiatives, concepts, and programs of record selectively network elements of the force and or deploy advanced software applications. These activities are often given a *name* that is only marginally useful in describing with any degree of specificity or precision the actual functionality of the concept/initiative/program. This is addressed in the analysis of Service and Agency initiatives, Section 11. Complicating this is the tendency for some concepts to be described strictly in the context of a single domain, when in reality, all three domains must often be employed to uniquely characterize a concept.

For example, some concepts have been described in terms of the types of entities in the physical domain that are networked and the primary functionality improved. For example, the terms "Sensor Network" and "Sensor Grid" have been used to describe "concepts" that selectively network various types of sensors that exist in the **physical domain** with the objective of enabling improved sensing functionality (sensor tasking, sensor fusion), which can be measured in terms of an improved information position in the **information domain.**[55] (This improvement can be measured with the attributes of accuracy and timeliness.)

Other concepts, such as the Single Integrated Air Picture (SIAP) and the COP, that correspond to a desired information position in the **information domain,** are often described in ways that would not lead one to understand they are enabled by the networking of various elements of the force in the **physical domain**. The relationship between a position in the information domain and networking in the physical domain is portrayed in Figure 3-4.

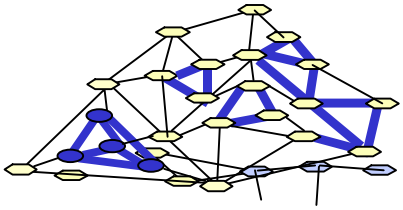
Other terms, such as "engagement networks" and "engagement grids" are used to describe concepts that primarily network shooters (and their embedded sensors) with C2 capabilities/nodes (decision makers with C2 responsibilities) with the objective of improving

---

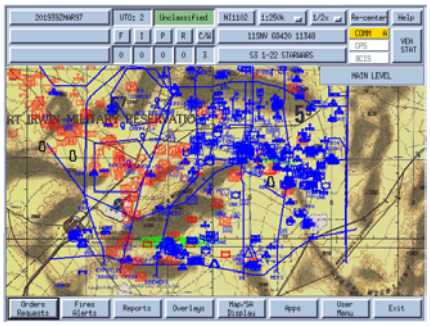
54 Personal conversation with VADM Walter Doran, Washington, D.C., 5 Feb 2001.

55 An in-depth discussion of sensor networks is provided in Alberts, Garstka, and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority,* p. 140-145.

engagement functionality (e.g., weapon target assignment, collaborative planning) which can also be measured.[56] Examples include the "Ring of Fire" and the "Cooperative Engagement Capability."



Network - Physical Domain



Common Operational Picture - Information Domain

Figure 3-4. Relationship Between Physical Domain and Information Domain

In some cases, these NCW concepts are enabled by the same network but employ different applications with distinct functional behavior and performance. For example, in the Cooperative Engagement Capability (CEC), sensing and engagement functionalities are both improved.

Selected examples of each of these NCW concepts are provided below. A description of each may be found in Appendix E.

Networked Sensors/Sensor Networks/Sensor Grids:

- **CEC Sensing Component** is described in Appendix E, paragraph 3.8.6
- **Network Centric Collaborative Targeting** is described in Appendix E, paragraph 5.3.1.5
- **Web-Centric ASW Network (WeCAN)** is described in Appendix E, paragraph 3.9.2
- **Expeditionary Sensor Grid** is described in Appendix A, paragraph 2, and Appendix E, paragraph 3.4.8

---

56 *Ibid.*, p. 157-186.

- **Reconnaissance, Surveillance, Targeting, Acquisition (RSTA) Cloud**: Army concepts for RSTA are addressed in Appendix E, paragraph 2.2; U.S. Marine Corps programs are described in Appendix E, paragraph 4.2 and 4.5.2
- **Joint Composite Tracking Network** is described in Appendix B, paragraph 5.4

Networked Shooters/Engagement Networks/Engagement Grids:

- **Ring of Fire** is described in connection with Navy experimentation in Appendix C, paragraph 2.3 and Appendix E paragraph 3.2.2.2.
- **Engagement Grid** is described in connection with Army Future Combat Systems in Appendix E, paragraph 2.5
- **CEC Engagement Component** is described in Appendix E, paragraph 3.8.6

Networks:

- **Link-16** is described in Appendix E, paragraph 3.4.18; and is referenced as a key capability in connection with Single Integrated Air Picture by BMDO (Appendix B, paragraph 5.4), Air Force (Appendix A, paragraph 4.2.2), in several locations in Navy's Appendix E, paragraph 3.2.12, and in connection with Defense Technology Objectives (Appendix F, paragraph 1)
- **SIPRNet**
- **NIPRNet**
- **Tactical Internet** is described in Appendix E, paragraph 2.2
- **Coalition Wide Area Network (CWAN)**
- **Joint Worldwide Intelligence Communications System (JWICS)** is described in Appendix D, paragraph 2.3.2

Network-Enabled Information Constructs:

- **Common Operational Picture (COP)**
- **Single Integrated Air Picture (SIAP)**
- **Common Relevant Operational Picture (CROP)**

To a greater or lesser degree, the vast majority of concepts currently being explored in Service and Joint Experiments and Demonstrations involve the networking of "things" in various ways, shapes, and forms, and employ software applications that reside on the network and enable significantly enhanced information sharing and collaboration. A vast and diverse variety of terms are employed to describe these initiatives, which serves to obscure the fact that they share a common theme—they all involve sharing of information

among distributed entities and/or "networking" in the form of collaboration or self-synchronization (which in turn is enabled by improved shared situational awareness).

3.4 Information Superiority, NCW, and the Principles of War

Several principles of war have emerged over thousands of years of conflict and are now taught both to U.S. officers and, with some differences, to military personnel around the world. They are listed in Table 3-1.

Table 3-1. Principles of War

Objective	Offensive	Mass
Economy of Force	Maneuver	Unity of Command
Security	Surprise	Simplicity

The DoD is undergoing twin revolutions driven by the concepts and technologies of the Information Age. The Revolution in Business Affairs (RBA), modeled on the successes experienced in the Commercial Sector, is transforming the business side of DoD while the Revolution in Military Affairs (RMA), based upon adapting lessons from other domains to the domain of warfare, is transforming military operations. These are not independent revolutions. Transformations in the business side not only free up resources that can be more highly leveraged by combatant commands, but also provide improvements in combat support that enable more effective concepts of operation, organization, doctrine, and the like. They enable the RMA and will transform military operations, increasing the tempo of operations, the speed of command, and, as a result, achieve greater lethality with increased survivability. The net result of RBA and RMA synergy will be an opportunity for quicker and more decisive victories, using less "tail" (support) and bringing to bear more "tooth" (warfighting capability).

The ongoing, information-driven RMA promises to improve our ability to realize each of these enduring principles in practice.

Objective. The principle of the objective refers to focusing the entire effort in ways that ensure the assigned military mission (the objective) is achieved. Information Superiority, which includes creating and maintaining a continuous, high quality information flow throughout the force and creating shared situational awareness in the form of a COP for all commands, helps to ensure a clear and common understanding of the objective to be supported, the threats to mission accomplishment, and the commander's chosen course of action for achieving the objective. Given the rapid pace of change in this battlespace and the decision cycle speed needed to dominate it, the ability to share information, maintain a

current COP, and enable commanders to work in a collaborative environment whenever necessary are central to this principle. As our competitors get access to even more powerful Commercial Off-the-Shelf (COTS) capabilities, only our ability to leverage these capabilities to achieve dominant speed in decision making (speed of command) will enable us to maintain the advantage.

Offensive. Seizing and maintaining the offensive, which enables the force to dictate the terms of combat, is directly dependent on the ability to work inside (or faster than) an opponent's decision cycle (the response time, sometimes referred to as the Observe, Orient, Decide, Act cycle (OODA) loop.) This is supported by Information Superiority both through effective offensive information operations (which disrupt and slow an adversary's decision making and force decisions under greater uncertainty) and by improving the integration and interoperability of C4ISR systems and processes across the board, from better monitoring of the battlespace to faster fusion, improved decision quality and speed, to faster planning and implementation times.

Mass. The principle of mass refers to concentrating military capabilities at the decisive time and place. This remains true even in non-linear battles, as when the Viet Minh brought major artillery and manpower to bear at Dien Bien Phu against the French. While this principle has referred to massing forces in the past, the RMA allows the United States to focus on massing effects through the use of enriched sensor capabilities and stand-off precision weapons. The ongoing shift from platform-centric to network-centric platforms and forces, enabled by Information Superiority, greatly improves our capacity to take advantage of all the information available, reduce the risk to U.S. forces, and still inflict maximum damage on an adversary.

Economy of Force. Economy of Force refers to the need to use as little capacity as possible on aspects of the battle that are not central to the objective. Commanders think of accepting risk in some parts of the battlespace in order to dominate in other parts considered more crucial. Given Information Superiority with the implied improvement in knowing adversary locations, status, and capabilities, as well as greater flexibility in using assets for multiple purposes, this principle would be enhanced. With improved logistics; e.g., less material forward and greater use of timely delivery, economy of force in transport and maintenance would also benefit from Information Superiority.

Maneuver. The principle of maneuver deals with placing the enemy at a disadvantage by wisely using the terrain and other aspects of the situation that constrain his courses of action and providing our forces with an advantage through flexibility and adaptation to the situation. Information Superiority provides high quality, current information about adversary force situation, terrain, weather (and their interaction such as mud and fog), and adversary capabilities as well as the knowledge necessary to exploit the mobility, stealth, and flexibility of our own forces.

Unity of Command. Unity of Command has long been understood as a prerequisite for effective military action. Even in coalition operations for "soft missions," such as peace operations, the lessons learned activities often point to problems arising from forces operating under different National commands and call for "unity of effort." Whatever the practical limits on unity for a particular operation, the ability to create and maintain a shared picture of the commander's intent, and the timely and assured dissemination of plans, orders, reports, and other key information—all core elements of Information Superiority—are vital.

Security. The principle of security is also fundamental to military success. In today's military this translates into Information Assurance providing an uninterrupted flow of authentic communications and information. If the information processing or communications channels are compromised, or feared to be compromised, military success is imperiled.

Surprise. Surprise is the ability to strike the enemy at a time, place, or manner for which he is not prepared. It confers massive military advantage. Both intelligence preparation of the battlespace and effective operational security (OPSEC) are essential to achieving surprise. Offensive information operations, both to know the enemy's state of readiness and to deceive him about our plans, can add to the likelihood of successful surprise. At the same time, the ability to know the battlespace in detail is crucial to finding opportunities for surprise actions. The increased understanding of the situation that is achieved by sharing information and collaboration and the ability to respond more rapidly that comes from new command concepts has the potential to make every engagement an ambush turning what was only an exceptional event into a standard operating procedure.

Simplicity. The principle of simplicity refers to the need to keep plans, guidance, and orders clear and uncomplicated. It has been established over history that the debilitating effects of human fatigue, excitement, and fear compounded by errors of miscommunication and ambiguity, have proven to be one of the greatest problems in war—the famous "fog and friction" of war. By reducing uncertainty (and thus simplifying the decisions to be made and the situational variations that need to be considered) and by streamlining the processes of situation assessment, planning, and execution, Information Superiority enables commanders to work at a simpler, more coherent level.

Thus, as explained above, NCW enhances our ability to achieve each of the enduring principles of war.

Section 4

Overview of Service Visions and Concepts for NCW

An in-depth description of the Service's and key Agencies' Visions for NCW, as well as their emerging concepts, their contributions to the Global Information Grid, and key NCW initiatives is provided in the Appendices to this Report. Each of these discussions also relates *Joint Vision 2020* to NCW from the perspective of the individual Service or Agency.

As noted in Section 3.2, the term NCW is not universally accepted in the Defense community, nor are NCW concepts universally understood. The Appendices further illustrate this point. The Services and Agencies use many different terms in describing initiatives and programs. However, the work they describe is consistent with the tenets of NCW defined in the Executive Summary:

- A robustly networked force improves information sharing.
- Information sharing enhances the quality of information and shared situational awareness.
- Shared situational awareness enables collaboration and self-synchronization; and enhances sustainability and speed of command.
- These, in turn, dramatically increase mission effectiveness.

An overview of Service NCW Visions is provided below, to provide context for the discussion in the body of the report and to provide an introduction for the rich and detailed NCW discussion in that appears in the Appendices to this report.

4.1 Army NCW Vision

4.1.1 *Joint Vision 2010/2020* and the Army Vision

Joint Vision 2010 and *Joint Vision 2020* guide the continuing transformation of America's Armed Forces toward a goal to create a force that is dominant across the full spectrum of military operations. Similarly, *The Army Vision* provides the conceptual template for transforming the Army into a force that is strategically responsive and dominant across the full spectrum of operations and an integral member of the Joint warfighting team. Both *Joint Vision 2020* and *The Army Vision* are strongly dependent on the potential of linking together networking, geographically dispersed combat elements. In doing so, the Army expects to achieve significant improvements to shared battlespace understanding and increased combat effectiveness through synchronized actions. This Joint concept of operations is **Network Centric Warfare (NCW).**

The NCW construct provides a valuable perspective for achieving success in a target-oriented warfare situation, where timely, relevant, accurate, and precise information is required to automatically engage targets expeditiously with the most effective weapons and forces available. NCW emphasizes using networked intelligence, surveillance, and reconnaissance (ISR) capabilities, and predetermined decision criteria, to support automated responses from the "network" to threats against individual platforms. It emphasizes the importance of situational awareness for both targeting and decision making. It promotes the value of information sharing, collaboration, synchronization, and improved interoperability within the information domain. It suggests that information superiority and victory on the battlefield will be dependent on technological solutions that will help us acquire, process, exploit, disseminate, and protect information. Information superiority, knowledge, and decision superiority are absolutely critical for the Army's transformation to the Objective Force and are key to maneuver- and execution-centric operations.

Some examples are:

- Collaborative and simultaneous planning and execution among widely dispersed commanders and staff saves planning and travel time, allowing commanders to focus on information collection, decision making, and execution.
- Enroute mission planning and rehearsal among dispersed force elements prior to deployment, enroute, and in theater.
- Command and Control on the Move allows commanders the freedom to move to critical points on the battlefield.
- Split-based operations reduces the number of staff and support personnel required to be deployed to theater thus reducing the associated Tactical Operations Center footprint.
- Virtual support services support deployed forces from centers of knowledge in the continental U.S.
- Distance learning and Knowledge Centers provide warfighters access to education, training and knowledge.
- Integrated and layered Intelligence, Surveillance and Reconnaissance (ISR) allows commanders, staffs and analysts worldwide to collaborate in the development of real time combat information and near real time, predictive intelligence products for the warfighter.

The theory behind NCW is that by linking sensor networks, command and control (C2) networks, and shooter networks, we can achieve efficiencies in all military operations from the synergy that would be derived by simultaneously sharing information in a common

operating environment. In addition, such linkages allow for the discovery of new concepts of operations both among Army forces and Joint forces in theater.

While NCW is the operational concept, the **Global Information Grid (GIG)**, a major Defense transformation initiative, is directed toward providing critical infrastructure networking to the forces.

The goals of the GIG are to provide communications, security, processing, and information dissemination management services to facilitate NCW; end-to-end connectivity; and intra-service, Joint and Allied interoperability. The sensor grid, or network, must anticipate and overcome future camouflage, concealment, and deception challenges to assure that commanders see a true picture of the battlefield. Processors and powerful automated decision aids must enable analysts to show not only what the enemy is currently doing, but predict what he *will most likely do* over time.

4.1.2 What is Needed to Realize NCW and GIG

While NCW is an approach to the conduct of warfare that derives its power from the effective linking together of battlespace entities, it is considerably more than that. It also derives its power from human and organizational behavior changes and innovative changes to the conduct of warfare that can be enabled by that networking.

To realize the potential of NCW we must:

- Turn ISR data into actionable combat information, knowledge and intelligence
- Disseminate knowledge over robust communications networks to decision makers and weapon platforms at all echelons in time to act inside an adversary's decision cycle
- Leverage technologies that allow for greater access to databases and analytical efforts located outside the theater of operations, thus enabling split-based operations
- Experiment with and exercise the elements of NCW and the GIG to determine critical doctrinal and organizational alignments

4.1.3 Army Objective Force Concepts

The degree to which the Objective Force fully embodies the characteristics outlined in the Army Vision—responsive, deployable, agile, versatile, lethal, survivable, sustainable—will determine to a significant degree the overall capability of the force to carry out its core operational tasks within the Joint campaign. From a C4ISR perspective, significantly improved capabilities will be available and organic to combat battalions and brigades. The current hierarchical nature of C4ISR will transition to a network-centric knowledge-based approach where combat units employ Information Superiority and layered ISR capabilities to

shape the battlespace and strike at decisive points and centers of gravity through distributed operations.

Objective Force agility and versatility will enable transition between benign and hostile environments, within and between operations, including transition from single area, single objective operations to higher intensive offensive and defensive operations, and vice versa. Objective Force units will deliver lethal overmatching combat power with integrated combined arms capability at the lowest levels of organizational design. Central to this capability is the ability to employ decisive fires, maneuver, and assault to assure complete destruction of the enemy as described earlier.

At the tactical level, the close combat zone will expand in size and shift focus toward organic capabilities to fight and win lethal close combat and beyond line of sight engagements. Lethality is the sum of actions taken to close with and destroy the enemy. Commanders will normally exhibit direct leadership through personal interaction and example with the soldiers executing the operation. Here, more than anywhere else, the commander qualities of physical courage, coolness, endurance, and the ability to make very quick, correct decisions are of paramount importance. Lethal units will dominate battle through employment of overmatching sensors and firepower capabilities at ranges that exceed those of the enemy. Freedom of maneuver for lethal units will be provided through mobile and survivable systems and units. Command concepts will emphasize the integration of superior commander development, advances in C4ISR, and a decentralized control structure. The commander's decision making will repeatedly cycle through the act of determining what conditions exist, what actions must be taken to master those conditions, and how to execute those actions. Future battles will be characterized by more numerous, discrete, and often nearly simultaneous tactical engagement executed by multiple combat battalions. Underlining this will be the ability of the Future Combat Systems to generate complementary and reinforcing firepower faster than the enemy. As the battalion closes on the enemy, its elements will attach by line of sight (LoS), non-LoS, and BLoS with precise destructive fires, obscuring effects, counter mobility fires and electronic warfare effects that shock, isolate, disrupt C2, fix enemy maneuver forces, suppress ISR and fires, neutralize enemy support, and blind the enemy. Each Future Combat System will be multifunctional, combining two or more battlefield functions such as direct and indirect fires, point air defense, battle command, mobility support, and ISR.

The ability of C4ISR systems to enable Information Superiority will be the key to the support of survivability. Offensive Information Operations will directly support the Objective Force capability to maneuver out of contact, target enemy C2, and hinder the enemy's ability to gain situational understanding. Likewise counter-reconnaissance and defensive Information Operations will integrate capabilities to protect and defend friendly information and information systems. Simply put, the paradigm of See First, Understand

First, Act First, and Finish Decisively acknowledges the increased lethality of the future battlefield and identifies the tasks necessary for soldiers to survive and win.

4.2 Navy NCW Vision

In response to the Enactment of Provisions of H.R. 5408, The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, the United States Navy would like to take the opportunity to thank the House of Representatives for this opportunity to provide the Congressional Defense Committees, via the Secretary of Defense, information relating to efforts being pursued in the area of NCW. The Navy's Network Centric Operations (NCO), as defined in our report, are essential to projecting U.S. power and influence and continuing the Navy contribution to National Security.

The United States Armed Forces' information and knowledge superiority are the first line benefactors during the implementation of the Navy's NCW. The Navy is uniquely positioned in current processes, capabilities, plans, and people to implement NCW philosophies throughout the Joint and Coalition Forces.

NCW is a concept that has not been totally implemented. Implementing NCW will require a holistic approach. It will require refinement of business practice, partnerships with Industry, plans, and programs over the next several months. The Navy considers this report to be an important beginning in the continuing development of Capstone Requirements and will continue its dedicated leadership to establishing NCW doctrine. We welcome the opportunity to provide you further information regarding the details as we progress in this endeavor.

The Navy has developed *"Network Centric Operations (NCO), A Capstone Concept for Naval Operations in the Information Age,"* which articulates the Navy's path to NCW**.** The Concept applies the defining tenets of Joint and naval warfare to network-centric warfighting and provides a vision of the new capabilities to be achieved. The improvements in the ability to quickly attain and sustain global access as a result of this transformation are critical to enabling the Navy's forces to decisively influence future events at sea and ashore—*Anytime, Anywhere*. Although the *Network Centric Operations Capstone Concept* is under review by the Chief of Naval Operations (CNO) and has not yet been approved, many of the principles contained within the NCO concept are contained in Naval doctrine, which is fundamentally network centric. Naval Doctrine serves as a foundation for the flexible tactics that will be the hallmark of a network-centric fighting force.

In developing NCW systems, a different approach to applying the principles must be taken. NCW requires that technology, tactics, and systems be developed together. The CNO Staff, the Fleet with the Navy Warfare Development Command, Naval Air Systems Command, Naval Sea Systems Command, and the Space and Naval Warfare Systems Command will work as a collaborative team in developing tactics, techniques, and procedures; technologies, experimentation, simulation, systems, test, evaluation, training,

and certification of the systems implementation of NCO as architectural systems and capability components that serve the warfighter and provide for integrated mission capabilities.

NCW serves the principals of forward presence, deterrence, reassurance, crisis response, and the projection of combat Power. The NCO concept will evolve from a concept in Naval Doctrine, to endure as an integral part of Joint Doctrine. The Navy will lead, in the development of this Joint Doctrine, the blueprinting and engineering, integration and certification of systems and capabilities that provide the CINC with a flexible combat force to influence events from ashore, sea, air, and space.

Joint Vision 2020, naval policy, and vision statements point to three inescapable military trends that will shape future operational capabilities:

- A shift in emphasis toward Joint, effects-based combat
- An increasing reliance on knowledge superiority
- Future adversaries will use technology to make rapid improvements in military capabilities designed to provide asymmetrical counters to U.S. military strengths

Each of these trends underscores the increasing importance of information as a source of power. Information protection, knowledge management, and networked sensor employment and exploitation are vitally important to future warfighters. The Navy is already engaged in a forward presence that is a built-in information advantage. The Navy-Marine Corps team, is able to fight for and win, based on the projection of combat Power using the information and knowledge advantage provided in NCW in any crisis or conflict.

The Navy vision for NCW is more fully stated in Appendix A.2 of the report.

4.3 U.S. Marine Corps NCW Vision

Throughout our Nation's history, Marines have responded to national and international brush fires, crises, and when necessary, war. The Marine Corps operates as MAGTFs, highly integrated and networked combined-arms forces that include air, ground, and combat service support (CSS) units under a single commander. In many respects the Marine Corps is by its very design a network-centric warfighting force. Our challenge is to take advantage of the rapid technological change that is continuously occurring, using industry standards to analyze technology against force requirements.

While the Marine Corps has not historically used the term Network Centric Warfare, its principles embodied by the term have been an integral part of Marine Corps operations for years.

MAGTFs are organized, trained, and equipped from the operating forces assigned to Marine Corps Forces, Pacific; Marine Corps Forces, Atlantic; and Marine Corps Forces,

Reserve. The Commanders of Marine Corps Forces Pacific and Atlantic provide geographic combatant commanders with scalable MAGTFs that possess the unique ability to project mobile, reinforceable, sustainable combat power across the spectrum of conflict. Marine Corps Forces, Reserve provides ready and responsive Marines and Marine Forces who are integrated into MAGTFs for mission accomplishment.

Marine Expeditionary Forces (MEFs) are task-organized to fight and win our Nation's battles in conflicts up to and including a major theater war. Marine Expeditionary Brigades (MEBs) are task-organized to respond to a full range of crises, from forcible entry to humanitarian assistance. They are our premier response force for smaller-scale contingencies that are so prevalent in today's security environment. Marine Expeditionary Units (Special Operations Capable) (MEU SOCs) are task-organized to provide a forward deployed presence to promote peace and stability and are designed to be the Marine Corps' first-on-the-scene force. Special Purpose MAGTFs (SPMAGTFs) are task-organized to accomplish specific missions, including humanitarian assistance, disaster relief, peacetime engagement activities, or regionally focused exercises.

MAGTFs, along with other Marine Corps unique forces, such as Fleet Anti-Terrorism Security Teams (FASTs) and the Chemical Biological Incident Response Force (CBIRF), represent a continuum of response capabilities tethered to national, Regional Combatant Commanders, and naval requirements. Whether coming from amphibious ships, marrying up with maritime prepositioning ships, arriving via strategic airlift, responding to terrorist attacks, or handling calls for consequence management, they provide a scalable, networked, and potent response force.

The Marine Corps provides today's Joint Force Commanders with fully integrated combined arms, effects focused, air-land-sea forces—forces fully networked to ensure interoperability across a range of functions, distances, and missions. Future Marine forces, task organized, forward deployed, and built around rapid effects oriented decision making, will give tomorrow's Joint Force Commander unparalleled options in a chaotic global environment. These attributes, together with our expeditionary culture and unique training and education, make the Marine Corps ideally suited to enable Joint, Allied, coalition, and interagency operations, both today and in the future.

Marine Corps Strategy 21 – rooted in *Joint Vision 2020* – provides the vision, goals, and aims to support the development of our future combat capabilities. The Marine Corps will continue to provide the National Command Authorities and Regional Combatant Commanders with Marine forces that promote peace and stability through forward presence and peacetime engagement. These forces will be able to respond across the complex spectrum of crisis and conflict, and will be prepared to lead, follow, or be part of any Joint or multinational force to defeat our nation's adversaries.

As we prepare to meet emerging challenges, Marines will capitalize on innovation, experimentation, and technology to enhance existing capabilities while exploring and developing new ones to maximize the effectiveness of our forces. Our new capstone operational concept, *Expeditionary Maneuver Warfare* provides the foundation for a Marine Corps organized, trained, and equipped to conduct expeditionary maneuver warfare in Joint and multinational environments that involve interagency cooperation within the complex

to capitalize on and expand our networked command and control structure to train and educate the future force in effects-sensitive decision making.

4.4 U.S. Air Force NCW Vision

The U.S. Air Force is an integrated aerospace force. Our operational domain stretches from the earth's surface to the outer reaches of space in a seamless operational medium. The Air Force operates aircraft and spacecraft optimized for their environments, but the key to meeting the nation's needs with aerospace power lies in integrating these systems as a network of interrelated capabilities and information. Using a network-centric approach to our operations and planning, we not only take full advantage of expertise in the air, space, and information domains, but we compound that expertise to achieve in Information Superiority effects beyond what is possible in isolation. Our information capabilities support operations across the entire aerospace domain. We are integrating air, space, and information operations to leverage the strengths of each. Our airmen think in terms of controlling, exploiting, and operating within the full aerospace continuum, on both a regional and global scale, to achieve effects extending beyond the horizon.

Intelligence, Surveillance, and Reconnaissance (ISR), aerospace power's oldest mission areas, provides Air Force and Joint decision makers at all levels of command with knowledge—not merely data—about the adversary's capabilities and intentions. Integrated ISR assets directly support the Air Force's ability to provide global awareness throughout the range of military operations. With knowledge that far exceeds that which was possible only a handful of years ago, decision makers achieve the fullest possible understanding of the adversary. ISR contributes to the commander's comprehensive battlespace awareness by providing a window to our adversary's intentions, capabilities, and vulnerabilities.

We are strengthening the ability of our commanders to employ aerospace forces through improvements to their command centers. Our Aerospace Operations Centers (AOCs) will enable them to control aerospace operations conducted in conjunction with Joint, Allied, and Coalition partners. Through efforts such as the Combined Aerospace Operations Center—Experimental (CAOC-X), we will develop new ways of directing aerospace forces, while thoroughly testing the solutions.

In the future, we will have the capability to gather and fuse the full range of information—from national to tactical, in real-time, and to rapidly convert that information to knowledge and understanding—to ensure dominance over adversaries.

The Air Force is configured as an Expeditionary Aerospace Force (EAF) capable of the full spectrum of aerospace operations. We have constituted ten deployable Aerospace Expeditionary Forces (AEFs). Two AEFs, trained to task, are always deployed or on call to meet current operational requirements while the remaining force reconstitutes, trains, exercises, and prepares for the full spectrum of operations. AEFs provide Joint force commanders with ready and complete aerospace force packages that can be quickly tailored to meet the spectrum of contingencies—ensuring situational awareness, freedom from attack, freedom to maneuver, and freedom to attack.

AEFs provide the means for enabling the core competencies described in Air Force Vision 2020:

- Aerospace Superiority
- Information Superiority
- Global Attack
- Precision Engagement
- Rapid Global Mobility
- Agile Combat Support

The operational environment in which these competencies are exercised includes numerous threats. Not just new adversarial aircraft, but advanced surface-to-air missiles, theater ballistic missiles, cruise missiles, a multitude of international space systems, and an ever-increasing information warfare threat. In this challenging environment, our improved capabilities will provide Joint forces with the capability to deny an adversary not only the traditional sanctuaries of night, weather, and terrain, but deny Information Superiority as well.

With advanced integrated ISR and C2 capabilities, networked into a SoS, we'll improve our capabilities to find, fix, assess, track, target, and engage anything of military significance, anywhere. We'll evolve from doing this in hours, to doing it in minutes. Information Superiority will be the pivotal enabler of this capability. We will continue to improve our decision cycle, making better decisions faster—faster than an adversary can react—to ensure information dominance over our adversaries.

We will continue to enhance our reach. We'll be able to achieve greater desired effects from whatever range we choose. Aerospace power's ability to strike directly from the U.S.,

or from regional bases, ensures maximum flexibility. Improvements in standoff and penetration capabilities will enable us to operate with reduced vulnerabilities.

With advanced networked airborne and spaceborne sensors and weapons systems capable of precisely engaging targets of all types, we will be able to strike effectively wherever and whenever necessary. With future capabilities, we'll harness new ways to achieve effects, ranging from directed energy to non-lethal weapons.

We continue to improve our strategic agility, providing the mobility to rapidly position and reposition forces in any environment, anywhere in the world. At the same time, our combat support is becoming more agile. We are streamlining what we take with us, reducing our forward support footprint by 50 percent. We will rely increasingly on distributed and reachback operations to efficiently sustain our forces, providing time-definite delivery of needed capabilities. Fast, flexible, responsive, reliable support will be the foundation of all Air Force operations. To accomplish this, we will leverage a broad range of information technologies to robustly network the force and continue transforming our operational capabilities.

The U.S. Air Force vision for NCW is more fully stated in Appendix A.4 of the report.

Section 5

Prerequisites for NCW

It is one thing to talk about network-centric concepts and quite another to see them implemented. A lot of things need to come together to make a network-centric capability a reality. This is because by their nature network-centric capabilities:

- Involve new ways of thinking about how task and missions can be accomplished
- Change organizational roles and responsibilities
- Require that information be shared outside of existing communities
- Depend, in part, upon the development of new technologies
- Require a better understanding of how to create, share, and exploit awareness
- Create combat and operational value in new ways

Therefore, to make NCW a reality, a number of conditions must exist. These include a climate that fosters disruptive innovation, an infostructure that is robustly networked to support information sharing and collaboration, an appropriate technology base, an improved understanding of related issues, and a way of analyzing and assessing network-centric capabilities. Each of these is discussed in more detail below beginning with the requirement for innovation.

5.1 Innovation

Innovation is an essential core component of DoD's transformation. However, innovation is not always easy, and some types of innovation are more difficult to achieve than other types. Organizations and individuals often tend to resist the change that is required to foster a culture that supports and exploits the output of innovation. The greater the change required the more resistance. The result is that many innovations often take a very long time to gain acceptance and be institutionalized, often are not implemented in the organization where they were conceived, and some innovations simply never see the light of day. For example, while Xerox's Palo Alto Research Center invented both the "computer mouse" and the "Graphical User Interface" (GUI)," it was Apple Computer that effectively exploited these innovations to create the Macintosh computer. Similarly, the British invented the tank. Although they first employed it in combat during the Battle of the Somme on September 15, 1916, and later at the Battle of Cambrai on November 20, 1917, they were not

the first to learn how to fully exploit its capabilities. This was first shown by the Germans with *Blitzkrieg* in 1939-1940.[57]

The President in his commencement address at the U.S. Naval Academy recently noted the importance of innovation and the need to create a culture within the DoD that can support and exploit innovation.[58]

> *Creativity and imaginative thinking are the great competitive advantages of America and America's military. Today, I call upon you to seize and to join this tradition of creativity and innovation. Our national and military leaders owe you a culture that supports innovation and a system that rewards it.*
>
> *As President, I am committed to fostering a military culture where intelligent risk taking and forward thinking are rewarded, not dreaded. And I'm committed to ensuring that visionary leaders who take risks are recognized and promoted.*

To understand why creating a culture and organizational environment that can support the type of innovation that is required for successful transformation within the DoD is likely to be challenging, it is important to understand that there are two distinct types of innovation.

In *The Innovator's Dilemma*, Clayton Christensen introduced the concepts of "sustaining innovation" and "disruptive innovation," and explained why so many great companies have failed when faced with the challenges posed by seemingly trivial or insignificant technologies.[59] Christensen describes sustaining innovations as those that improve the performance of existing products or services along the dimensions of performance that mainstream customers in major markets have historically valued. In other words, they give customers something more or better in the attributes they already value.[60] In contrast, disruptive innovations bring to market value propositions that are very different than those previously available. Generally disruptive technologies underperform established products when measured with mainstream market metrics. But they have other features that are valued by some (usually new) customers that enable the products based on disruptive technologies to gain an initial beachhead in a market. Christensen found that products based

---

57 Richard O. Hundley, *Past Revolutions—Future Transformations,* National Defense Research Institute, RAND, 1999, p. 13-14.

58 President George W. Bush, Commencement Speech at U.S. Naval Academy, 25 May 2001.

59 Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail,* Harvard Business School Press, 1997, p. xv-xvi.

60 Anirudh Dhebar, "Six Chasms in Need of Crossing," *MIT Sloan Management Review*, Spring 2001, p. 95-99.

on disruptive technologies are typically cheaper, simpler, smaller, frequently more convenient to use, and initially garner lower profit margins. As a consequence, products based on disruptive technologies are not viewed by large companies as being adequate to meet their growth needs. Over time, however, through a combination of technological and process improvement and market feedback, the performance of products based on disruptive technologies improves to the point that they are more attractive in terms of price and performance than products produced by mainstream companies for the mainstream markets. It is at this point that the market defects and embraces the disruptive innovation, and as a consequence these new products displace existing products.

Central to Christensen's argument is the observation of the key role that an organization's core competencies play in determining the success and failure of innovation. For example, in the process of developing, marketing, and selling their products, companies develop core competencies that can be described in terms of resources, processes, and values. Resources include tangible items, such as people, equipment, technologies, and cash, as well as intangible ones, such as product designs, brands, information, and relationships with suppliers, distributors, and customers. Christensen defines processes as "the patterns of interaction, coordination, communication, and decision making into products or services of greater worth." Most organizations have formal processes that are visible and explicitly defined that co-exist with informal processes that are less visible and evolve over time. Values are defined as "the standards by which employees set priorities that enable them to judge whether an order is attractive or unattractive, whether a customer is more or less important, whether an idea for a new product is attractive or marginal, etc."[61] The impact of the interaction between values, processes, and resources is described below in the context of sustaining innovation in the commercial sector and in the DoD.

A key finding is that ***the competencies that organizations develop in becoming successful at sustaining innovation create impediments to disruptive innovation.*** Although Christensen focused on the commercial sector, it is clear that the concepts he proposed apply to innovation in warfare and military organizations and are particularly relevant to DoD's on-going transformation efforts. In retrospect, one sees the key role that values and processes played in the success and failure of innovation in previous RMAs.

Sustaining Innovation: Most successful companies, at one time or another, become very good at sustaining innovation, because they must continuously innovate to develop new products to remain viable as business entities. In the process of developing, marketing, and selling their products, companies develop a suite of core competencies that can be described in terms of resources, processes, and values. For example, for companies to grow sales at a

---

61 Clayton M. Christensen and Michael Overdorf, "Meeting the Challenge of Disruptive Change," *Harvard Business Review,* March-April 2000, p. 66-76.

healthy rate (15% to 20%), they need to be able to listen to and understand the needs of their largest customers or customer base and to develop products that have features these customers are interested in. In the process of becoming successful, companies develop processes and values (rule sets, decision basis) for allocating resources internally and for deciding how big a market needs to be to be worth pursuing. For example, a company with $10 billion in sales, that is growing sales at a rate of 15%, needs to add $1.5 billion in new sales to continue growing at the same rate. Consequently, only products or services that are perceived able to contribute directly to achieving this level of sales or to provide profit margins required to meet earnings objectives, are viewed as worth pursuing. As a result of this decision logic, technology innovations that don't meet these criteria are not pursued or developed by large companies.[62]

An example of sustaining innovation is the innovation performed by Intel in developing the Intel 486 chip after it had already developed the Intel 386 chip. A clear market existed for the Intel 386 chip, and companies, such as Compaq and IBM, that bought the Intel 386 chip to include in their computer products were clearly interested in the improved performance provided by the Intel 486 chip. Consequently, it was clear to the leadership at Intel that a market existed for the Intel 486 chip, a product that improved the performance of a computing architecture already proven and accepted in the market place.

Based on these insights, one can observe that DoD is second to none at sustaining innovation. We build very good platforms and weapons and continuously perfect them. DoD's success at the development of stealth and precision weapons is a testimonial to our ability to succeed at sustaining innovation. These capabilities are currently aligned with existing "community values." Senior leaders in key resource allocation positions share these values. Warfighting commanders have a similar value system and demand these capabilities and performance improvements from the business side of DoD. Consequently (and logically) resources are allocated based on the warfighting calculus these leaders have developed over their careers. Similarly, our processes for allocating resources and the organizational relationships required for supporting the acquisition of major systems work well.

Disruptive Innovation: Disruptive innovations pose challenges for commercial and military organizations alike. In the commercial sector, disruptive technologies generally underperform established products in mainstream markets when measured with traditional value metrics, but have other features valued by small market segments.[63] A key feature of disruptive technologies is that initially there is a great deal of uncertainty regarding the size

---

62 Christensen, *The Innovator's Dilemma*, p. xx-xxi.

63 *Ibid.,* p. xv.

and attributes of the potential market. In fact, as Christensen notes, there is a high likelihood that no market data exists for the disruptive innovation.[64] As a result, in the judgment of mainstream market decision making, the initial market opportunity is either viewed as being inadequate to meet the growth needs of large companies or perhaps even non-existent. This phenomenon generates a key insight into how one can begin to cope with the management struggle required as an organization searches for ways to sustain market leadership in a changing market environment. Examples of disruptive technological innovations in the commercial sector include hydraulic construction equipment, steel minimills, and computer disk drives.

Hydraulic vs. Cable Actuated Construction Equipment: Excavators and their steam shovel predecessors are huge pieces of capital equipment sold to excavation contractors (requiring significant levels of capital investment that are analogous to those made by DoD and other armed forces). Over its history, leading firms successfully adapted a series of sustaining innovations to improve their cable-actuated equipment. They effectively developed competencies required to perform both incremental and radical technological innovation at both the component and architecture level. However, almost the entire population of cable-actuated shovel manufacturers was wiped out by a disruptive technology, hydraulics, that market leaders, by listening to their best customers and honing their economic structures with best business school practices had caused them to ignore. Hydraulic construction equipment, when first introduced, did not have performance attributes that allowed it to compete with cable-actuated equipment. It first succeeded commercially in the mid-1950s in the form of the "backhoe" used to dig trenches for water and sewer lines from the street to the foundations of houses, a relatively small segment of the construction market, one that was not high margin or high volume for large equipment manufacturers. These small jobs had never merited the time or expense required to bring in big, imprecise, cable-actuated shovels. Consequently, the jobs had been done by hand. The backhoe succeeded in this niche market by meeting the cost and performance needs of a new customer base that was not served by existing products. Over time, the performance of hydraulic construction equipment was improved, and over a period of years, hydraulic construction equipment replaced cable-actuated construction equipment in almost all markets. Only a small fraction of the established manufacturers (4 of 30) in the 1950s were able to successfully transform themselves and produce competitive products that employed hydraulic technology.[65]

Minimills vs. Integrated Steel Mills: A similar story is playing out in the steel industry, where steel minimills' share of the steel market has grown from zero in the mid-1960s to

---

64 *Ibid.,* p. xxi-xxii, 147-163.

65 *Ibid.,* p. 64-73.

over 40 percent in 1995. Minimills get their name from the scale at which they produce cost-competitive finished steel from scrap: in less than one-tenth the scale required for an integrated steel mill, which uses traditional methods of iron ore and blast and basic oxygen furnaces. When steel minimills first became operational in the mid-1960s, they could only manufacture "rebar" (concrete reinforcement bars) from scrap steel, a relatively low quality, low profit margin product that the big mills were happy to let go to the insurgents. Over time, minimill technology gradually improved, producing higher quality products, first rebar, and then seamless pipe, then structural steel, and finally sheet steel that could compete in terms of quality and cost with the high margin product of integrated steel mills. Today, minimills virtually dominate the North American markets for rods, bars, and structural beams. Yet not a single one of the world's major integrated steel companies has built a mill employing minimill technology.[66]

Computer Disk Drives: Perhaps the most compelling case for the power of disruptive innovation is the story of the IT companies that produced successive generations of computer disk drives. From 1975 to the present, the computer industry has successfully developed five different classes of disk drives to meet the demands of successive generations of computers:

Mainframe Computer	14 inch drives
Minicomputers	8 and 5.25 inch drives
Desktop Personal Computer	5.25 and 3.5 inch drives
Portable Notebook Computer	3.5 and 2.5 inch drives

While many people are aware of these successive generations of technology, few are aware of the fact that, with few exceptions, the leaders in one generation of technology were not the leaders of the next generation of technology. For example, when Seagate Technology introduced the 5.25-inch drive in 1980, with an initial capacity of 5 and 10 megabytes (MB), minicomputer manufactures were not interested. They were demanding drives with 40 and 60 MB. The initial success of the 5.25-drive was linked to the development of the personal computer. Once the 5.25-inch drive became commercially viable, its performance measured in terms of capacity improved by roughly 50% a year between 1980 and 1990. As the rapidly increasing performance of 5.25-inch drives intersected the more slowly growing performance of 8-inch drives, minicomputer manufacturers started using 5.25-inch drives. By 1985 only half of the firms producing 8-inch drives had introduced 5.25-inch models. The other half never did. Of the four leading 8-inch drive makers, Shugart Associates, Micropolis, Priam, and Quantum, only Micropolis survived to become a significant

66 *Ibid.,* p. 87-93.

manufacturer of 5.25- drives, and that was only accomplished with Herculean managerial efforts.[67]

A similar story took place at each of the other technology transitions. In each case, the market leaders in one generation of disk drive technology were not the market leaders in the next generation of disk drive technology.

In each of these historic examples, the market leaders had developed core competencies that enabled them to excel at sustaining innovation and dominate their markets. They grew their businesses by listening to their largest customers and developing products that met their needs. However, in each case, the dominant companies were unseated in key markets by competitors who were able to successfully perform disruptive innovation.

Implications for Military Organizations*:* In the context of warfare and military organizations, it is now clear in retrospect that the theory of disruptive innovation, appropriately modified, helps explain the revolutionary impact that key technologies have had in warfare. In World War I (WWI), when the British first introduced the tank, its technical performance was limited; consequently it was employed in a supporting role to infantry. The full "revolutionary" potential of the tank was not fully realized until tank technology improved and the German army developed the tactics, techniques, and procedures of *Blitzkrieg,* which paired the tank with tactical aviation and the radio. One can see that the same factors that inhibit successful companies from exploiting disruptive technologies in the commercial sector (uncertainty, threats to existing values, competition for resources with existing organizational power structures) were at work in the American, British, and French Armies in the inter-war years. In retrospect, it is clear that the disruptive attributes of the tank, which inhibited its early adoption by the Armies of the Allies, resulted in the revolutionary impact of *Blitzkrieg* when the Germans first introduced it. In the German Army, it was the leadership of General von Seeckt and others that enabled the core competencies of the infantry (with its associated resources, processes, and values) to be successfully disrupted. General von Seeckt was successful in part because he understood that structural changes in the security environment created the need for innovation, he had already established himself in the German Army based on traditional criteria for performance, and he had the power necessary to champion disruptive innovation.[68]

---

67 *Ibid.,* p. 3-28.

68 Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military,* Cornell University Press, Ithaca, New York, 1991, p. 76-105.

> *Military organizations don't necessarily "evolve." They may or may not have leaders able to create organizational processes and institutional rules that are essential to that military's ability to increase its combat potential.*
> ***American & British Aircraft Carrier Development, 1919-1941**, p. 192.*

A similar story was played out with carrier aviation. Here, the challenges of disruptive innovation were met head on by the U.S. and Imperial Japanese Navies, but not by the Royal Navy. In the U.S. and Japanese Navies, the combination of improving technology (aircraft, aircraft carriers) and new tactics, techniques, and procedures were matured to the point that they successfully displaced the battleship (with its associated resources, processes, and values—including the "battleship admirals"[69]) as the dominant "core competency" of naval forces. What made carrier aviation in the U.S. Navy a success was the combination of the right people, a set of organizations, and a potentially huge aviation industrial base, which included the automobile industry.[70] It is important to point out that the situation in the Pacific War, with both the U.S. and Japanese Navies successfully introducing aircraft carriers and naval aviation, was dramatically different from the situation in the European theater where only the German Army had matured the competencies associated with *Blitzkrieg*. Consequently, the Germans were able to achieve revolutionary effects at the onset of World War II that were to a large extent denied to the Japanese.[71]

> *The history of innovation in carrier aviation says something of great importance about military innovation generally: it is not a process that usually proceeds in a linear way. But hindsight tends to make us think that it does. Because we try to compose coherent histories of innovation, we may actually overlook the uncertainty and chance that inevitably exist.*
> ***American & British Aircraft Carrier Development: 1919-1941**, p. 188.*

With the benefit of these historical insights, one can gain a better perspective into the current day challenges associated with the successful implementation of disruptive innovation in military organizations, of which Network Centric Warfare can and should be viewed as an example. Clearly, key aspects and attributes of Network Centric Warfare are fundamentally disruptive in nature. For example, information sharing and collaboration disrupt existing organizational decision making processes, authorities, and values. Allocating resources to the networking of the force, potentially at the expense of platform

---

69 Thomas C. Hone, Norman Friedman, and Mark D. Mandeles, *American & British Aircraft Carrier Development: 1914-1941,* Naval Institute Press, Annapolis, MD, 1999, p. 2-3.

70 *Ibid.,* p. 174.

71 *Ibid,* p. 51-82.

and weapon acquisition and "modernization," threatens existing "platform-centric" power structures.

Platform-centric values reinforce platform-centric thinking, which left unchecked, will lead only to incremental, sustaining innovation. Platform-centric thinking leads to questions such as:

- If existing platforms and their associated tactics, techniques, and procedures were clearly decisive in *Operation Desert Shield, Desert Storm,* why is NCW relevant?
- In the present absence of a peer competitor, what is the compelling rationale for pursuing disruptive innovation in the form of NCW?

In contrast, network-centric thinking leads to questions such as:

- How can the digitization and networking of existing platforms increase combat power?
- Can investments in NCW provide comparatively larger returns on investment than investments in sustaining innovation?

The inability to deal effectively with disruptive innovation can have significant consequences. In a number of industries, many companies have foundered and gone out of business, are currently in the process of foundering, or have foundered and been acquired because they were unable to deal effectively with challenges posed by disruptive innovation. This list of companies is both long and distinguished. James Utterback has noted several phenomena regarding innovation in markets that reinforce Christensen's findings:[72]

- Every change in market requirements, even trivial ones, results in changes in leadership.
- When challenged, the status quo technology always increases capability by several orders of magnitude.
- Complex and overly complicated products often lead to market failure.

If the current DoD transformation were about sustaining innovation we would not need to make any major policy, process, strategy, or organizational changes. But the principle component of this transformation is information. As we have discussed, advances in information technologies are enabling us to operate in a new part of the information domain—with both increased information richness and reach—that, in turn, creates

---

72 Presentation at the CapGemini Ernst&Young innovation Management Roundtable, 17 May 2001. See also James M. Utterback, *Mastering the Dynamics of Innovation,* Harvard Business School Press, 1994, 1996.

opportunities to do things differently. In order to do things differently, the established order of things must change resulting in disruption to:

- Patterns of investment
- Organizational relationships
- Institutional values

Left to their own devices, absent an external threat, organizations will choose the path of least resistance—the path of sustaining innovation.[73] In this case, that path would be to continue a platform-centric rather than a network-centric approach to warfare. Military history is replete with examples demonstrating that even when the technology was widely available, disruptive innovations made possible by this technology did not occur concurrently with the availability of the technology, but only occurred when a number of conditions were met. A combination of the right people, a set of organizations that could learn, the proper institutional relationships among those organizations, and an established industrial base to supply the technology, products, and services is necessary for disruptive innovation to occur.

As discussed previously in this section, *Blitzkreig* and Carrier Aviation are two recent examples where these conditions came together to allow disruptive innovation. We have the industrial base necessary to support NCW. Now we need to make sure that the other conditions are met. Among these conditions are those listed below, called out in a RAND report on transformation.[74] The degree to which these conditions are satisfied is provided in the right column of Table 4-1.

---

73 Evidence of this is presented by Christensen as well as John Kotter in *Leading Change.*

74 Richard O. Hundley, *Past Revolutions–Future Transformations,* National Defense Research Institute - RAND, 1999.

Table 5-1. Preconditions for RMA and State of DoD NCW

Preconditions for RMA	State of DoD NCW
Fertile set of enabling technologies	Have means but not the infostructure
Unmet military challenges	These exist
Receptive organizational climate	Needs to be fostered
Support from the top	Presidential support must be acted upon by DoD civilian and military leadership
Mechanisms for experimentation	Need to improve and coordinate
Focus on definite things or a short list of things	NCW provides this focus
Ultimately challenge someone's core competency	NCW challenges DoD core competency
Ways of responding positively to successful experiments	Need to improve

To realize the potential that NCW offers, DoD must commit itself to overcoming the obstacles posed by disruptive innovation. Creating the conditions necessary for successful change requires a highly visible senior-level advocate dedicated to creating the conditions that will enable us to overcome impediments to progress. It is for this reason that an Office of Transformation, reporting to the highest levels of the Department, is so essential. To make NCW a reality, this office needs to work effectively across organizational lines to ensure that a coordinated strategy is developed and implemented. This will require an unprecedented degree of collaboration among the various communities of interest within DoD. Elements of this coordinated strategy are discussed in Section 6, as well as the rest of this section. The Office of Transformation will need to be independent of established organizations and values, yet will need to work through these established organizations to effect change. This Office of Transformation must take the "corporate view" and serve as an honest broker to forge new relationships and investment strategies. This office needs to be the advocate for NCW and related transformational issues. The challenges to be faced are on a scale unprecedented in history because the changes that will be brought about will touch every significant organization in DoD. **What separates this RMA from previous RMAs is that it is not associated predominately with a tangible asset (such as tanks, aircraft carriers, and carrier aircraft,) but with information and how it can be leveraged by a warfighting force.**

For innovation to occur, a military force must have a set of organizational relationships and a process that examines critically and fairly all new concepts with the potential for exploitation. No such process or set of relationships can be foolproof. No such process or relationships, no matter how faithfully or intelligently executed, will always succeed. Moreover, no such process and organizational relationship will be, or should be immune from larger questions taken up by organizations, such as the American Congress, that are outside the military. ***American & British Aircraft Carrier Development 1914-1941***, p. 196.

5.2 Infostructure

Just as the commercial sector required a critical mass of connectivity, computers, and customers to successfully innovate with e-business solutions, DoD requires a similar critical mass of integrated communications and computing capability. Therefore, DoD's infostructure is on the critical path to transformation. The ability to conceive of, experiment with, and implement new network-centric ways of doing business that leverage the power of Information Age concepts and technologies depends upon what information can be collected, how it can be processed, and the extent to which it can be distributed throughout the organization. The ability to bring this capability to war will depend upon how well it can be secured and upon its reliability. The DoD requires an infostructure that is secure, robustly networked, seamless, and coherent; that has access to required radio frequency spectrum; that has built-in security; that supports Joint and coalition operations; that is able to generate synergy between the RBA and the Revolution in Military Affairs (RMA); that leverages commercial technology and accommodates evolution, and that can exploit space-based capabilities.

Security Built In. The ability to protect our information, systems, programs, people, and facilities in a risk management environment directly impacts our ability to successfully prosecute the military mission. DoD must develop improved methods and techniques to anticipate probable threats to DoD mission success, ascertain our vulnerabilities, and integrate practical countermeasures—maintaining a security-conscious workforce during concept formulation through deployment and sustainment of systems, applying effective countermeasures to the full range of systems, programs, and critical technologies.[75] Security, like interoperability, must be engineered into systems from the beginning to be effective and affordable. The forging of a coherent infostructure out of many legacy systems poses a significant challenge in this regard. The ability to maintain security as information

---

75 McGroddy, et el., *Realizing the Potential of C4I: Fundamental Challenges,* National Academy Press, Washington, D.C., 1999, p. 130-178.

transits system interfaces is the key. DoD's continuing migration from analog to digital systems will facilitate these efforts. However, there will always be legacy systems and systems that coalition partners bring to the table that do not have adequate security. DoD is exploring ways to deal with these exceptions; however, these will, in all likelihood, entail limiting the functionality and utility of these non-conforming systems. A technique is to provide such coalition partners the minimum required equipment or architecture to interoperate.

Robustly Networked. The robustness of the infostructure is dependent on sufficient connectivity and bandwidth. The explosive growth of cell phones, the Internet, and personal digital devices (PDAs) has increased competition for bandwidth in general, and radio frequency spectrum in particular. Access to adequate radio frequency spectrum for data transport like satellite links, wireless networks, and mobile communications systems are essential for DoD to operate effectively on a global basis. Spectrum limitations will adversely impact the ability of DoD to carry out Network Centric Operations. To ensure access to adequate spectrum in the short term, DoD must articulate the spectrum requirements associated with current operations and work with national and international forums and individual nation states to secure the required spectrum. For the longer term, DoD must conduct research into better ways to utilize spectrum, identify spectrum requirements necessary to support mature Network Centric Operations, and work with others to ensure that spectrum is allocated in a way that does not adversely impact DoD ability to carry out its assigned missions.

Seamless and Coherent. To facilitate the end-to-end flow of information throughout the DoD necessary to support Network Centric Operations, information processes must be transparent to users. To accomplish this, DoD systems must transition from isolated stovepiped environments to a seamless and coherent infostructure. Creating this requires the establishment of a Department-wide mechanism for gaining visibility into the many separate planning, budgeting, acquisition, operations, and maintenance activities that contribute to DoD's information systems and processes. DoD's Global Information Grid is designed to achieve this by creating a DoD-wide network management solution, comprised of enterprise network policies, strategies, architectures, focused investments, and network management control centers that bring order out of the currently highly fragmented Service-centric DoD information infrastructure.

Born Joint and Combined. Future operations will be Joint and Combined. Their effectiveness will depend upon the ability of DoD to share information and to collaborate externally as well as internally. Therefore, interoperability is a key parameter in all DoD operational and systems architectures.[76] Experience has shown that retrofitting

---

[76] *Ibid.,* 64-129.

interoperability is costly, does not satisfy mission requirements, and creates security problems. Born Joint and Combined systems, achieved by engineering in interoperability attributes from the start, will provide the needed capabilities more economically and without the vulnerabilities created by retrofitting. There must however remain a balance between legacy reach back and leaps in technology. We cannot allow legacy interoperability to overburden and therefore limit better performance and combat power.

RBA and RMA Synergy. The DoD is undergoing twin revolutions driven by the concepts and technologies of the Information Age. The RBA, modeled on the successes experienced in the commercial sector, is transforming the business side of DoD while the RMA, based upon adapting lessons from other domains to the domain of warfare, is transforming military operations. These are not independent revolutions. Transformations in the business side not only free up resources that can be more highly leveraged by combatant commands, but also provide improvements in combat support (CS) that enable more effective concepts of operation, organization, doctrine, and the like. They enable the RMA and will transform military operations, increasing the tempo of operations, the speed of command, and, as a result, achieve greater lethality with increased survivability. The net result of RBA and RMA synergy will be an opportunity for quicker and more decisive victories, using less "tail" (support) and bringing to bear more "tooth" (warfighting capability).

Leverages Commercial Technology. The engine driving advances in IT is in the commercial sector. Commercial firms are adopting information technologies and finding new ways to create competitive advantages that leverage IT. The DoD benefits from the enormity of the commercial IT market because its scale drives down the costs of off-the-shelf capabilities and fuels an unprecedented rate of improvement in cost and performance. As a result, DoD now can reap the benefits of private sector investments, thus saving its scarce R&D dollars to invest in militarily significant areas that the commercial sector is not addressing. Furthermore, adopting commercial standards and leveraging COTS capabilities to the extent possible makes it easier to achieve and maintain desired levels of interoperability. There are, of course, some drawbacks in this role reversal. In the past, government led the way in new information technologies and was able to control the most sensitive of them. Now the latest technology is available to potential foes and Allies alike. With rapidly changing commercial innovation now the source of the latest breakthroughs, DoD is no longer master of the course that technology takes. DoD therefore must learn to work closely with industry to ensure that the Department's requirements can be satisfied and can influence industry's future technology developments. The Department is looking for non-traditional partners in many of these areas. For example, the banking industry has many of the same requirements Defense has for privacy and authentication of transactions. Similarly, the robotics and medical instrument industry, like the military, has requirements for computers that can operate in high electrical noise environments. By leveraging buying

power across these non-traditional market sectors, Defense requirements can be met at a fraction of the IT R&D investments of the Cold War era.

Accommodates Evolution. Change is the constant of the Information Age. DoD infostructure therefore must be designed to accommodate change as both requirements and as technology evolves. A comprehensive strategy that consists of appropriate architectures, standards, design principles, configuration management, and regression testing will be incorporated into DoD's infostructure processes.

5.3 Technology

A host of information technologies provide capabilities needed to facilitate the sharing of information, the creation of high quality awareness, and the development of shared situational awareness. These fall into the following categories: collection, exploitation, storage, retrieval, distribution, collaborative environments, presentation, Information Operations and Assurance, and the technologies that help extract knowledge and understanding from data and information. These knowledge-related technologies include a variety of analyses, modeling, simulation, problem solving, and other decision support tools. For DoD to maintain and enhance its information advantage, R&D efforts must be focused upon technologies and/or specific applications of technology that are not being adequately addressed by the commercial sector. Section 10.4, Science and Technology, provides an in-depth discussion of ongoing Science and Technology activities related to NCW.

Other technologies will enable best management of complex adaptive systems and help achieve increased synchronization.

Experience shows that advances in technology do not automatically translate into cost-effective applications. In fact, it takes a great deal of time and effort to understand operational implications of advances in information technologies, develop military CONOPS and modify doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) to exploit new capability. Thus, while investments in IT are necessary to achieve Information Superiority, these investments are not in and of themselves sufficient to achieve. Achieving Information Superiority requires a close partnership between technologists and warfighters, and a balanced set of investments that ensure that each of the elements of Information Superiority is adequately addressed.

5.4 Research

There is much about the very nature of network-centric concepts and the application of these concepts to the domain of warfare that we do not understand or even know where our understanding is very limited. To begin with, we know relatively little about how to turn the information we collect and display into shared situational awareness. Most of our efforts to date have been focused upon getting better information in the first place. Now that we have been able to greatly improve what we can collect, it is time to pay more attention to how we

can move this data up the knowledge chain so that it will result in improved awareness. Second, we have a very limited understanding of how to achieve shared situational awareness given that similar information is available to two or more parties. Again we have spent most of our time and resource in enabling the sharing of information. Now that we can share information widely, the time is here to begin to understand how we can turn shared information into shared situational awareness. Third, to date most work in decision theory and tools has focused upon a single decision maker. We need to move beyond this to shed light upon how distributed teams behave and how these teams can collaborate to make synergistic or synchronized decisions. Fourth, we have heretofore focused upon how good information helps decision making. Now we need to expand upon decision making related research to deal with how bad information affects decision making and how decision makers can best deal with a large variety of disparate sources of information with unknown pedigree and veracity.

Other areas that will require increased focus include the behavior of complex adaptive systems (or more accurately, federations of systems), the emergent properties of small semi-autonomous forces, and the effects of culture on perceptions and behaviors. The above represent just a sampling of the areas that require increased research focus. Existing research organizations are well adapted to addressing the issues and subjects that have occupied them for years. It will not be easy to reallocate resources nor will it be easy to identify and recruit the talent necessary to address these new research areas. Without significant attention to these new research focus areas, there will be only limited intellectual capital available to spur the development and support the implementation of more mature network-centric capabilities.

5.5 Analysis

The value of analysis is directly related to its ability to shed light on the issues, distinguish among the alternatives, and/or reflect reality to, at least, first order. For some time C2-related analyses have been challenged beyond their capabilities. For the most part these analyses have barely been able to reflect rudimentary C4ISR-related capabilities let alone trace their impacts to mission effectiveness. Connectivity has often been used as a surrogate for information sharing. The impacts of cognitive processes and the conditions that affect their performance have generally been ignored. Decision making behavior is usually treated by assumption and is more likely than not a reflection of long standing doctrine rather than behavior designed to match information-related capabilities. The quality of the decisions is usually found in the form of implicit assumptions. Therefore, the effects of improvements in information richness and reach have proven beyond the current state of the practice except for a class of simple, time-critical decisions whose success depends upon the presence or absence of a particular set of data at a given point in time. The treatment of more complex decisions remains largely unexplored.

If analysis activities are going to provide real support to investment decisions related to the development and implementation of network-centric concepts and capabilities, a major effort at improving analysis methodologies and the models that support analysis will be required. The formal adoption of a code of best practice for C2 analysis that provides analysis and customers of analysis assistance dealing with the challenges inherent in analyzing issues related to Information Superiority and NCW would be a good first step. Such a code has already been adopted by the NATO C3 Agency, and is in the process of being updated and enhanced.[77] DoD will consider the new version, expected to be released in 2001, for adoption. Continued research into appropriate metrics and the development of models that are designed to reflect information flows and effects will also be needed if the analytic community is to meet the considerable challenges associated with a network-centric transformation of DoD.

---

77 *NATO Code of Best Practice for Command and Control Assessment,* AC/243 (Panel 7) TR/8, 1998 Edition.

Section 6

Enabling Network Centric Warfare

6.1 Implementation Overview

The capability to conduct NCW depends upon the ability of a critical mass of the force being able to conduct Network Centric Operations. While it has been estimated that only a relatively small portion of the force needs to have this capability to produce a qualitative effect on the battlefield, the network-centric portion of the force must be comprised of the right functional elements. Getting the greatest benefit from a network-centric capability often requires that portions of the force that currently do not work closely together, or work together in an arms length, sequential fashion, need to be part of the network-centric team to enable a new way of doing business—one that is more dynamic and collaborative. First this requires recognition that there may be a better way. Often this recognition comes about only after individuals and organizations have hands-on experience in exchanging information with others. The existence or absence of the following set of enablers strongly influences the nature of the network-centric capabilities that are likely to be developed:

- Connectivity
- Technical Interoperability
- Sense Making (Semantic Interoperability)
- Integrated Processes
- Integrated Protection
- Network-ready Battlespace Enablers

6.1.1 Connectivity

If you have access to the "net," then you can be a player. But connectivity takes on different forms and one's level of participation is limited by the nature of the connectivity that exists across the set of mission participants. Voice connectivity, for example, significantly restricts the richness of the exchange while data connectivity enhances the ability of distributed parties to exchange information and to collaborate with one another.

6.1.2 Technical Interoperability

Technical interoperability exists at a variety of levels that affect the nature of the "conversation" that can take place. There is a huge difference between the ability to send messages back and forth and the ability to directly update databases that feed COPs. In

general, these differences affect the amount of time it takes and the number of people that need to get involved to affect an exchange of information. The more time and human resources involved, the less responsive the resulting process.

6.1.3 Sense Making (Semantic Interoperability)

Network Centric Warfare is based upon the ability of a force to develop shared situational awareness in the cognitive domain. Technical interoperability will get us to the point where the information is correctly represented in distributed systems, but does not ensure that the individuals in different locations, in different organizations, at different echelons have a similar understanding even though they "see" the same thing. With the added complexity of coalition operations that involve different cultures, the problem is greatly compounded. Semantic interoperability is the capability to routinely translate the same information into the same understanding. This is, of course, necessary to develop the shared situational awareness upon which mature forms of Network Centric Warfare are based.

6.1.4 Integrated Processes

Sharing information and collaboration are two different things. One "shares" information in a sequential process that passes output from one stage to the next. Contrast this with a collaborative process in which the product is formed and developed as a result of continuous interactions among key participants. Collaborative planning is such an application. Integrated processes are essential ingredients for mature network-centric applications.

6.1.5 Integrated Protection

In a network-centric environment, security is only as good as the weakest link. Since security is essential to warfighting operations, a lack of integrated protection will constrain network-centric applications and/or organizations individually

6.1.6 Network-Ready Battlespace Enablers

A "net" without its nodes has no potential value. Nodes that are not connected or have limited connectivity (and all of the enablers previously discussed) have limited value. In a platform-centric environment, the potential value of adding or enhancing an entity that is not a node is additive. The potential value of a force is the sum of the potential value of its entities, which in turn is heavily dependent on the nature of the "net" that connects them. A robust, interoperable network adds value to each and every one of its nodes. Hence the potential value of improvements to the capabilities of the network (interoperability, robustness, services provided, etc.) is multiplicative. When nodes are "net-ready," that is, when they are capable of fully interacting with other nodes on the net, the potential value that they contribute is also multiplicative.

6.1.7 Turning Potential Value Into Real Value

The above enablers of Network Centric Operations increase the potential value of the force (the network and its nodes). The following enablers contribute to turning this potential value into real value on the battlefields of the future:

- A personnel system that rewards disruptive innovation
- A personnel system that rewards Jointness
- Experimental environments that provide hands-on experience with advanced information technologies
- Opportunities for Joint and coalition experimentation
- Organizational incentives to share information and to collaborate
- A requirements process that is closely tied to the results of experimentation
- An acquisition process that can take the results of experimentation and produce fielded capability quickly.

Section 7

DoD NCW Implementation Strategy

7.1 Overview

Bringing network-centric concepts and capabilities to fruition will require a coordinated strategy that is characterized by an unprecedented degree of collaboration among the various communities of interest within DoD.

This collaboration is necessary to bring different perspectives to the table to facilitate disruptive innovation by creating crosscutting processes that support the co-evolution of concepts, mature them, and then develop and implement integrated capability packages. Moving from concepts to reality requires the development of network-centric mission capability packages and an infostructure that can support them.

7.1.1 A Strategy of Co-Evolution

The challenges associated with stimulating and protecting disruptive innovation must be addressed head on. There is an increasing realization that a new process is required to achieve transformation objectives. History teaches many lessons with respect to warfighting innovation. One is that innovation is messy. Another is the importance of creating an environment where discovery, failure, and learning are tolerated and fostered. Out of this analysis of history and ongoing developments in the science of complexity has emerged the concept of co-evolution. Co-evolution refers to a process through which simultaneous changes or modifications take place in an ecosystem or system.

In a biological context, species within an ecosystem can co-evolve with each other as a result of changes in the environment or individual changes at the species level.[78]

In a warfighting context, technology (Material), organization, and process (Doctrine, and also Tactics, Techniques, and Procedures) must co-evolve with each other to achieve dramatic changes in warfighting effectiveness. This is what transpired as the disruptive innovations of *Blitzkrieg* and Carrier Aviation matured from concept to reality. Without being actively encouraged and protected, these innovations would probably not have become viable capabilities when they did.

---

78 Stuart Kauffman, *At Home in the Universe: The Search for the Laws of Self-Organization and Complexity*, Oxford University Press, 1995, p. 215-224.

7.1.2 Mission Capability Packages

The notion of a Mission Capability Package (MCP) is central to the development of NCW capabilities. It provides a useful construct for describing an operational concept and the integrated collection of Doctrine, Organization, Training, Material, Leadership and Education, Personnel, and Facilities and Infrastructure (DOTMLPF) that is required to make this concept a reality. In some instances, only a subset of DOTMLPF may require significant changes to create a new or improved operational capability.

It should be noted that the concept of MCPs has been developing over the last several years. However, specific management approaches, across DoD Components, are just now under development. Recent changes to Acquisition Policy within the DoD engendered the management of Systems-of-Systems (SoS) to achieve a capability within a Mission Area. The approaches to managing the achievement of these capabilities have been referenced in various ways to include SoS Management, Family-of-Systems (FoS) Management, Portfolio Management, and Mission Capability Management. No specific terminology has yet been adopted across the Department to describe the development or management of MCP or MCP-like approaches. However, in terms of NCW, MCPs do provide a framework for moving forward, and many existing initiatives can be characterized as MCPs.

7.2 Development and Maturation of Network-Centric Mission Capability Packages

The process the DoD will use to take NCW concepts from ideas to fielded operational capability is depicted in Figure 5-1. The notion of a mission capability package is central to this process. A mission capability package consists of an operational concept and associated command concepts, doctrine, organizational arrangements, personnel, information flows, systems, materiel, education, training, and logistics; that is, everything needed to make the concept work in an operational setting. Network-centric MCPs always start as ideas for how things could be done—or MCP concepts.

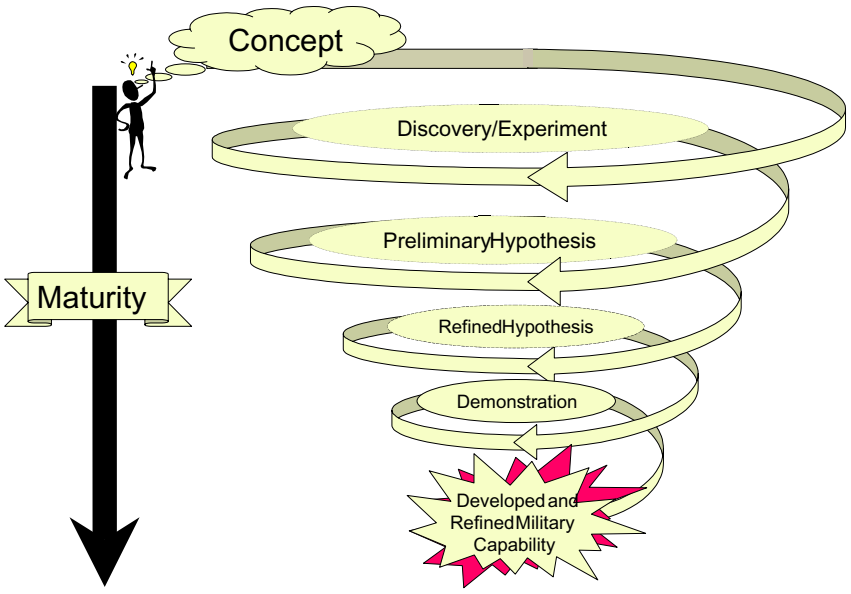


Figure 7-1. From Concept to Capability

Figure 7-2 represents a set of iterations. Each iteration increases in the degree to which it corresponds to reality and, correspondingly, the cost of the iteration and the time needed to accomplish it. Ideas for MCPs can and will be rejected and/or refined at each stage of this process. The concept moves to three main phases on its way to a field capability—concept development, concept refinement, and MCP implementation as analysis, modeling, and simulation give way to different types of experiments and eventually to exercises and demonstrations. Progress may not be linear. MCPs may need to return to previous stages when they are significantly modified or potential problems are identified.

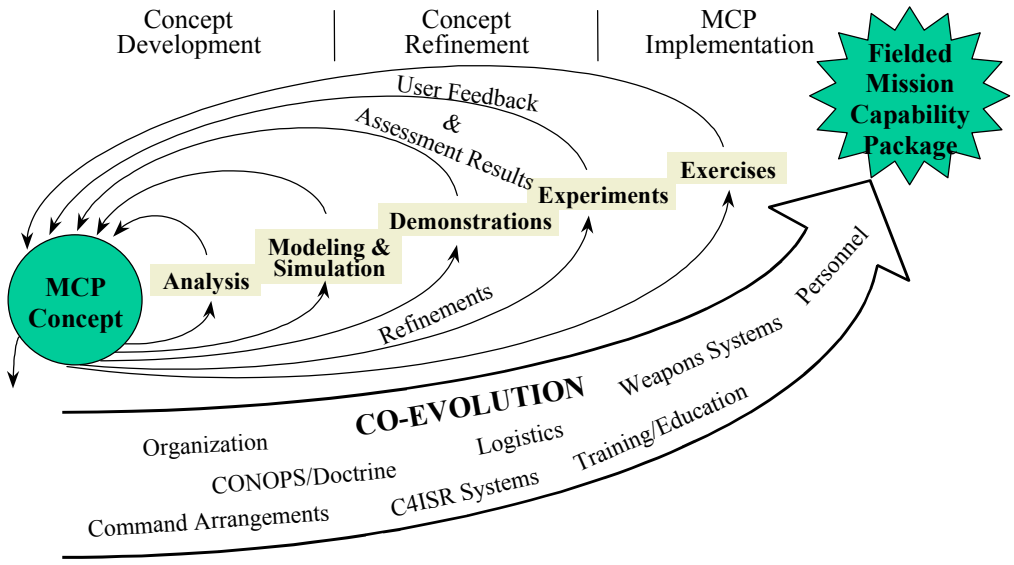


Figure 7-2. The MCP Process

7.2.1 FBE-Delta: A Mission Capability Package Case Study

As a result of the success of the Counter Special Operations Forces (CSOF) component of FBE-Delta, a number of actions were taken by Commander, 7th Fleet, which resulted in an improved capability for the Naval Component Commander to prosecute the CSOF mission in conjunction with Service and Republic of Korea (ROK) forces. (A detailed overview of the CSOF mission explored in FBE-Delta is provided in Section 8.)

The combination of these actions provides a real world example of the changes needed to "co-evolve" an MCP.

Material:

- Improved communications paths to shooters at sea
- Installed Land Attack Warfare System (LAWS) on forward deployed CSOF C2 nodes
- Integrated new Theater TTP into LAWS
- Integrated LAWS with the Automated Deep Operations Coordination System (ADOCS)
- Established logistics support for LAWS

Doctrine:

- Developed new CSOF Tactics

Training/Exercises:

- Quarterly CSOF Exercises
- Foal Eagle: Annual Combined Exercise
- Developed LAWS training program

Each MCP will be different and will need to explicitly address a different set of elements. In all cases, co-evolution of a selected subset of elements will be required for success. Some will be focused upon developing new doctrine and organizations adapted to new information capabilities; others will be engineered to take advantage of new weapons capabilities.

7.3 Co-Evolving the Infostructure

The strategy that the Department will use to co-evolve the infostructure capabilities to support emerging network-centric capability packages is based upon the following:

- Creating awareness: The development of a widespread understanding of why the DoD is moving towards NCW and what this means in terms of the nature of the infostructure necessary to support these capabilities
- Changing Priorities: Increasing the importance of connectivity and interoperability as critical performance factors in the design and acquisition of C4ISR and weapons systems
- Increased Visibility: Creating an annual report on the status of the infostructure
- Improved Oversight: Moving from a system that is program-centric to one that examines portfolios of infostructure-related capabilities

More details regarding DoD approach to developing the infostructure needed to support network-centric MCPs can be found in Section 9, Global Information Grid.

7.4 Evolution of NCW Concepts and Applications

DoD's strategy for developing and implementing network-centric concepts recognizes that the network centric capabilities that are fielded not only need to continuously co-evolve over time, adapting to new threats and opportunities, but also will continue to become "mature." As indicated earlier in this report, there can, and will be, many instantiations of NCW. As experience is gained with these applications of theory, both the theory and the practice will mature. At this point in time, the majority of work is being devoted to networking the force and to improving the quality of the information from which situational

awareness is derived. Other efforts are trying to come to grips with how to adapt traditional command and control processes to take advantage of vastly improved shared situational awareness. Vanguard efforts are beginning to explore new ways of synchronizing actions that could replace traditional notions of command and control. As time goes by, it can be expected that the mix of these efforts will change to be more heavily weighted toward those that are exploring new ways of achieving synchronized effects, including efforts exploring ways that redefine existing missions. For example, the need for conducting close air support operations may be significantly reduced or even eliminated by the increased ability to anticipate the need for air support, and thus avoid or minimize situations that involve a time-critical requirement for conducting air operations in very close proximity to friendly forces.

Section 8

NCW Assessment, Analysis, and Evaluation, Including Evidence of NCW Impacts

8.1 Assessment, Analysis, and Evaluation

Assessments, analyses, and evaluations are an integral part of our strategy to implement NCW. It is important to have the ability to assess what has been achieved at any given point in time relative to a set of explicit milestones in order to determine the degree of progress that has been made and the continued viability of existing plans. Determining the rate of progress will depend upon being able to ascertain what we understand about network-centric concepts, organizations, and operations and where DoD is in the process of translating network-centric concepts into real operational capabilities. We need to know what we understand and what we do not know, not only to measure progress, but also to make progress. This understanding is essential in order to (a) assess the success of our research efforts, (b) focus (or refocus) future efforts, (c) determine what concepts require further experimentation, and (d) identify those that are ripe for implementation. To understand what we know and what we do not know about network-centric concepts and operations, we need the ability to analyze the following:

- The relationships among degree of networking, information sharing, improved awareness, and shared situational awareness (SSA).
- The relationship between SSA and synchronization. For example, the effect of different degrees of SSA and/or collaboration on synchronization.
- The link between synchronization and mission effectiveness.

We also need to be able to analyze enterprise level issues, such as the impact of various levels of connectivity and interoperability on enterprise agility, responsiveness, and effectiveness. A better understanding of these complex relationships will provide the foundation for evaluations of alternative investment strategies, assessments of specific mission capability packages, and decisions regarding (a) the desired nature and characteristics of an infostructure to support Network Centric Operations, (b) force structure, and (c) other decisions related to DOTMLPF.

Thus, it is clear that the ability to make progress is closely related to the ability to measure progress. Recognizing this relationship, DoD will be placing increased emphasis upon the conduct of rigorous assessments, analyses, and evaluations. In the second part of this section, evidence from Service experimentation and operations in peace and combat is presented to show the value of network-centric concepts and capabilities.

8.1.1 Methodology

This report presents current thinking about how to approach the problem of measuring NCW capabilities and their value. Given the immaturity of the theory and practice, it should be expected that the approach and specific measures discussed here would, in time, give way to better ones. In the meantime, the approach and measures suggested below will serve to provide useful benchmarks.

A methodology is needed that can satisfy two interrelated, yet distinct, measurement objectives. The first measurement objective is to determine the links that form the "network-centric value chain," depicted in Figure 8-1 and previously introduced in Section 3. This objective can be satisfied by instantiating a series of linkage hypotheses that correspond to these links.

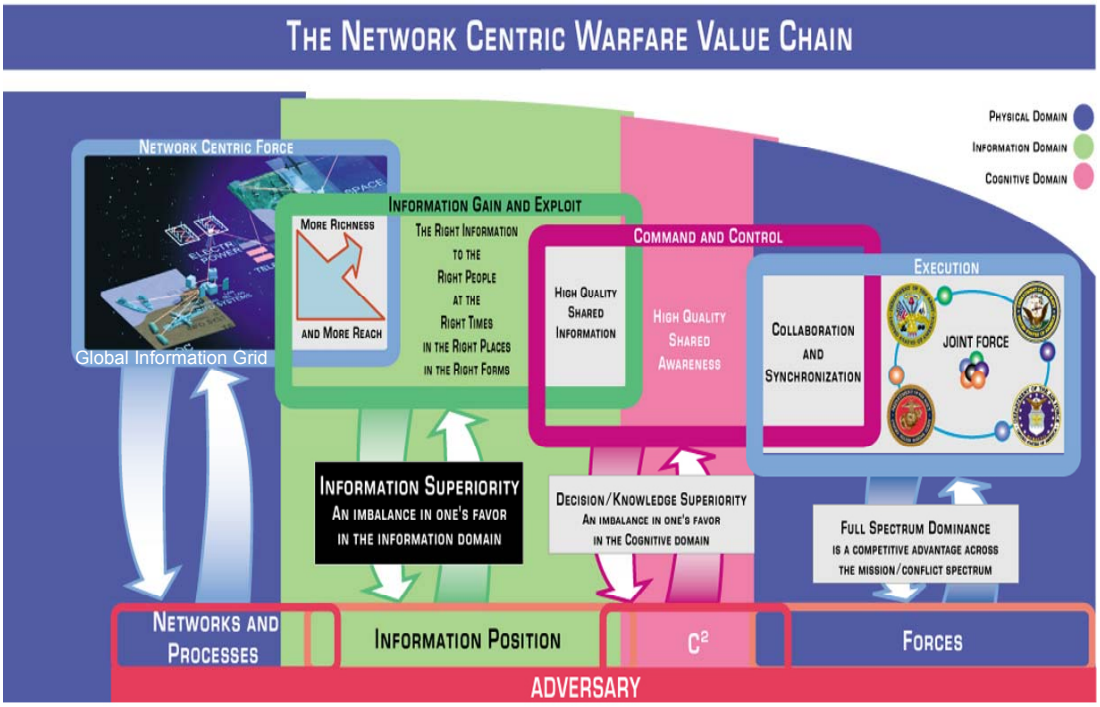


Figure 8-1. The NCW Value Chain

The second objective, that of measuring our progress toward a network-centric force, can be ascertained either directly or indirectly—directly, by measuring the ability of the force to conduct these types of operation, or indirectly, by measuring key capabilities associated with the conduct of network-centric operations including the ability to share information, collaborate, develop SSA, and synchronize effects over the range of "assigned" missions.

Section 934 of Public Law 106-398 calls for, among other things, "the methodology being used to measure progress toward stated goals." DoD's NCW-related goals are articulated in the Department's initial response to the Congress (7 March 2001) as follows.

> *The Department is fully committed to creating a 21st Century military by taking advantage of Information Age concepts and technologies, particularly new "business models" and information technologies. IT provided the building blocks for the Internet, radically restructured the economics of information, and enabled new ways of doing business that have created a "new economy." These same dynamics can help the Department transform its primarily platform-centric force to a network-centric force—a force with the capability to create and leverage an information advantage and dramatically increase combat power.*

Accordingly, this report focuses on presenting a methodology for satisfying the second measurement objective. (A detailed treatment of a methodology and set of metrics to satisfy the first objective can be found in *Understanding Information Age Warfare.)*[79]

8.1.2 Measuring DoD Progress Toward a Network-Centric Force

As indicated earlier, progress toward the Department's goal of achieving a network-centric force can be measured directly or indirectly. DoD will employ both approaches because they are complementary, each providing useful information.

The direct approach provides, for any given mission or set of nested missions, an assessment of the Department's ability to create and leverage an information advantage. This can be thought of as measuring the "state of the practice" and is illustrated in the example cited in the second part of this section. But only measuring the state of the practice will not provide an accurate picture of where DoD is on the road to a network-centric capability.

To complete the picture, a measure of the status of network-centric capabilities under development (a direct measure of future capabilities), a measure of network-centric potential (an indirect measure), and two maturity scales are needed. Taken together, these measures will provide the information necessary to judge both relative and absolute progress.

The status of network-centric capabilities can be measured by identifying where the capability is in the process of mission capability package co-evolution (see Figure 8-2). This, in turn, will provide a measure of the degree of risk associated with bringing the capability to fruition and an estimate of the time required to have a fielded capability.

---

79 Alberts, Garstka, Hayes, and Signori, *Understanding Information Age Warfare*, CCRP Publication Series, Washington, D.C., Available Summer/Fall 2001. http://www.dodccrp.org/publicat.htm

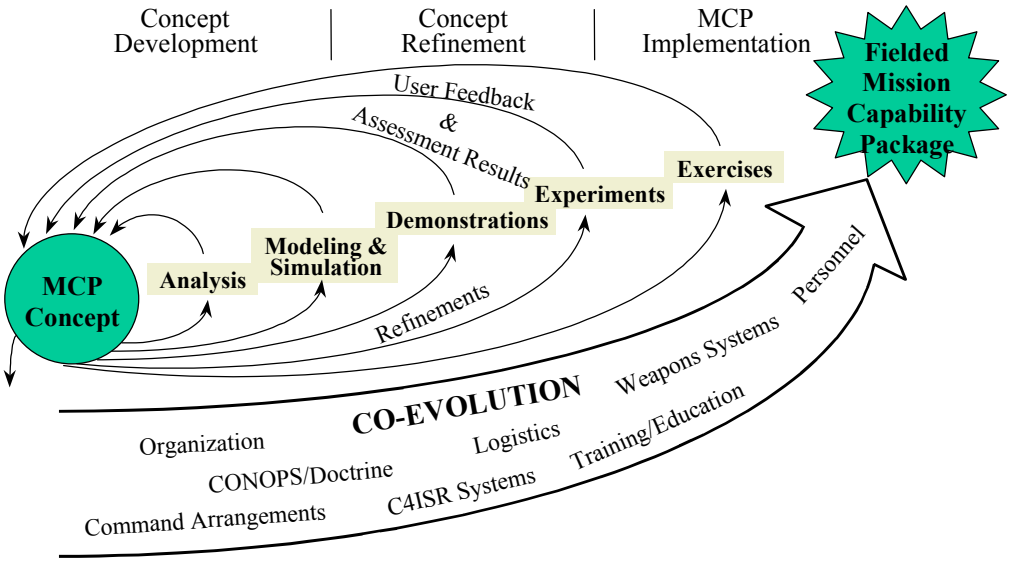


Figure 8-2. MCP Process

A measure of network-centric potential can be constructed around the enablers of Network Centric Warfare—the force's connectivity and interoperability. The extent to which these attributes are achieved is directly related to the *opportunity* to conduct Network Centric Operations, which, in turn, is directly related to the ability to create and leverage an advantage in the Information Domain and translate it into combat power in the case of war or into mission effectiveness in the case of operations other than war. Thus, measures of connectivity and interoperability are indicants of network-centric *potential*. Network-centric potential is a useful measure that serves to set an upper bound for the degree to which a force can conduct Network Centric Operations.

An initial formulation of a measure of network-centric potential that assumes that connectivity and interoperability go together (since being connected without the ability to effectively exchange information is meaningless) is a ratio of connected entities to total entities. A more refined measure is currently under development: one that takes into consideration the fact that not everyone has the same need to interact with everyone.[80]

---

80 See discussion of the value of networks in Appendix A of *Network Centric Warfare: Developing and Leveraging Information Superiority,* 2nd Edition (Revised), CCRP Publication Series, 1999.

8.1.3 Maturity Scales for Network Centric Operations

The ability to conduct Network Centric Operations like, for example, the ability to play soccer, can vary from barely being able to execute the basics to a very sophisticated, professional-level mastery of the concepts and techniques. Therefore, it is important to be able to distinguish among different levels of maturity of the application of Network Centric Warfare theory. Unlike soccer, where all teams consist of eleven players, network-centric applications can vary greatly in size and complexity, from single service squads at the tactical level to theatre-level Joint forces to coalition operations. Hence, two scales are needed: the first, a scale to measure the level of maturity of a particular NCW application; the second, to measure the scope and complexity of the application that achieves selected levels of maturity.

8.1.3.1 Network Centric Operations Maturity Model

Figure 8-3 depicts a five-level maturity model for Network Centric Operations. This model is an initial formulation of a micro-level metric that compares the basic features of an application (state of the practice) against the theory (state of the art).

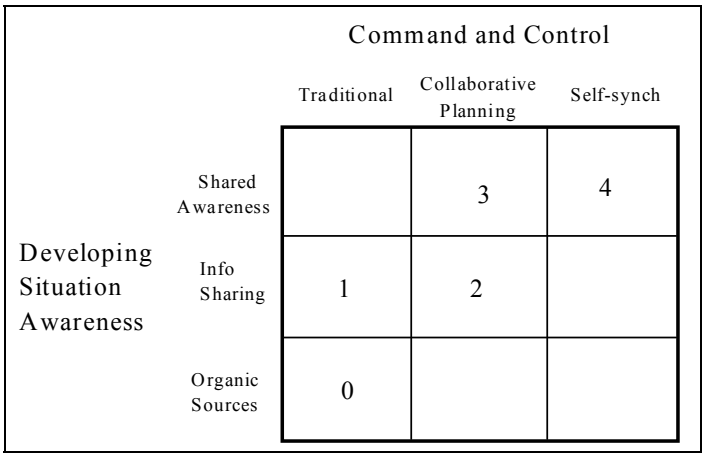


Figure 8-3. NCW Levels of Application Maturity

Each of the values for the maturity of a network-centric warfighting capability is defined by considering these two aspects of network-centric behavior. The first, the process of developing SSA, is meant to be a reflection of the degree to which information and awareness are shared. The second, the nature of command and control, is meant as a surrogate for how SSA is leveraged. Platform-centric operations anchor the Network Centric Warfare Value at Zero. At the other end of this "scale" (value Four) are "mature" Network Centric Operations that involve widespread information sharing, the development of a fully

integrated common operational picture (COP) that promotes SSA, collaborative planning processes, and a self-synchronizing approach to command and control.

Moving from Value Zero (platform-centric operations) to NCW maturity Value One involves the ability to share information. Information sharing is assumed to be associated with improved awareness. Moving from Value One to Value Two involves the addition of some form of collaborative planning among the participants. Movement from Value Two to Value Three involves richer collaboration, involving more actors and integrating more aspects of the operation. In many cases, there is less communication among the participants because of the SSA achieved (though early in the process of learning to collaborate, there may be more, and cases have been reported where communication stays the same, but has richer content). Movement from Value Three to Value Four requires a Mission Capability Package that allows integration across doctrine, organization, training, material, and other aspects of the force and its supporting systems that permit self-synchronization.

The ability to conduct Network Centric Operations can vary widely depending on the capabilities of the forces, the command and control systems that support them, and the command arrangements. A useful analogy for describing these concepts is provided by soccer. Soccer has few rules and few opportunities to restart the play on favorable terms. Each player must be aware of the field, who has control of the ball and where it is on the field, the capabilities and positions of the other players (friendly and adversary), and the dynamic interactions among those factors. Young players are taught to play specific roles and to react to "standard" situations. More experienced players are given both more freedom and more responsibilities—for example, defenders are taught to recognize opportunities to slip forward into the attack and create numerical and positional advantages for their team. At the highest level of soccer the play is fluid, with constantly changing shapes for both the attack and the defense. Their ability to read and react to these dynamics, with minimal verbal communication (calling for the ball attracts the attention of the defense), often determines match outcomes.

Of course, NCW concepts are much more complex than soccer, which has only 11 players on a side. Network Centric Warfare situations can vary greatly in size and complexity, from single service squads at the tactical level to theater-level Joint forces and coalition operations. The examples of NCW concepts and capabilities described in this chapter vary in scope and complexity from tactical air-to-air engagements (1 vs. 1 to 8 vs. 16) to multi-brigade ground maneuvers with 7000 plus soldiers opposed by an active opposing force (OPFOR). In addition, the degree to which the various elements of the force have been networked varies considerably, as well as degree to which information sharing and SSA were achieved. In addition, the maturity of the TTPs employed by the forces varied from very few changes in TTPs to new TTPs that effectively leverage the power of the network.

The Maturity matrix combined with the scope and scale of network-centric applications will allow us to interpret these examples and measure progress toward a force with network-centric warfighting capabilities.

8.1.4 Assessing Progress

To determine their NCW maturity level, we will be able to construct a picture of where the force is, and where we expect it to be in the future, by assessing a range of DoD missions as they are conducted, or as they are planned to be conducted at various points in the future. Furthermore, expressing the Department's NCW goals in terms of reaching selected levels of maturity for selected missions by certain dates will provide us with a clear set of targets or milestones against which progress can be measured. For example, one could consider as a DoD goal, the achievement, by 2012, of:

- A maturity level of Value Two for the entire force
- A maturity level of Value Three for selected core missions
- A maturity level of Value Four for a vanguard force.

We will need to begin by developing an "as is" assessment to serve as a baseline from which progress can be measured. Given that NCW is most easily understood and measured in a mission context, it will be challenging to develop a "roll up" from individual mission assessments to achieve a single measure for the whole of DoD. At this point, the focus should be on ascertaining where we are with respect to key missions.

Determining specific NCW maturity targets over time for DoD missions is not a trivial task. First, mission priorities will need to be determined based upon the results of the on-going review of defense strategy. Second, the relative values of our ability to conduct various missions at selected levels of NCW-maturity are interrelated because of synergistic effects. Third, these values are a function of the threat. Fourth, the time required to co-evolve and implement a network-centric mission capability package that operates at a given level of maturity for a given mission will vary as a function of the degree of technological challenge involved and the nature of the procurements or organizational and doctrinal changes required. Hence, considerable thought and analysis will be required to map the defense strategy that is developed into a set of mission maturity targets.

Given that this will take time, DoD proposes to begin its assessment of progress by looking at leading and trailing indicators of maturity; in other words, the number of missions that have achieved or will achieve each level of maturity at a given point in time. A nominal target associated with *Joint Vision 2020* involves reaching Value Four for all missions by that time. Actual targets will need to be developed for a set of critical DoD missions based upon programmed capabilities and the results of Joint and Service experimentation.

8.2 Evidence of NCW Impacts

8.2.1 Growing Body of Evidence

There is a growing body of evidence that provides an existence proof for the validity of each of the different classes of NCW hypotheses (delineated in Section 3.2.8.).

- Hypotheses of the first class deal with the relationships among degree of networking, degree of information sharing, and improved SSA.
- Hypotheses in the second class include those that involve the relationship between SSA and synchronization. For example, the effect of different degrees of SSA and collaboration on synchronization.
- The third class of hypotheses involves the link between collaboration or synchronization and mission effectiveness.

The most compelling evidence identified to date exists at the tactical level in a broad range of mission areas. This evidence has been assembled from a variety of Service and combined experimentation and operational demonstrations, as well as high intensity, tactical conflict situations. Examples were identified that supported the relationship between:

- Improved *networking* capabilities and increased *information sharing*
- Increased *information sharing* and increased *shared situational awareness*
- Increased *shared situational awareness* and improved *collaboration* and *synchronization*
- Increased mission effectiveness as result of the presence of one or more of these factors.

The strongest evidence uncovered to date exists in the following mission areas: air-to-air, maneuver, CSOF, TAMD, and strike. In addition, experimental findings have highlighted the benefits of distributed C2 and split-based operations. Figure 8-4 provides a framework for organizing the evidence. This evidence clearly demonstrates how NCW Concepts are enabling the *Joint Vision 2020* concepts of Dominant Maneuver, Precision Engagement, and Full Dimensional Protection.

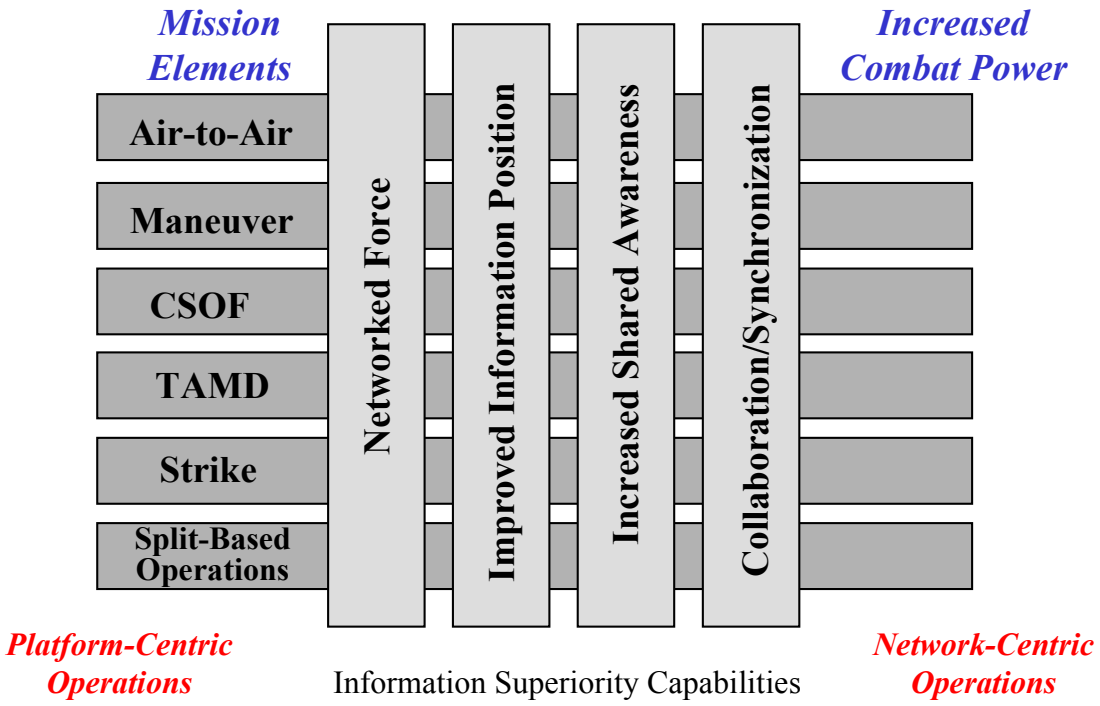


Figure 8-4. Framework for Emerging NCW Evidence

8.2.1.1 Air-to-Air Mission: Offensive and Defensive Counter

Compelling evidence exists in the air-to-air mission area for the NCW linkage hypotheses. In this high-priority mission area, the networking of sensors and shooters with data links, such as Link-16, enables a force to operate in the network-centric region of the information domain. The improved information position that can be achieved with networking is portrayed in Figure 8-5.

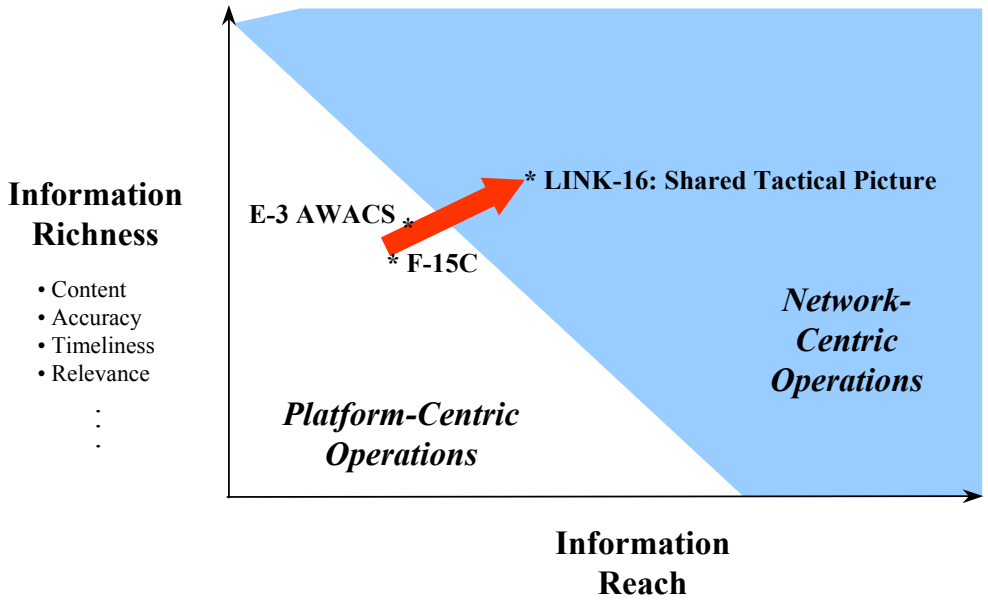


Figure 8-5. Air-to-Air: Improved Information Position

The tactical foundation for the air-to-air mission consists of Basic Flight Maneuver (BFM) Tactics.[81] These tactics call for a pilot to first observe an adversary with onboard sensors or the naked eye. Then the pilot predicts a course of maneuver for the enemy based on an assessment of the adversary's energy state, knowledge of the enemy's tactics, aircraft, and relative advantage in position. Next, the pilot assesses a maneuver needed for himself in order to defeat an adversary's or counter an adversary's defensive move while on the offensive. Finally, a maneuver is accomplished with great speed, which is designed to be unpredictable. This cycle is repeated as required through the engagement. If a pilot is capable of maneuvering with enough quickness that an adversary cannot react with appropriate counter-maneuver, then he or she will be decisive. The tactics described above are referred to as OPAM, for Observe, Predict, Assess, and Maneuver (a rephrasing of the OODA loop, from which they are derived).

Salient aspects of the tactics described above can be represented graphically, as shown in Figure 8-6, employing the domain approach discussed previously in Section 3. This

---

81 *Air Force Tactics, Techniques, and Procedures (AFTTP) 3-3-4: Combat Aircraft Fundamentals-F-15.* The AFTTP 3-3 series publications are the primary aircraft fundamental reference document for the USAF. This series provides a comprehensive, single-source document containing fundamental employment procedures and techniques necessary to accomplish various missions.

representation of two coupled OODA loops can represent either two pilots or pilot and controller sharing information via voice traffic. Controllers are usually located on C2 aircraft such as an E-3 AWACS aircraft (or in typical naval operations, an E-2 Hawkeye), which carry a broad area sensor that forms the basis for the information position that is available to controllers for observing and orienting.

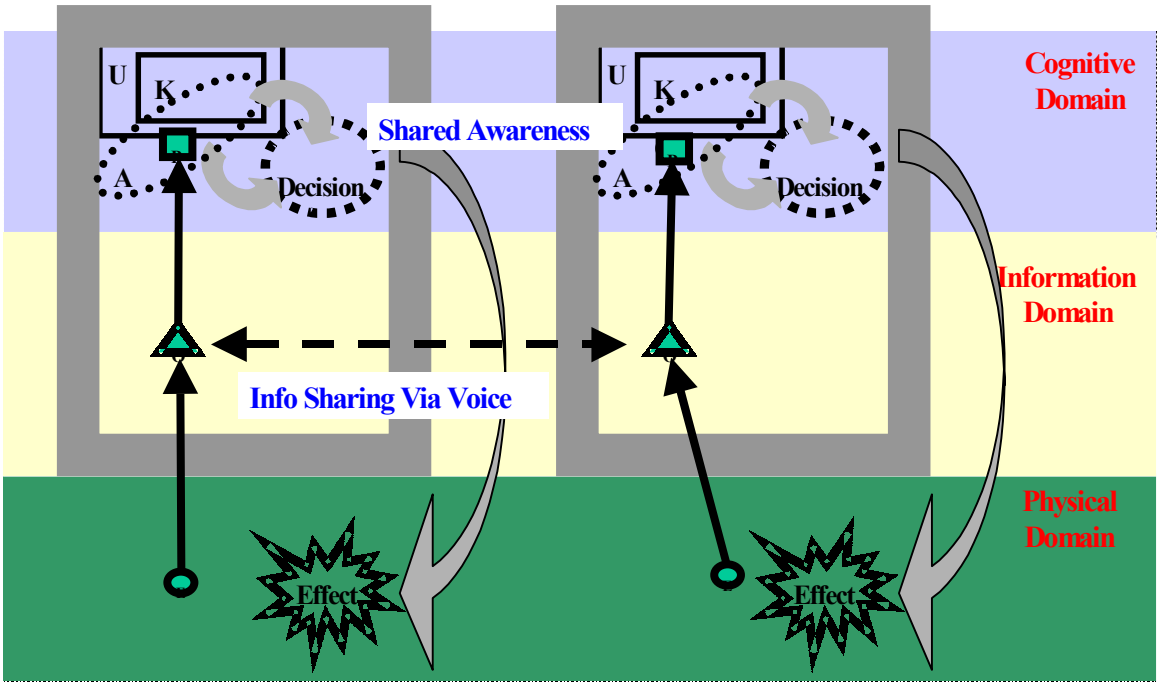


Figure 8-6. Coupled OODA Loops: Voice Only

Consider the tactical situation in the 4 vs. 4 engagement portrayed in Figure 8-7. A representative platform-centric information position that is available to a fighter pilot via heads-up display is portrayed on the left side of Figure 8-8. In this operational situation, the lead aircraft in Blue's defensive formation can only see those Red aircraft in a very narrow field of view directly to its front—the zone covered by its onboard radar. Consequently, when orienting and trying to establish the general orientation of attacking and defending aircraft, the pilot must combine his organic information position with information communicated by voice from other pilots or controllers. His orientation is facilitated by knowledge of Blue and potentially Red TTPs, as well as preflight mission briefs.

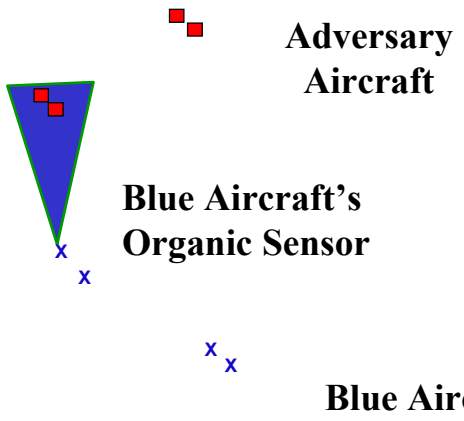
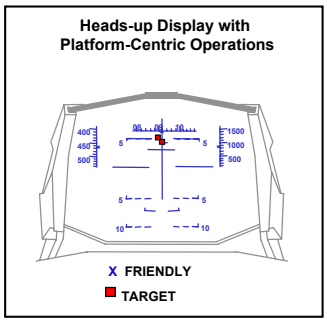


Figure 8-7. Air-to-Air: Tactical Situation: 4 vs. 4

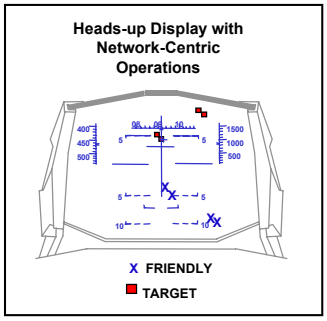
Before tactical closure, controllers are cycling through the OODA process and sharing information with pilots via voice as they vector fighter aircraft to attack positions and attempt to put Blue pilots in the most advantageous attack positions while simultaneously attempting to control the actions of all the defending aircraft to ensure that a sound defensive posture is maintained. If C2 platforms are not available, direction may come from a surface vessel or ground control radar station. If this control function is not performed, mission performance may be degraded for one or more of the following reasons:

- Attacking aircraft may slip through the defensive screen because the organic sensors of the defending aircraft themselves are short range and local, leaving gaps in coverage. This can result in "leakers" or attack aircraft that penetrate the air defenses.
- To compensate for the lack of control, more aircraft may have to be put on station to detect and intercept attacking aircraft, resulting in lower operational tempo and less efficient use of assets.
- Speed of tactical decision making may be slower with respect to the pace of the air-to-air battle because information about attacking aircraft will take longer to generate and deliver to those who need it.
- Loss ratios may be less favorable because interceptions occur under less favorable conditions.

Voice vs. Voice Plus Data Links



Warfighter View which results from sharing info via voice only communications



Warfighter View which results from sharing info via voice and data communications

Figure 8-8. Voice vs. Voice Plus Data Links

In contrast to platform-centric operations, which are dominated by voice traffic, network-centric operations are dominated by data traffic augmented by voice. The networking of sensors and shooters with data links such as Link-16 creates a robustly networked force that has the ability to share information among all platforms and create significantly improved information positions vis-à-vis platform-centric operations.

The source of the increase in combat power that can result from the ability to share digital information can be understood by once again employing the domain approach. Figure 8-9 portrays two coupled OODAs that can correspond to two pilots, or a pilot and a controller. It is clear from this diagram that the OODA loops of these two individuals are tightly coupled since the data link allows the pilots to share crucial data and information on a continuing basis. If the sensors of one aircraft detect a target (observe), then this track information can be shared along with position information of both Blue aircraft. The result of information sharing is a dramatically improved information position, which is portrayed in Figure 8-10.

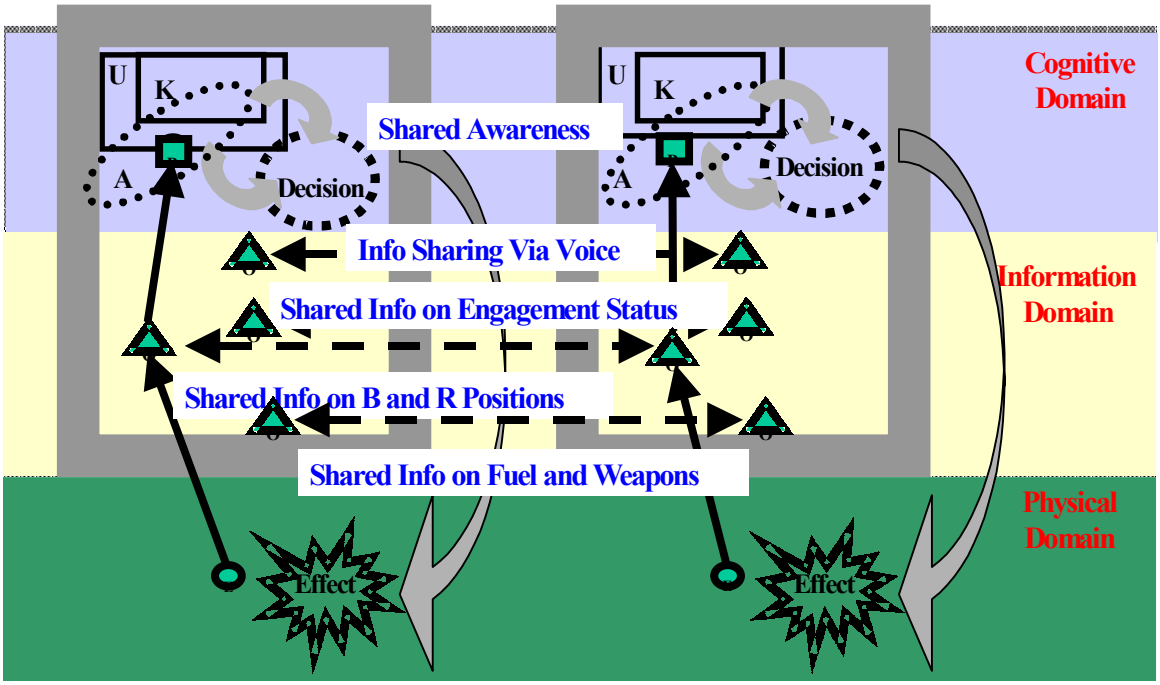


Figure 8-9. Coupled OODA Loops: Voice Plus Data

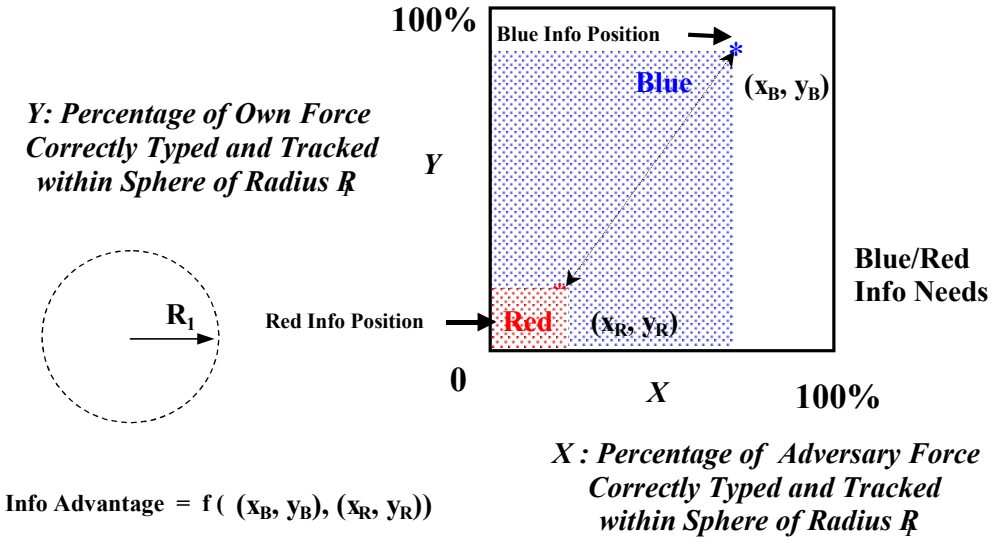


Figure 8-10. Air-to-Air: Relative Information Advantage

This dramatically improved information position allows Blue force pilots and controllers to orient on the same position location information. Sharing additional information, such as weapons loading and fuel status, as well as the status of the current engagement, results in the creation of a significant information advantage. This information advantage enables pilots and controllers to more rapidly orient themselves by using common information. This has several observable effects. Most obviously, the information directly available to every pilot to orient with is richer. For example, the heads-up display on the right side of Figure 8-11 illustrates the fact that the lead Blue pilot now has a richer view of the Red aircraft (he sees all four of them, not just the two in front). As a result, during the orientation process, the pilot can more effectively locate himself, his wingman, and a trail flight of two other Blue interceptors to form a mental three-dimensional picture. This picture can be merged with other engagement information, prior knowledge (e.g., the capabilities of each type of aircraft involved in the action), and understanding (from mission briefings, etc.) to create improved SSA.

This improved SSA enables two or more pilots (and others on the network) to form similar mental patterns of the engagement that aid them in tactical decision making (decide) and influences Blue pilot actions (act) in several important ways. First, the pilots themselves can make decisions that are mutually reinforcing about how to approach the Red aircraft and gain advantageous positions for the interception and battle that follows. Second, they can see one another's actions. As a result, the trail flight can act independently and intelligently to support the actions of the lead flight. Perhaps equally important, there is less talk on the radio. Rather than having to vector aircraft and describe what cannot be seen via voice, the supporting platforms are largely just feeding basic information over Link-16. This reduces the load on the controllers, and very importantly, reduces the cognitive load on the pilots of the interceptors. Less voice traffic is needed, which means pilots can concentrate on the battlespace and their actions.

The overall effect is one that enables the pilots to self-synchronize their efforts, though they also have the ability to talk with one another and the controllers. At a minimum, these pilots have the capacity to increase their awareness of the battlespace and, in theory, to greatly improve their SSA since they all see the additional information.

The operational benefit of employing F15-C aircraft equipped with Link-16 was explored in an Operational Special Project (OSP) undertaken by the U.S. Air Force during the mid-1990s. The JTIDS OSP compared mission effectiveness for voice only versus voice plus Link-16 in a wide range of tactical situations (1 vs. 1 to 8 vs. 16) in day and night operations. Data was collected during more than 12,000 sorties and 19,000 flying hours. In daylight operations, the average kill ratio increased from 3.10:1 to 8.11:1, a 2.61 fold improvement. During night operations the average kill ratio increased from 3.62:1 to 9.40:1,

a 2.59 fold improvement.[82] For both day and night operations, this translates to an increase of over 150 percent, a major gain against any standard. While the actual increase in awareness and SSA were not measured, the observables reported (less use of tactical radios, supporting maneuvers without discussion, etc.) support the conclusion that there were significant changes in these attributes of the cognitive domain.

At the qualitative level, the JTIDS OSP Report to Congress summarized the impact of data links to augment voice communications in air-to-air combat in this way:

- SSA drastically increased with data links due to continual positional awareness of friendly elements and adversaries' elements, which reduced the need for radio communications.
- Each flight member was able to see the disposition of flight members, regardless of their separation.
- This SSA made split tactics easier, led to greater flight effectiveness and afforded quicker rejoins when desired.
- The mutual support enhancements proved even more significant against a non-equipped adversary in night and weather conditions since the adversary formation either had to stay together or substantially degrade mutual support.
- When voice was used, the pilots often referred to a common picture making the voice more meaningful.
- In testing with the data link, a perfect sortie was routine with four (and two) ship flights. This had strong positive implications concerning first pass kill results, fighting outnumbered, survivability, and cost effectiveness employing expensive aircraft/missiles. When an F-15 inadvertently locked onto another flight member, the error was graphically displayed (by the lock line going to the friendly fighter), and the pilot lost little time in determining the error and avoiding possible fratricide.[83]

The complex relationships among information sharing, improved information position, SSA, increased OPTEMPO, and an increased kill ratio are portrayed in Figure 8-11. Embedded in this relationship are the new TTPs that were developed by the pilots that participated in the JTIDS OSP to dramatically increase combat power by taking advantage of improved SSA.

---

82 Mission Area Director for Information Dominance, Office of the Secretary of the Air Force for Acquisition, *JTIDS Operational Special Project (OSP) Report to Congress*, December 1997, Headquarters U.S. Air Force, Washington, D.C.

83 *Op. cit.*

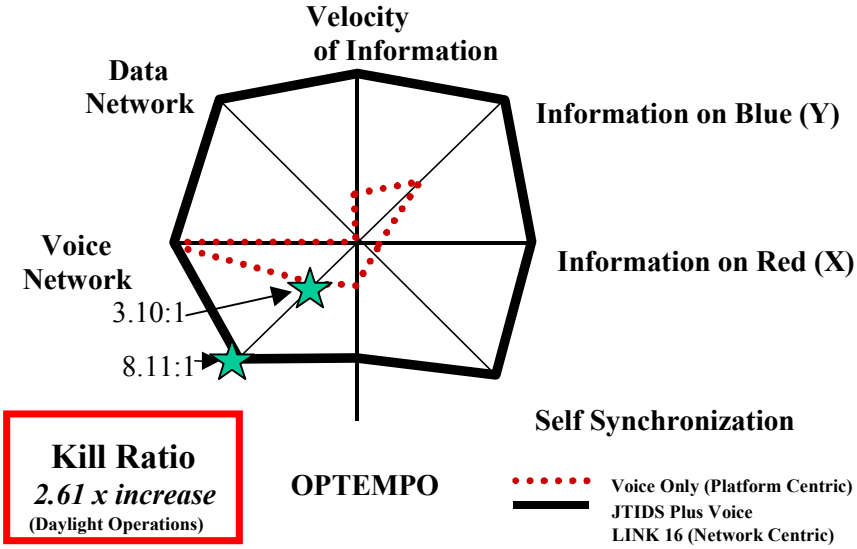


Figure 8-11. Air-to-Air

8.2.1.2 Maneuver

The evidence from exercise, experiments, and analyses that have dealt explicitly with maneuver demonstrates both the challenges and payoffs of Network Centric Operations. During the early phases of experimentation, U.S. Army units were not able to field a high performance tactical network or develop and employ mature TTPs that could enable them to leverage high quality SSA. However, the recently completed Division Capstone Exercise-Phase I showcased the increased combat power that maneuver forces employing more mature NCW capabilities can achieve. The discussion that follows clearly highlights the progress the Army has made in understanding both the challenges and the opportunities faced by maneuver forces in leveraging the power of the network.

The U.S. Army's Advanced Warfighting Experiments (AWEs) have been key to putting digital technologies on the battlefield. These experiments, as well as experiments conducted by Army Battle Laboratories and the Army Research and Development Centers, have provided the Army with a means for exploring and gaining insight into the feasibility of NCW technologies and the related doctrinal and organizational implications. AWEs have provided valuable lessons learned as well as some of the first analytical underpinnings to support the theory of NCW as a combat multiplier.

The U.S. Army conducts a variety of activities under the umbrella of AWEs. They conduct staged engagements at the brigade level with experimental systems, capabilities, and concepts (e.g., Task Force XXI). They also conduct command post exercises (CPXs) with real staffs and real C2 systems and simulated forces (e.g. division AWE). In addition, they

also conduct extensive analyses and simulations (e.g., pre- and post-experimentation analysis as they did before and after the Task Force XXI AWE). The results of these different kinds of experiments and exercises are not strictly comparable, but a careful examination of their findings provides support to the hypotheses discussed earlier.

The U.S. Army's first AWE, the Desert Hammer VI AWE, was conducted in April of 1994. The purpose of this initial AWE was to examine the impacts of a Battalion Task Force possessing digital communications across each Battlefield Operating System (BOS). The results of this AWE, and several subsequent AWEs, when viewed in hindsight, highlight the significant progress the U.S. Army has made in developing and maturing NCW capabilities. The anticipated benefits of digitization and networking, increased lethality, survivability, and OPTEMPO, were slow to materialize in initial experiments. A number of factors were identified that influenced the divergence between potential performance and observed performance. These factors formed the basis for insights and lessons learned that paved the way for future success. These insights included:

- The importance of a high performance communications network
- The need for adequate training with new digital capabilities
- The importance of unit collective training time with digital capabilities
- The importance of limiting the number of capabilities introduced prior to a given experiment
- The need to screen digital capabilities for maturity[84]

The Task Force XXI AWE was conducted at the National Training Center (NTC), Fort Irwin, California, in March of 1997. Although the results from the Task Force XXI AWE were less than conclusive, the results of the Division AWE conducted at Fort Hood in 1997, subsequent training operations with digitized forces after the Task Force XXI AWE, the results of Allied exercises, and Phase I of the Division Capstone Exercise conducted in April of 2001 have highlighted that significant gains in combat power can be achieved with Network Centric Operations.

8.2.1.2.1 Task Force XXI AWE

The objective of Task Force XXI was to explore whether a digitized force, with properly integrated doctrine and technologies, would attain increases in lethality, OPTEMPO, and survivability. Task Force XXI unveiled the first effort to integrate tactical radios with commercially based routers, thus providing a networking capability at lower echelons to

---

[84] Robert C. Holcomb, "Some Lessons Learned While Digitizing the Battlefield," *Proceedings of the Battlefield Systems International Conference*, London, 1998.

rapidly share information and enable SSA. The Army demonstrated technologies that enabled information sharing down to the individual platform level, improved C2, and for the first time, showed that time-sensitive information could be shared "horizontally" rather than having to follow the traditional "chain of command" path.

Task Force XXI also demonstrated the power of networking multiple sensors and rapidly turning sensor data into useful information. The full range of digital weather support was delivered from garrison to the field through satellite communications links. The division Analytical Control Element received battlefield information from maneuver unit spot reports and various Army and Joint sensor platforms. Analysts used the All-Source Analysis System to correlate and fuse this information into a coherent, timely enemy picture that was used to update the COP, not only at the TOC, but also down to the individual digitized weapons platform. For the first time, soldiers in the tank could see what was happening around them.

The Experimental Force (EXFOR) for the Task Force XXI AXE consisted of an armor battalion, a mechanized infantry battalion, a light infantry battalion, and various support units. Within the EXFOR's two heavy maneuver battalions there were 873 digitized and networked platforms, consisting of M1A1 tanks and M2A2 Bradley fighting vehicles equipped with appliques. The EXFOR's light infantry battalion contained 186 dismounted soldier systems, and was equipped with the Javelin anti-tank missile system. A battalion of M109A6 Paladins provided field artillery support, and the Aviation Task Force consisted of eight AH-4A Apaches, two AH-64D Apache Longbows, and eight OH-58 Kiowa Warriors.[85]

The EXFOR prepared for the AWE at Fort Hood by conducting platoon, company, and battalion collective training, as well as a culminating brigade exercise that took place in December of 1996. During this training, a significant amount of time was dedicated to the mastery of the hardware and software that digitized and networked the platforms. An undesirable consequence of this focus on new hardware and software was a decrease in the time available for unit training.[86]

During the AWE, the EXFOR conducted a total of eight missions against the opposing OPFOR at the NTC. These missions included movement to contact, deliberate attack, and hasty defense. Of the eight missions, three were similar to missions conducted by non-digitized forces during normal training rotations, and five were characterized as unique missions designed for the digital force. The size of EXFOR was relatively constant for all eight missions and tactics employed by the EXFOR did not vary significantly across the

---

85 *Op. cit.*

86 *Op. cit.*

missions. However, the EXFOR was dispersed to a greater degree than normal during the five unique missions.[87]

The performance of the EXFOR's network during the AWE was limited by hardware and software problems, which resulted in an information position that was significantly degraded from what could have been achieved with a higher performing network. For example, the message completion rate for digital message traffic was under 30 percent. The net result was that SSA did not increase to the degree achieved in the air-to-air mission in the JTIDS OSP.

However, it is interesting to note that the most significant Blue victory, which took place in the final battle, was directly attributable to the excellent performance of UAVs linked to the attack helicopters during the battle. This gave the Blue Force a local information advantage that they were able to effectively exploit. The other seven battles resulted in Red victories or in tactical draws. These results were similar to outcomes observed in most rotations at the NTC. However, one of the key observations made by the EXFOR was the value of increased Blue SSA that resulted from the use of the Tactical Internet, with about 75% of platoons visible at the battalion command post. This increased positional location capability was used by combat service support units to find the vehicles they needed to rearm and refuel, as well as to mark and avoid minefields and chemical strike areas. In addition, shared positional information helped artillery units see with some certainty the location of the friendly forces, which assisted them in clearing fires.[88]

8.2.1.2.2 U.S. Army Division AWE

The U.S. Army conducted a Division AWE at Fort Hood in 1997 with the objective of determining the warfighting effectiveness of a digitized division-sized force. This AWE was conducted over a period of nine days with elements of an Infantry division in the context of a Battle Command Training Program (BCTP) command post exercise. This exercise differed from previous exercises in that it was conducted largely through the use of the Corps Battle Simulation, a computer-assisted wargame. The focus of the exercise was the command and control of digitized forces. Consequently, all units smaller than command posts were simulated, and the division and brigade command posts were deployed in the garrison area of Fort Hood, and connected via radio and landline links.[89]

The Division AWE wide area network architecture employed at Fort Hood was up to 48 times faster than the wide area network developed for Task Force XXI. Similarly, local area

---

87 *Op. cit.*

88 *Op. cit.*

89 *Op. cit.*

networks inside each Division AWE command post were markedly better than those used in Task Force XXI. This augmented network supported additional applications, such as video teleconferencing and higher volume, faster data transfers. The network also supported previously-used network applications, such as exchanging formatted messages, client-server operations, and web-based operations.

As in Task Force XXI, there were striking examples during the Division AWE of commanders and staff members perceiving the battlespace with greater clarity than ever before and then acting on that perception with great speed. This time, digitization of the battlefield led to the Experimental Force achieving and sustaining SSA and information dominance over the world-class Opposing Force. In turn, this permitted the Experimental Force to conduct distributed, non-contiguous operations over an extended battlefield. As the enemy attempted to maneuver, the Experimental Force was able to locate and track the enemy's most critical forces and bring massed, destructive fires on them. The subsequent close fight allowed cohesive, mobile Experimental Force brigade combat teams (BCTs) to engage and defeat the disrupted and attrited Opposing Force units.

Despite numerous problems along the lines of those discussed previously (software interoperability problems, need for adequate training on new C2 systems), the following improvements, relative to previous warfighters (CPXs), were observed:

- Operational tempo: division-level plan development time was reduced from 72 hours to 12 hours, making a six-fold increase in OPTEMPO possible.
- Speed of calls for fire: time required for processing calls for fire was reduced from 3 minutes to 0.5 minutes, again a six-fold increase in the potential for bringing fire assets to bear, with increased potential lethality as well as potential for saving friendly lives and improving the pace of battle or friendly OPTEMPO.
- Planning time for deliberate attacks at the company level was cut in half, from 40 to 20 minutes. Substantial improvements in OPTEMPO and the ability to operate within the adversary's OODA loop were therefore demonstrated.[90]

8.2.1.2.3 United Kingdom (UK) Exercise Big Picture 1

In February of 1997, UK Exercise Big Picture 1 (BP1) demonstrated the potential combat power that can be generated with a networked ground force. BP1 was conducted at Grafenwoehr Simulation Center with a UK squadron/company level unit in a simulated environment that overcame many of the observed limitations of the tactical Internet. During the exercise, 18 tank simulators and 17 infantry fighting vehicle simulators were hardwired

---

90 BG William L. Bond, USA, *Army Digitization Overview*, Briefing to Dr. Jacques Gansler, USD (A&T), at the Pentagon, Washington, D.C., on May 20, 1998.

in an attempt to replicate a level of network performance that could be achieved theoretically with a high performance tactical Internet. Each simulated digitized platform contained full color map displays and a touch screen. In addition, a robust experimental design methodology was employed to remove the effects of geography, level of training, and unit in the estimation of performance gains from digitization. These simulators were then manned, and various tactical missions were conducted. A key observation made by the UK soldiers who participated in the experiment was the tremendous value of increased SSA of Blue forces that was realized through digitization and networking. The following results were observed in comparison to similar simulations with non-digitized forces.[91]

- Survivability/Lethality: Blue force suffered up to 50% fewer losses as a proportion of the total kills inflicted in the attack mission.
- OPTEMPO: Mean time to complete the C2 phase of the attacks was 40% lower.

8.2.1.2.4 Observations From U.S. Army Training Exercises

Numerous training exercises conducted with digitized U.S. Army units have provided insight into the validity of individual components of the Network Centric Warfare hypotheses. As research and experimentation proceed, it is expected that these qualitative insights will be converted into quantifiable findings.

Value of Increased Shared Situational Awareness (SSA) at the Unit Level. Increased SSA, enabled by information sharing over the network, allows units at the platoon level to focus more of their mental efforts on fighting the enemy and less on keeping track of their location and the location of the rest of their unit. This increase in SSA has the potential, yet unmeasured, to result in increased survivability and lethality.[92]

Value of Increased SSA in Increasing OPTEMPO. Increases in SSA have allowed units at the platoon and company level to remain in tactical march formations longer, utilizing the speed of these formations to increase the operational tempo of battle. On several occasions, this increased operational tempo has allowed Blue forces to surprise opposition forces and gain a tactical advantage. Before, the increase in shared situational awareness enabled by information sharing, units had to move into attack formation earlier to avoid surprise contact with the enemy and to conserve combat power.[93]

---

91 Defense Evaluation and Research Agency, *Exercise Big Picture 1 Final Report*, October 1997.

92 *NCW—Emerging Lessons Learned from the First Digital Division*, Presentation by COL (Ret) Fred Stein at conference on "Network Centric Warfare: Missions, Needs, Opportunities, and Challenges, " Washington, D.C.; Oct 21-22, 1999.

93 *Op. cit.*

Value of Increased SSA in Maintaining Force Ratio. At the brigade and division level, increased shared situational awareness has allowed commanders to leave forces in contact longer with the enemy. Increased SSA of Blue and Red forces allows commanders to develop a better real time understanding of the status and disposition of their forces, of Red forces, and force ratios. This increased battlespace awareness gives them the confidence to allow units to stay in contact longer with the enemy, resulting in increased combat power.[94]

Value of Increased SSA in Reducing Risk. Both at Fort Hood and the National Training Center (NTC), units at the company and battalion level have reportedly been able to conduct more complex tactical maneuvers with less risk as a result of increased situation awareness enabled by the network. For example, the double-envelopment maneuver, during which the central part of a ground force retreats or stays in place while the flanks hold their ground or advance to gain superior position and then advance simultaneously to envelop, surround, and cut off an advancing enemy force, has proven easier to execute, with less risk. Similarly, passage of lines, in which a major new force passes through a blocking force to occupy a key position, has been executed more successfully at the NTC.[95]

Value of Increased SSA to Battle Command. Finally, networking the force has reportedly assisted a division commander by giving him the increased SSA needed to maneuver against an adversary. In this case, the commander was able to monitor an enemy column on his right that was maneuvering. Rather than being forced to deploy his forces and alter his scheme of maneuver to engage the force, he was able to monitor its progress as it moved into an area not vital to him. Knowing its location, he was able to first complete his primary mission by executing his original plan, then maneuver his forces to defeat the now-isolated enemy force.[96]

8.2.1.2.5 Division Capstone Exercise—Phase I

Phase I of the Division Capstone Exercise (DCX) was conducted from 11 March through 28 April of 2001, at Fort Irwin, California. The purpose of this DCX-I was to demonstrate and assess the 4th Infantry Division's mechanized and aviation brigades' ability to contribute decisively to III Corps' land campaign counteroffensive capability in the context of a Joint exercise. One of the principle goals of the DCX was the demonstration and assessment of the increased combat power enabled by multiple ongoing digitization and equipment modernization programs. The DCX Blue Force (BLUEFOR) was composed of

---

94 *Op. cit.*

95 *Op. cit.*

96 *Op. cit.*

approximately 7500 soldiers in two brigade combat teams (BCTs) consisting of elements of the 2nd and 4th Brigades of the 4th Infantry Division, F-16's and A-10s from the Arizona National Guard close-air-support, and Joint Surveillance Target Attack Radar System (JSTARS). The DCX Opposing Force (OPFOR) consisted of NTC OPFOR elements fighting with their traditional home field advantage.

The 2nd BCT comprised a "heavy" force of three battalions (three companies each) equipped with state-of-the-art M1A2-SEP Abrams tanks and M2A3 Bradley fighting vehicles. One of the battalions was composed of three tank companies; another two tank companies and one infantry fighting vehicle company; and the third, one tank company and two infantry fighting vehicle companies. Supporting the operations of the 2nd BCT were an M109A6 Paladin field artillery battalion, an engineer battalion, and a forward support battalion.[97] The 4th BCT consisted of a "battalion minus" (two companies) of AH-64D Longbow Apache attack helicopters, a battalion minus of UH-60 Blackhawk helicopters, two troops of OH-58D Kiowa Warrior reconnaissance helicopters, and an aviation support battalion.[98] The DCX also evaluated several new brigade organizational structures, including a brigade reconnaissance troop (BRT), three company battalions, forward support battalions, and organic engineer assets. [99]

Leveraging the dramatic increases in SSA enabled by the networking of the digitized force, the 4th Infantry Division's two BCTs were more agile, had greater precision, and were more adaptable in changing situations. Although official TRADOC findings from the DCX-I have not yet been released, an initial quick-look analysis highlighted the ability of the Blue Force (BLUEFOR) to significantly improve its warfighting effectiveness by creating and leveraging an information advantage.[100] Qualitative insights support key elements of the NCW hypothesis. In comparison with the Task Force XXI AWE, the BLUEFOR that participated in DCX-I appeared to have developed and mastered new TTP, which enabled it to leverage the power of the network to significantly increase its warfighting effectiveness.

Information sharing, enabled by the network, allowed the BLUEFOR to develop a superior information position and exploit this position to gain overmatching SSA. The

---

97 Scott R. Gourley, "Redefining War," *Military Information Technology,* Volume 5, Issue 5, June 2001, p. 22-23.

98 *Op. cit.*

99 *Op. cit.*

100 Frederick P. Stein, *Presentation on "DCX-Phase I" to Network Centric Warfare… Understanding the Operations and Systems of the Revolution in Military Affairs*, AFCEA Course 513, Washington, D.C., 1 June 2001.

BLUEFOR was able to leverage this SSA advantage to rapidly focus lethality with precision maneuver (M1A2-SEP Abrams, M2A3 Bradley, AH-64D Apache) and conduct successful, simultaneous, and decisive operations. The ability of the BLUEFOR to share information over the network and develop a common operational picture had dramatic impact across all echelons of command. A key theme was increased speed. Vignettes that illustrate the employment of NCW concepts are presented below.

Armor to Artillery horizontal information sharing, increased speed, improved OODA performance, distributed OODA. An M1A2-SEP tank identified an OPFOR armored personnel carrier (a BMP) during a company raid at a distance of 5 km. Since the BMP was beyond direct fire range, the tank used its far target location capability to precisely locate the target (OBSERVE) by lazing and selecting the call-for-fire template from the reports menu on the Force XXI Battle Command Brigade and Below (FBCB2). The tank commander then digitally relayed a "Call for Fire" to the company fire support team vehicle (FIST-V), and it relayed the call-for-fire to the direct support firing battery (ORIENT, DECIDE).

The initial fires achieved a firepower kill on the BMP and the following fire-for-effect resulted in a catastrophic kill (ACT).

This far target location capability gives the M1A2-SEP tank and the M2A3 Bradley an exceptional capability to call for accurate, lethal fires out to the limit of their ability to laze.

Factors contributing to reduced OPFOR SSA

Three key factors contribute to the BLUEFOR's ability to develop a SSA overmatch over the OPFOR. The BLUEFOR's rapid scheme of maneuver, combined with their ability to conduct bold maneuvers at night in difficult terrain, significantly reduced OPFOR's capability to develop SSA on the status and disposition of the BLUEFOR. The OPFOR stated that it was only able to develop a 70% solution of battalion task force areas rather than the normal 6-digit grid coordinate for vehicles that they had been able to develop during previous rotations. This situation was exacerbated by Blues' ability, in several instances, to attrit the OPFORs reconnaissance capabilities. During one operational situation, the BCT's UAV spotted an OPFOR division reconnaissance company moving south. The BCT's military intelligence company relayed this information via FM radio to a mechanized company in close proximity that was escorting a rearward movement of refugees. The mechanized company moved to and destroyed seven of the OPFOR's division reconnaissance vehicles.

Benefit of Multi-Echelon C2 (Collaborative OODA)

The shared operational picture enabled the Division Tactical Command Center to assist the 2nd BCT in performing C2 (Collaborative OODA). At one point during the BLUEFOR's maneuver, the C2 element manning the Division Tactical Command Center was able to use

the common operational picture to rapidly identify a situation where elements of a Battalion Combat Team (BCT) were out of position and provide guidance to reposition the BCT. In this specific situation, the 2nd BCT was in the execution phase of clearing CMF forces/movement to contact up to a Phase Line. One of the operators from the FSE observed that several tanks from the 2nd BCT had moved north of the Phase Line (the limit of advance for the 2ndBCT, with the exception of the BRT [Brigade Reconnaissance Troop]). This instance of rapid collaborative C2 enabled 2nd BCT's forces to relocate themselves to support the Commander's operational plan.

Shared Knowledge of Commander's Intent

Digitization and networking has enabled staffs to share information on commanders' intent to the lowest levels, resulting in the capability of the 4th Infantry Division (ID) to develop a shared knowledge of commander's intent (in the cognitive domain). During the initial movement of the 4th ID, the staff was able to understand the commander's intent to the lowest level. Specialists and privates monitoring the battle were able to understand the big picture. Enlisted soldiers could monitor the battlefield and develop a better understanding of what was happening on the battlefield.

Sensors (UAV, JSTARS) contributions to Increased SSA

The BLUEFOR's ability to employ organic sensors and exploit sensors such as JSTARS enabled commanders to visualize the enemy and terrain and to see and strike quickly before the enemy was prepared or when he did not expect to be attacked. Particularly lethal in the deep attack were the AH-64 D Longbow Apache helicopters teamed with UAVs to form hunter-killer teams. On several occasions, the commander was able use UAVs to identify OPFOR forces and then maneuver attack helicopters to engage and perform shaping operations before contact OPFOR engagement of BLUEFOR. In another operational situation, increased SSA of BLUEFOR enabled the assistant division commander for maneuver (ADC-M) to conduct interdicting fires with MLRS and F-16 close air support sorties. In the course of the air strikes, the pilots identified approximately forty-five vehicles in a ravine. The ADC-M then ordered additional strikes on these vehicles before releasing the sorties to 2nd BCT control.

Benefit of Improved SSA to Logistics and Support

Greater SSA played a key role in increasing the effectiveness of logistics and support units and creating a force multiplier. For example, the increased SSA available to logistics and support units improved their ability to find and fix broken and disabled platforms and increased velocity of repair. The net result was increased combat effectiveness of the 2nd BCT. An additional demonstrated benefit of total asset visibility and anticipatory logistics was the ability to employ modular and tailorable approaches that resulted in smaller logistics footprints and reduced lift requirements.

8.2.1.2.6 Operational Benefits

The anticipated operational benefits of digitization and networking for maneuver are portrayed in Figure 8-12. While the gains in information quality, information sharing, situational awareness, SSA, collaboration, and synchronization must be estimated, the data on planning speed, mission outcomes, calls for fire, and force lethality are consistent with the hypothesized patterns.

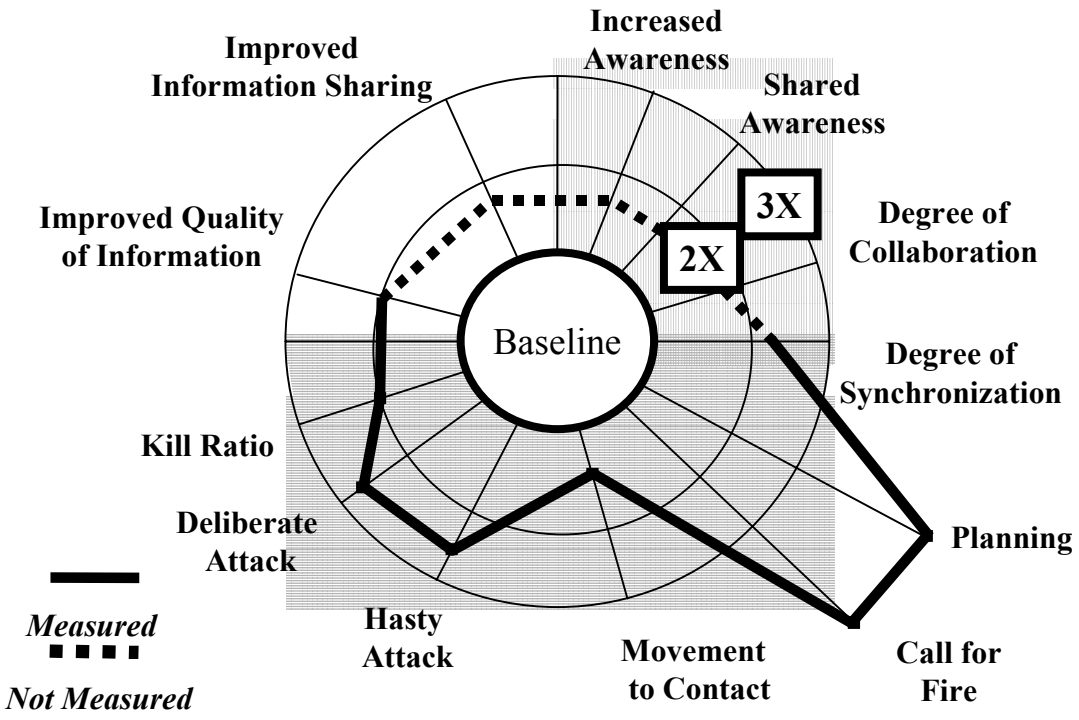


Figure 8-12. Maneuver

8.2.1.3 Counter Special Operation Forces Mission

One of the most significant examples of the power of Network Centric Operations to date occurred when FBE Delta was conducted by the U.S. Navy in conjunction with Combined Forces Command Korea. This command faces major warfighting challenges in three mission areas: Counter Fire, Counter Special Operations Force, and Theater Air and Missile Defense. Each of these missions was addressed in FBE-Delta, conducted in October 1998 in conjunction with Exercise Foal Eagle '98, an annual Joint and combined exercise sponsored by Combined Forces Command Korea.

In this experiment, the results with the greatest operational significance were generated in the CSOF mission area, where the seemingly intractable problem of countering hundreds of North Korean special operations boats (a CSOF mission) was dealt with on a timeline previously not thought possible.

In this experiment, elements of the Army's 2nd Infantry Division, AH-64 Apache Helicopter Squadrons from the 6th Combat Air Brigade, a range of Navy and Marine Corps units, and a Maritime Air Support Operations Center were networked via a wide area network to form a land-sea engagement network. Operating on this network were two command and control applications, the Automated Deep Operations Coordination System (ADOCS) and Land Attack Warfare System, a prototype software application derived from ADOCS. The use of these applications enabled all elements to share information and develop a common operational picture, resulting in improved coordination between Naval, Air, and Ground Component Commanders.[101] The ability of networked forces to develop a COP enabled them to simultaneously achieve a very high level of SSA that, when combined with new TTPs, enabled them to synchronize their efforts from the bottom up to achieve dramatically increased combat power and to accomplish their mission in half the time required with traditional platform-centric operations.[102]

The empirical results from FBE-Delta and subsequent modeling and simulation are as follows:[103] [104]

- Average Decision Cycle Time was reduced from 43 to 23 minutes
- Average Mission Timeline (C2 time plus operational time) was cut in half
- Shooter effectiveness (kills per shot) was increased 50 percent
- Assets scrambled was decreased by 15 percent
- Leakers (special operations vessels that passed through the engagement zone to their operational destinations) were decreased by a factor of 10.

---

101 Maritime Battle Center, Naval Warfare Development Command, "Fleet Battle Experiment Delta Quick Look Report," 2 November 1998, Newport, R.I.

102 VADM A.K. Cebrowki, *Written testimony to hearing on Defense Information Superiority and Information Assurance—Entering the 21st Century*, held by the House Armed Services Committee, Subcommittee on Military Procurement.23 February 1999.

103 Maritime Battle Center, Naval Warfare Development Command, "Fleet Battle Experiment Delta Quick Look Report," 2 November 1998, Newport, R.I.

104 *An Assessment of IT-21 Warfighting Value-Added*, 1 March 1999.

The qualitative implications of this experiment are very impressive. The network increased SSA to such an extent that the units involved could self-synchronize. That process increased operational tempo and shooter effectiveness, which in turn, saved assets. The consequences of an order of magnitude decrease in the number of special operations vessels reaching their intended destination is also of significance in that it would greatly simplify the defensive operations on the South Korean peninsula.

CINCPAC, Admiral Blair, highlighted the implications of FBE Delta during a speech at WEST 2001 in San Diego in January of 2001, where he stated:

"FBE Delta unlocked the potential combat power that was latent in the Joint task force, but had been wasted due to segmentation of the battlespace."[105]

An in-depth discussion of FBE Delta is provided in the classified Appendix to this Report.

8.2.1.4 Theater Air and Missile Defense (TAMD)

In the TAMD mission, networking was shown to enable a force to significantly improve its warfighting capability. In this mission, sensors play a key role in generating battlespace awareness (Figure 8-13). Stand-alone radar sensors, such as the E-2 Hawkeye, and sensors on weapons platforms, such as AEGIS radar, detect and track objects ranging from aircraft to cruise and ballistic missiles. When these sensors are employed in the battleforce in stand-alone mode (platform-centric operations), scattering effects and environmental factors can combine and interact to degrade both detection and tracking quality. These problems are most serious against stressing targets, those characterized by high speed and/or low observables. This may mean loss of track continuity, unacceptably slow track convergence, or even failure to initiate a track against certain types of objects. The net result is poor SSA in the cognitive domain, which can significantly impact mission performance. Operational performance can be significantly increased through employment of the NCW concepts of Sensor and Engagement Grids. These concepts are operationalized with the Cooperative Engagement Capability (CEC).

---

105 ADM Dennis Blair, CINCPAC, *Remarks during Keynote Address at WEST 2001*, January 23rd, San Diego, Ca.

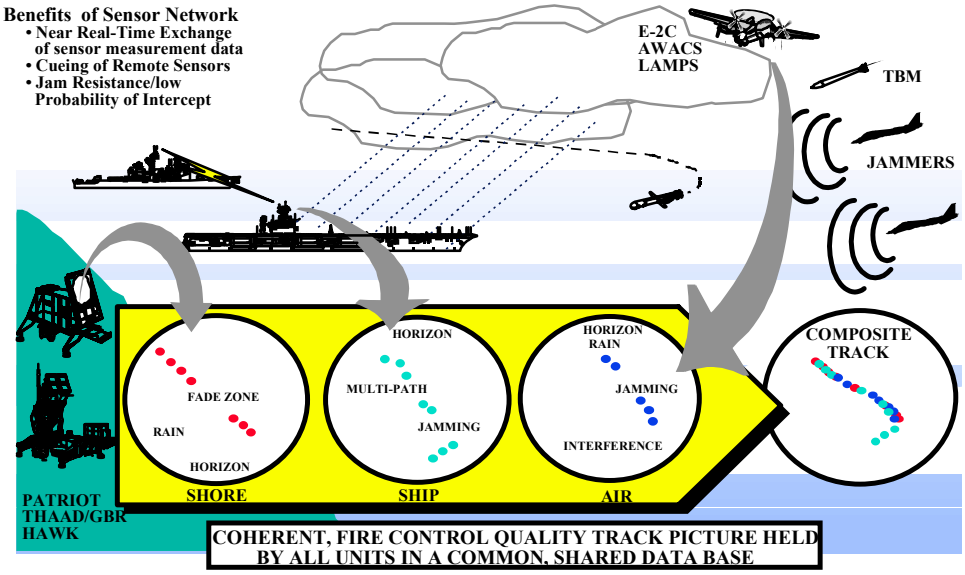


Figure 8-13. Theater Air and Missile Defense

The CEC networks battle-force sensors and enables the battle-force to share information and improve its information position by overcoming the limits of individual sensors. CEC is a unique battle force sensor netting system consisting of cooperative engagement processors and data distribution systems on all cooperating units—ship, air, and shore. Utilizing highly advanced data transfer and processing techniques, CEC is able to integrate the air defense sensors of CEC equipped surface ships, aircraft, and land sites into a single composite network that generates fire control quality information (an example of increased information richness enabled by increased reach). CEC integrates the radar and IFF measurements on each platform and distributes the measurement data to all cooperating units. This provides each cooperating unit an identical, real time air picture based on all CEC battle force sensors. This improved capability for information sharing is a key enabler of the Single Integrated Air Picture (SIAP). CEC's greater track accuracy, better identification (lower uncertainty), and decreased time to achieve a given level of track accuracy combine to give battle force commanders a higher quality of information to work with. Equally important, detection ranges are extended, which allows further time compression and more rapid achievement of engagement quality battlespace awareness, as portrayed in Figure 8-14. Warfighting benefits that result from extended detection ranges and improved information (in the form of reduced dual tracks, track swaps, and improve long term track consistency) include the ability to extend the range at which ships can engage hostile targets to well beyond the radar horizon and the ability to significantly improve area, local, and self-defense capabilities.

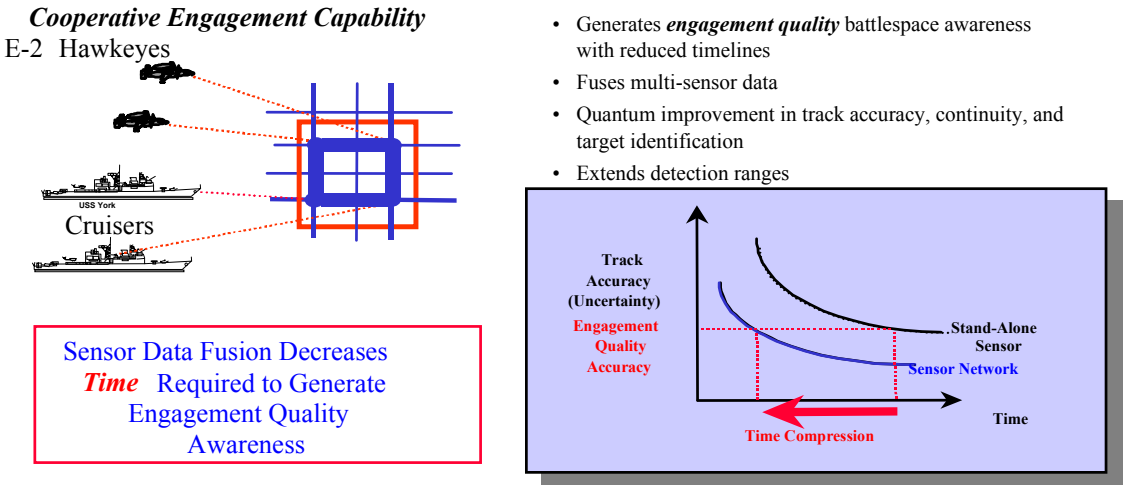


Figure 8-14. TAMD

Tactical decision making in the TAMD arena is improved directly by facilitating key decisions: which target to engage, when to engage it, and which shooter and which weapon should be used to maximize the probability of a kill. New TTPs are emerging to allow commanders to exploit the significantly improved battlespace awareness that can be achieved in this mission area through the employment of CEC. For example, Fire of Remote Data, in which a shooter engages a target it never acquires directly, but rather uses information provided by an external sensor, holds considerable promise for improving battle force asset utilization and TAMD mission effectiveness.[106]

8.2.1.5 Strike

Network-centric concepts are also enabling new warfighting capabilities in the strike arena. During *Operation Allied Force*, the Kosovo air operation, U.S. and coalition air crews flew more than 36,000 sorties in support of a wide range of missions. Numerous firsts were achieved, including the first combat deployment of the B-2 Spirit and the largest employment of Unmanned Aerial Vehicles (UAV) in history. The UAVs were employed not only as stand-alone platforms, but also in conjunction of a wide range of other ISR assets, including JSTARS, RIVET JOINT, AWACS, U-2, and other coalition and sister-service sensors.[107]

---

106 "The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest* 16, 4 (1995): p. 377-96.

107 Earl H. Tilford, "Operation Allied Force and the Role of Air Power," *Parameters,* Vol. 29, Issue 4, Winter 1999/2000, p. 24-38. Jacques de Lestapis, *DRONES, UAVs Widely Used in Kosovo Operations*, http://www.periscope.ucg.com/docs/special/archive/special-199907011327.shtml.

One of the major challenges faced by Allied Air Forces was finding, fixing, targeting, and engaging mobile ground targets. JSTARS operators, which had been extremely successful during *Operation Desert Shield/Desert Storm* at detecting and tracking moving ground targets in the desert, found that weather, terrain, and other factors made it very difficult to identify and classify possible targets in Kosovo. Moreover, Forward Air Controllers (FAC) and strike aircraft found it difficult to identify small, mobile targets from 15,000 feet (the approximate altitude needed to reduce vulnerability to surface-to-air missiles in the theater) with their onboard sensors.[108]

In an attempt to overcome some of these obstacles, the kill chain was networked, as illustrated in Figure 8-15. This linked sensors, analysts, decision makers, and shooters in new ways. The Predator (UAV) operated by the U.S. Air Force's 11th Reconnaissance Squadron was deployed to Tuzla Air Base in Bosnia. Imagery from the UAV was transmitted via SATCOM to a ground station in England, then via fiber optic cable to a processing facility in the United States. The processed information was then transmitted to the Washington, D.C. area, where it was up-linked to a Global Broadcast Service (GBS) satellite and transmitted back into the operational theater. This information was received at the Combined Air Operations Center (CAOC) in Vicenza, Italy. Targeting information was then communicated to controllers aboard an airborne command and control aircraft, which then provided it to the FAC. The FAC, in turn, provided the information to strike aircraft in accordance with established TTPs.

---

[108] David A. Fulghum, "DARPA Tackles Kosovo Problems," *Aviation Week and Space Technology* August 2, 1999, p. 55-56. John A. Tirpik, "Short's View of the Air Campaign," *Air Force Magazine,* September 1999, p. 43-47.

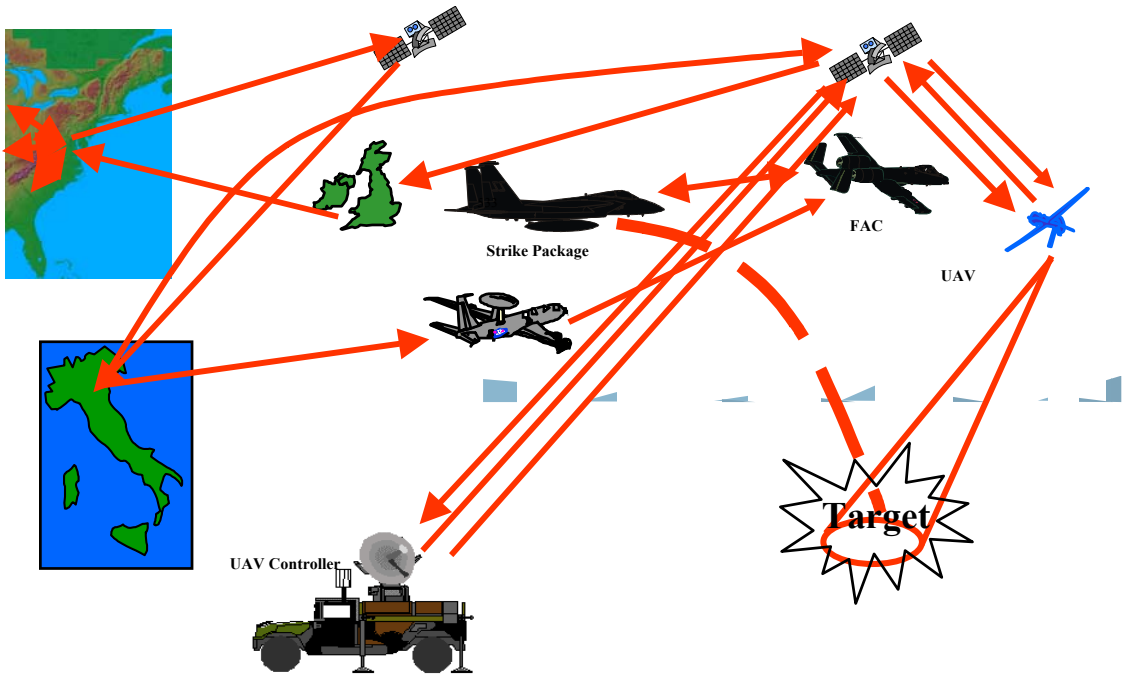


Figure 8-15. Strike: Networking the Kill Chain

The employment of this network-centric kill chain enabled the force to significantly improve its information position, as portrayed in Figure 8-16, employing reach-back linkages to generate analysis and targeting decisions promptly. As a result, the delays that often enable mobile targets to avoid detection and attack were minimized.

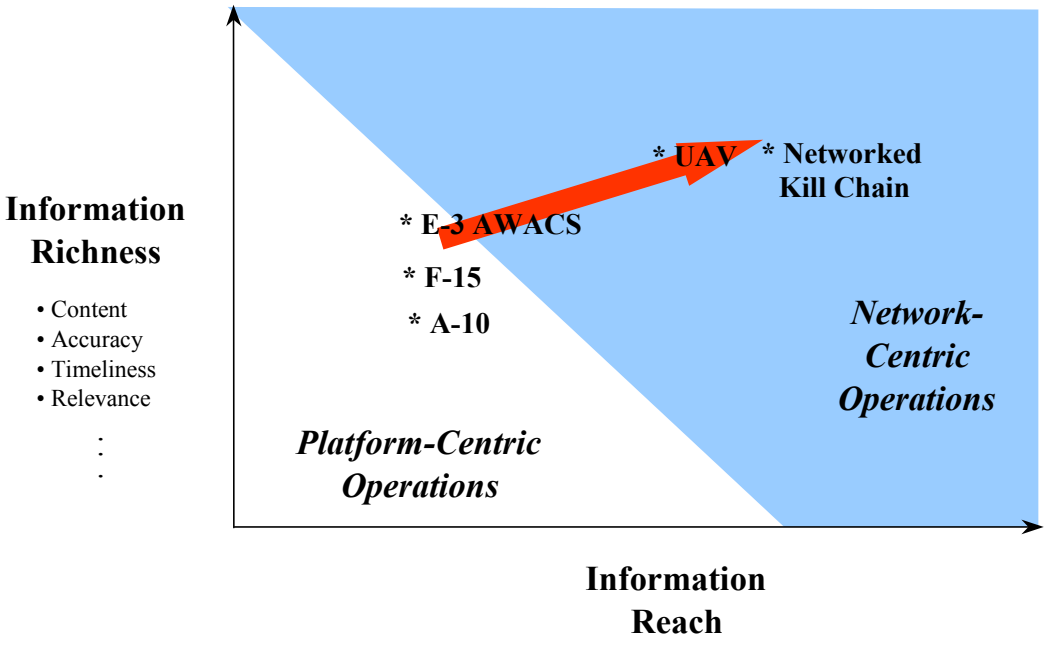


Figure 8-16. Strike: Improved Information Position

8.2.1.6 Split-Based Operations

The final example, taken from Air Force experimentation efforts in Expeditionary Force Experiments (EFX) 98 and 99, highlights the power of collaboration and synchronization. During these experiments, the Air Force, supported by Joint and coalition partners, explored more than 50 concepts, processes, and technology initiatives.[109]

Employing networks to increase combat power was central to both EFXs. A core theme was distributed operations. During JEFX 99, a forward CAOC, which consisted of approximately 300 people, was linked to and supported from a much larger, CONUS-based Operations Support Center (OSC).[110] The operational benefits of this organizational arrangement are significant. In the past the forward-deployed organization employed 1,500 to 2,000 people as shown in Figure 8-17. These personnel needed to be taken into theater along with the equipment they needed to do their jobs. This forward organization also makes major demands on transportation (reportedly 10 C-17 loads) during the early phases of an operation, reducing the lift available to move shooters and essential logistics to support them

---

[109] EFX Fact Sheet, http://efx.acc.af.mil/factsheet.htm, accessed 17 September 1998.

[110] JEFX 99 Final Report, http://jefxlink.langley.af.mil/milfinal99/main.htm, accessed 1 January 2000.

into the theater. Not only Air Force personnel and material, but also those of other Services must compete for this lift. Hence, learning to network the force at this level and operate with an effective and efficient split-based CAOC will pay major dividends in combat power. While the Air Force has reported key operational challenges based on the JEFX experience, they have also made a commitment to operationalizing this concept.

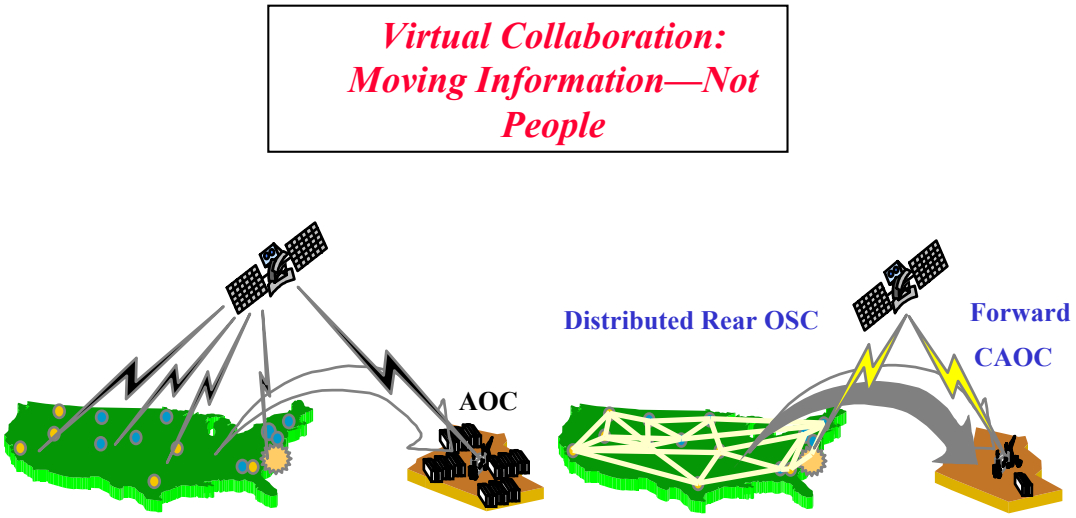


Figure 8-17. Split-Based Operations

The ability to use networks to increase SSA in control aircraft, fighters, bombers, and other support aircraft (fuel tankers, jammers, etc.) has also been a core theme during both EFX 98 and JEFX 99. At its limits, this will enable us to launch long-range bombers from secure bases in CONUS and to either provide specific targets or update target lists while they are en route to the operational theater.[111] This can improve our ability to conduct effective and efficient air operations in any corner of the planet. An in-depth discussion of CAOC-Experimental is provided in Appendix E, paragraph 5.2.6.

8.3 Observations and Conclusions

These examples clearly demonstrate that U.S. and Allied Armed Forces are beginning to understand the potential power of network-centric concepts, approaches, and capabilities. The evidence shows that, enabled by a sufficient degree of connectivity and interoperability,

---

[111] *Ibid.*

a variety of organizations have achieved increased awareness, created SSA, and leveraged this by developing new ways of doing business that increase speed of command and the tempo of operations.

While the breadth of these mission areas is impressive, it should be pointed out that this evidence comes from a limited portion of the mission spectrum. As noted in the introduction to this section, efforts to develop evidence of the power of NCO/NCW remain scattered or hit and miss, rather than focused or systematic. The fact that few of these examples actually reach across whole mission areas and that none of them really deal with the complexity inherent in Joint Task Force, operational level missions, or the Operations Other Than War (OOTW) that dominate practical experience today, mean that a great deal of research remains to be done.

In addition, the widespread acceptance of a common framework for measuring the value and/or maturity of network-centric operations has hindered the evaluation of exercises, experimentation, and operational evidence.

However, the importance of this evidence should not be minimized. The significant improvements in combat power documented here lends considerable weight to the central hypotheses of Network Centric Warfare and the ability of maturing network-centric concepts and capabilities to make *Joint Vision 2020* a reality. Clearly, there is a benefit to employing a more systematic approach to organizing research, collecting evidence in operations, exercises, experiments, and demonstrations, and in assessing that evidence. In addition, there is also a compelling benefit to going beyond traditional combat to explore the full range of command and control concepts enabled by Information Age technologies.

Section 9

Global Information Grid

NCW is shorthand for a set of broad operational concepts and material wherein warfare (and also support) capabilities are focused and directed by entities that form an operating network. That network allows the elements to best utilize an effective combination of organically available information and information obtained from other entities operating at a distance. NCW operations can be hierarchical or collaborative or a combination of decisional styles needed to meet the Commander's intent. In the final analysis, NCW is all about warfare.

The GIG is shorthand for operating concepts and material that form the information matrix upon which NCW warfighting entities exist, operate, and depend. The GIG enables the collection, processing, and protection of data; the elevation of that data to useful information; and the flow of and access to information among the networked warfighting entities. The GIG represents the foundation for secure and assured access to information needed by Joint combat and combat support elements. Many of the advanced technologies that are to be implemented within the GIG architecture are, in themselves, transformational in that they directly enable the robust experimentation needed to rapidly explore new operational concepts within the network-centric environment. In the final analysis, the GIG is all about enabling the flow of information.

9.1 GIG Defined

This report earlier emphasized how Information Superiority derives from the ability to create a relative information advantage vis-a-vis an adversary. And after having achieved Information Superiority operationally, making the optimal use of this advantage means effectively and efficiently meeting the critical information needs of the operational forces. Competitive advantages accrue to organizations that successfully master the art of realizing an information advantage—using the position of Information Superiority for maximum leverage. The concepts and capabilities inherent in the GIG will be the means to best ensure Information Superiority.

The concept of a “Global Information Grid” was born out of concerns regarding interoperability and end-to-end integration of automated information systems. Issues such as streamlined management and the improvement of information infrastructure investment have also contributed to the heightened interest in the GIG. The real demand for a GIG is driven by the requirement for Information Superiority and decision superiority as expressed in *Joint Vision 2020,* and discussed previously in Section 2.2.

Today’s threats present a wide array of asymmetric challenges to warfighting capability across the variety of warfighting missions the US military undertakes in both Joint and

Multinational environments. These missions are tasked around the world in support of ad hoc military and civil structures. The current IT infrastructure constructs no longer optimally meet the globally distributed information superiority needs of warfighters and sustainers within the increasingly important context of coalition operations. The GIG will provide the Joint and coalition warfighter with a single, end-to-end information system capability that includes a secure network environment, allowing users to access shared data and applications, regardless of location, and supported by a robust network/information-centric infrastructure.

The GIG is a system of systems (SoS) that provides a set of value-added functions operating in a global context to support processing, storage, and transport of information; human-GIG interaction; network management; information dissemination management; and information assurance (IA). These functions are fully interrelated, integrated, and interoperable with one another in order to achieve overall interoperability across the GIG. The integration of these functions is portrayed in the GIG Systems Reference Model and GIG Sub-Systems View, portrayed in Figures 9-1 and 9-2. As a result, the GIG is an information environment comprised of interoperable computing and communication components.

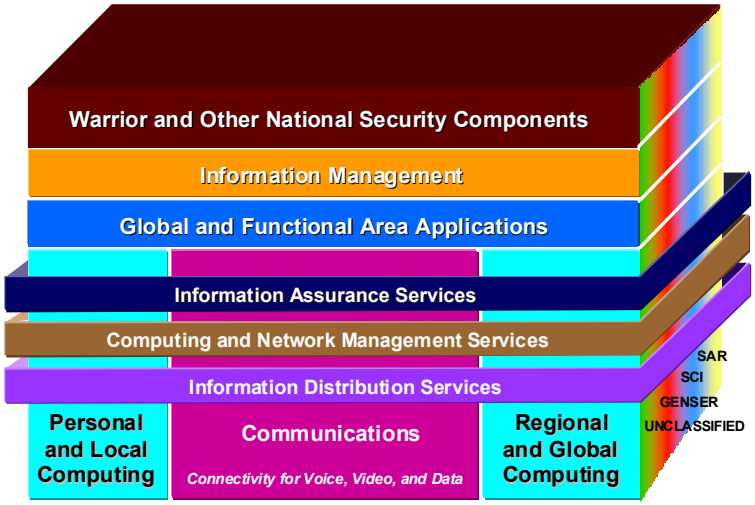


Figure 9-1. GIG Reference Model

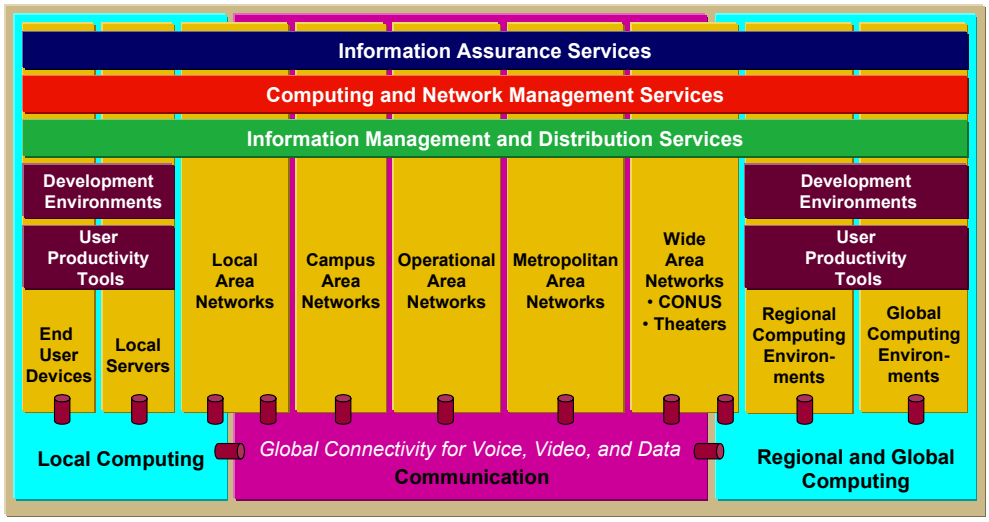


Figure 9-2. GIG Sub-Systems View

The GIG is essential for information and decision superiority. It will enable C4I integration of Joint forces, improve interoperability of systems, and increase optimization of bandwidth capacity, thereby dramatically improving the warfighting capabilities of Joint forces across the full spectrum of conflict. The GIG will enhance operational capabilities while providing a common operational environment for conventional and nuclear command and control (C2), combat support, combat service support, intelligence, and business functions. In particular, the GIG will support:

- Warfighters' ability to operate with reduced forces at high operational tempos where dynamic planning and redirection of assets is the norm
- Delivery of information concerning targets, movement of forces, condition of equipment, levels of supplies, and disposition of assets to Joint commanders, their forces, and the National Command Authority within required timeframes
- Warfighters' ability to obtain and use combat and administrative support information from national and widely dispersed assets
- Collection, processing, storage, distribution, and display of information horizontally and vertically throughout organizational structures across the battlespace
- Rapid and seamless flow and exchange of information around the globe to enable collaborative mission planning and execution from widely dispersed locations and at different levels (to include strategic, operational, tactical, and business)
- Timely, assured connectivity and information availability for decision makers and their advisors to support effective decision making

- Integrated, survivable, and enduring communications for the NCA, Integrated Tactical Warning and Attack Assessment (ITW/AA), and strategic forces

Currently, the GIG concept is supported by the DoD CIO memorandum "Global Information Grid," September 22, 1999, validating the requirement for this initiative. Additional clarification has been made to this definition, as agreed by the Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics), the Office of ASD (C3I) and DoD Chief Information Officer, and the Joint Staff (J6). The clarification cited below was signed in May 2001, agreeing that GIG is:

The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in Section 5042 of the Clinger-Cohen Act of 1996. The GIG supports all missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, Allied, and non-DoD users and systems.

[GIG] Includes any system, equipment, software, or service that meets one or more of the following criteria:

- *Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services*
- *Provides retention, organization, visualization, IA, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services*
- *Processes data or information for use by other equipment, software, and services*

Non GIG IT—Stand-alone, self contained, or embedded IT that is not or will not be connected to the enterprise network.

9.2 Policy, Governance, and Architecture

9.2.1 Policy and Governance

There is an overarching GIG policy and seven supporting policies that have been developed in Guidance and Policy Memoranda as part of the GIG program. Each is described below.

- *DoD Directive 8800.aa, GIG Overarching Policy, (replaced DOD Chief Information Officer Guidance and Policy Memorandum (CIO G&PM) No. 8-8001, March 31, 2000) Global Information Grid*: Provides the overarching guidance which defines the major policy principles and associated responsibilities for the Global Information Grid. The GIG will be based on a common, or enterprise-level, communications and computing architecture to provide a full range of information services at all major security classifications, and new systems will use common GIG assets.
- *CIO G&PM 4-8460, August 24, 2000, "GIG Networks"*: Provides guidance on constraints for network selection, architecture development, security and information assurance, network operations, performance, financial strategies, and governance. GIG networks will operate as a fully interoperable, end-to-end network through managed application of standards and configuration management discipline. Existing Wide and Metropolitan Area Networks, not presently part of Defense Information Systems Network (DISN), will be reviewed for migration to the DISN. Policy covers all outsourcing activity.
- *DOD CIO G&PM 10-8460, August 24, 2000, "GIG Network Operations"*: Provides guidance intended to place an operational perspective on the management of networks. Includes direction for distributed management and control functions with integrated operational oversight; architecture development; standardized, interoperable control and management capabilities; tiered management hierarchy; integration of network management, IA, and information dissemination management activities; end-to-end visibility for services across all other DoD component transport networks; global, as well as regional network SSA; maintaining a network COP for their AOR; authority; and governance.
- *DOD CIO G&PM 7-8170, August 24, 2000, "GIG Information Management"*: Provides guidance on identification, documentation, and validation of GIG information requirements; discovery, retrieval, and management of the flow of GIG information; implementation of mechanisms for access and delivery; processes and methods to facilitate the proper understanding and use of information; and performance measures, associated metrics, and reporting processes.
- *DOD CIO Guidance and Policy Memorandum 6-8510 - Department of Defense Global Information Grid Information Assurance and Information Assurance Implementation Guide," signed June 16, 2000:* Provides guidance on assignment of a mission category (mission critical, mission support, or administrative) that reflects the type of information handled by the system relative to requirements for integrity; employment of protection mechanisms in accordance with the level of concern; confidentially of network and infrastructure services (e.g., link encryption, one-time passwords, virtual private networks(VPN)); defenses against denial of service attacks (e.g., diversity, routing table protection, planned degraded operation); defense of the

perimeters of well-defined information enclaves (e.g., firewalls, intrusion detection, uniform policy on protocols allowed across perimeter boundaries); use of supporting IA infrastructures (e.g., key management, public key certificates, directories); certification and accreditation; management of all inter-connections of GIG information systems; COMSEC equipment; use of COTS hardware, firmware, and software components, and public domain software products.

- *DOD CIO Guidance and Policy Memorandum 12-8430, Acquiring Commercially Available Software,* signed July 26, 2000: Provides guidance on acquiring and managing software as a DoD-wide asset, to include the aggregation of the acquisition of commercially available software and software maintenance.
- *DoD 8190.2, DOD Electronic Business/ Electronic Commerce (EB/EC) Program, dated June 23, 2000:* Provides guidance or the direction, management, and coordination of EB/EC activities within the DoD.
- *DoD CIO 11-8450, GIG Computing, 6 April 2001*. Provides guidance on consolidation of computing operations; use of DoD-designated regional or global computing centers; use of standard GIG configurations for user and local computing environments; conduct of best value Business Case Analyses (BCA) and performance assessments, migration plans, inventories, and Service Level Agreements (SLAs) between the using organizations and computing service providers; continuity of operations; and performance measurement.

Additionally, the GIG CRD is currently in final review within the Pentagon. The task of preparing the GIG CRD was assigned to the United States Joint Forces Command (USJFCOM) by the Joint Requirements Oversight Council (JROC) under the sponsorship of the Joint Staff/Command, Control, Communications and Computer (C4) Systems Directorate (J6) and the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD C3I). The JROC Memorandum 135-99 (JROCM 135-99) of 23 November 1999 outlined the task for the development of this CRD. This document is the culmination of multiple strategy meetings and coordination initiatives that have occurred since then. The CRD development process was assisted by representatives from other CINCs, Services, and Agencies who participated in the GIG requirements development conference held 4-6 April 2000, and who provided input during subsequent document review and comment phases.

The organization and content of the CRD are in accordance with *CJCSI 3170.01A Requirements Generation System* document dated 10 August 1999. It is also consistent with:

- GIG Vision of the Chairman, Joint Chiefs of Staff
- OASD(C3I) GIG Systems Reference Model
- DoD Chief Information Officer's (CIO) GIG definition

The GIG CRD contains validated capability requirements and Key Performance Parameters (KPP) (including the information exchange requirements and the interoperability KPP). These requirements and KPPs will guide all DoD and Intelligence Community components in developing ORDs for new systems and for upgrading legacy systems. The GIG CRD will guide future Information Technology (IT) investments to ensure interoperability. All Mission Need Statements (MNSs), ORDs, or CRDs that are associated with GIG-enabled systems,[112] regardless of acquisition category (ACAT), must show compliance with this CRD, as appropriate/applicable.

9.2.2 GIG Architecture Development

On 1 February 2001, the GIG Senior Steering Council (SSC) received a briefing on the status of the GIG program to develop GIG Architecture Version 1.0. This information brief presented by Office of the DoD Chief Information Officer (ODCIO) updated the Board on efforts over the past six months in constructing the first version of the GIG architecture. The key emphasis of the brief was on developing clear ties between the operational and business missions supported by the GIG, and the systems, application, and processes comprising the GIG. The goal of the Version 1.0 architecture effort is to create a vehicle for facilitating interoperability and sound IT investment decisions. GIG SSC principals, including the Joint Staff (JS) J-6 and the Deputy Assistant Secretary of Defense for C3, Intelligence, Surveillance, Reconnaissance, and Space, questioned whether or not the baseline information received from CINCs, Services, and Agencies was consistent enough to provide for "apples to apples" comparisons. The ODCIO briefer expressed a low degree of confidence they were, but observed that Version 1.0 of the GIG Architecture serves as a foundation on which to build more complete and consistent editions. The GIG SSC was told to expect that DoD CIO would approve release within the next six weeks with subsequent releases following once every year.

9.2.2.1 Coalition Wide Area Network

The GIG SSC was also briefed about the Combined Communications Electronics Board (CCEB) Coalition Wide Area Network (CWAN). This brief by Joint Staff /J6T was the first formal presentation of this topic to CINCs and MCEB Principals of the CWAN Initiative. The effort originated by Multinational Interoperability Council in October 1999. It was further refined by May 2000 CCEB to construct capability to deliver SECRET classification e-mail with attachments, and to interconnect CCEB nations' C2 systems critical to the warfighter. The U.S. Navy Principal participating in the GIG SSC brought to the Board's

---

[112] Any system that exchanges and/or disseminates information in the manner described in the GIG definition, and is in compliance with the capability requirements stated in the GIG CRD, as appropriate and necessary to fulfill the system's operational purpose(s)/mission(s), is considered to be GIG-enabled.

attention Navy effort to develop a CWAN afloat capability as part of a larger initiative in the Navy venue of Australia, Canada, New Zealand, United Kingdom, and U.S. (AUSCANZUKUS). The U.S. Navy Principal also mentioned Navy's use of Naval Computer and Telecommunications Area Master Station (NCTAMS) Pacific at Wahiawa, HI, as the Network Operations Center (NOC) for USCINCPAC's CWAN initiative and its potential as a baseline for future CWAN initiatives.

9.2.2.2 Coalition Interoperability and CWAN

The GIG SSC subsequently received a Coalition Interoperability brief presented by J6 as a follow-on issue to that discussed previously in the CCEB CWAN brief. The Coalition Interoperability brief was intended to answer a previous tasking from the June 2000 GIG SSC. Central to this discussion was the many CWAN initiatives being pursued by various CINCs. GIG SSC Principals quickly recognized the need for a standardized methodology for designing and implementing CWANs to leverage past lessons learned. One expressed concern however was the limited number of nations with which the CINCs can implement a CWAN. To be truly effective, the number of nations must be expanded to recognize other key coalition partners, particularly in the Pacific theater. Conversely, one attendee noted there also must be a process for removing nations from an established CWAN. The DISA Principal added that technically these types of strategic planning information exchange mechanisms are achievable, but the real challenge involves information management. The GIG SSC endorsed development of CWAN CJCSI to standardize CWAN construction.

9.2.3 Protecting the Information Infrastructure

One of the first major thrusts of the GIG architecture and implementation is the area of network operations. This is bringing an integrated, synergistic approach to IA, network management, and information dissemination services. Development of operational and system concepts to support the protection of the information infrastructure is ongoing. Requirements for capabilities have been identified and include:

- **Full-time operations for best NetOps support**
- **Automated Tools:** Integrate, procure, and develop real time analysis tools for:
  - Network Management
  - Intrusion Detection
  - Data and Computing
  - Automatic response
- **Centralize Operation Centers:**
  - Report NetOps status as part of Readiness

  - Organizational Changes:
    - Support NetOps SSA at CINC's Theater C4ISR Coordination Centers (TCCC) and the National Command Authority (NCA)
    - Integrate NetOps into coalition operations
- **Interoperability:** Incorporate NetOps into all future operational and interoperability test & evaluation activities.

9.3 Strategy for Implementing GIG

The Defense Science Board[113] recommended establishment of an Executive Office for implementing GIG. The Board's recommendations are quoted for information:

> The Task Force recommends that the Information Superiority Board of Directors establish an Executive Office responsible for leading and implementing the DoD-wide, common-user virtual Intranet, the GIG. We recommend that the office and leadership position be established by 29 February 2000.
>
> It is recommended that the Executive Director be a minimum five-year appointment and be tasked to develop an implementation plan, including technical milestones and measurable interim goals, and identify resources to permit the transition to and completion of the GIG by 30 September 2003. It is further recommended that systems engineering support be provided to the Executive Office through a dedicated systems engineering team. The Task Force recommends that the Implementation Plan for moving from DoD's present circuit-based infrastructure to the GIG be developed by 31 October 2000 and updated semi-annually.
>
> It is recommended that the Executive Director, with support from ASD/C3I and USD/AT&L, task all DoD and Service Program Managers/Program Executive Officers (PM/PEO) responsible for tactical/strategic telecommunication systems to conduct studies on how to transition their systems to permit integration into a common-user DoD virtual Intranet. Furthermore, the Executive Director should fund two competitive industry studies that address how (not if) emerging commercial communication satellite systems, fiber infrastructures, and mobile Internet technologies can be exploited to implement the DoD-wide virtual Intranet. These studies should be completed by 31 July 2000.

---

[113] Office of the Under Secretary of Defense (Acquisition and Technology), *The Defense Science Board Task Force on Tactical Battlefield Communications Final Report,* December 1999.

Based on this study's results, it is recommended that the Executive Director be given the task to transform DoD communications from a circuit/broadcast and system-centric framework to a common-user, Internet framework.

OASD (C3I) and OUSD (AT&L) have been working these recommendations at the Principal Deputy level. They have worked out many of the relationship details to assure OASD (C3I) efforts are correctly focused and coordinated with the Defense Acquisition Executive. The GIG implementation plan is being developed, and should be presented for approval by principals in late FY01 or early FY02. At this time, it is not appropriate to incorporate details of the plan that may change prior to approval.

9.4 Snapshot of Where We Are Today

An authoritative source of information about where the DoD is in progressing toward NCW is provided by the Defense Science Board[114] 1999 report on Tactical Battlefield Communications. The Board noted that they exceeded their terms of reference, addressing end-to-end communication requirements rather than limiting themselves to consideration of the "battlefield" only.

The DoD and commercial sector members of the Board found that they had some differences of perspective worth noting in the report. In particular, the commercial sector was more optimistic about the contribution of technology as a solution to limitations. For example, they noted that commercial satellite system planners expect to recapitalize the space-based infrastructure every five to eight years, and continuously upgrade fiber optic system capacity and technology. Commercial sector participants in the Board cited the investment rate of one network provider as being $3,000,000 per day.[115]

DoD members of the Board focused more on policy issues that currently limit DoD capability, and are likely to continue to do so. Principal among these limitations is "Title 10 arguments about who is in charge."[116] They noted other constraints, such as complicated national and international processes for frequency allocation, but emphasized most strongly the need for progress in looking at DoD NCW as an enterprise, rather than as CINC, Service, and Agency independent domains.

---

114 *Op. cit.*

115 *Ibid,* p. vi.

116 *Ibid.*, p. vii.

9.4.1 Connectivity

Connectivity has greatly improved in the last two decades. Army Echelon Above Corps (EAC), Naval Force Component Commander (NAVFOR), Marine Air-Ground Task Force (MAGTF), and Air Force Wing Operations Centers (WOC) have voice and data connectivity that was previously only available to fixed base forces.

Voice connectivity has greatly improved, with introduction of standards-based secure and non-secure telephony. Some enclaves of connectivity problems remain, as noted in paragraph 9.4.3 below addressing interoperability. Voice remains almost entirely separate from data, however. This is partly due to the lack of reliable, seamless implementation of Voice over Internet Protocol (VoIP) standards by commercial industry. The lack of momentum toward VoIP or Voice over Asynchronous Transfer Mode (ATM) is also due in part to reluctance to recapitalize investment in Standard Telephone Unit (analog) and Standard Telephone Equipment (STE) (digital) secure telephony. In fact, STE is being proliferated into higher echelons of tactical forces where the Integrated Services Digital Network (ISDN) bandwidth requirements (64 kilobits per second minimum) are problematic.

Data connectivity is migrating to industry standard IP. Within individual units, IP is the protocol of choice, with the notable exception of aircraft. Use of IP for aircraft systems is limited to a few command control platforms, with the standard for data exchange being the 1553 data bus.

9.4.2 Bandwidth

The Defense Science Board noted differences between commercial and DoD sector members in the area of bandwidth. Commercial sector members saw bandwidth as an opportunity; DoD members saw it as an expense. The opportunity for commercial sector members lay in the potential of broadband transmission links to support services that generate revenue. They noted that in some cases, ownership of capacity in broadband transmission links is in itself a valuable source of revenue.

DoD members saw the demand for bandwidth as an affordability issue. They particularly noted that they were not able to find enterprise-wide requirements for bandwidth: they found quantified requirements at the Service operations level. Further, they noted that these requirements "…were based on prior experiences and perceived, but unsubstantiated needs for the future." The DoD Decision Support Center study, "Global Information Grid Support to CINC Requirements,"[117] provides a characterization of bandwidth requirements and indicated ongoing study of this topic is required.

---

[117] DoD Decision Support Center, *Global Information Grid Support to CINC Requirements,* DSC study FY00-05, FY01-05.

Quality of Service (QoS) is emerging as a technology approach to improving the use of bandwidth. Current transmission system implementations allocate fixed shares of bandwidth to voice, data, and video teleconferencing. QoS mechanisms will, in combination with ATM or QoS-compliant IP switches, enable disciplined bandwidth sharing among these (and other) users of bandwidth. High-priority (but infrequent) users will be able to get bandwidth on demand, and lower priority (but more constant) users will be able to utilize available bandwidth on a not-to-interfere bases. QoS is not widely implemented across DoD, however. Industry has offered standards-based QoS ATM services, but DoD is not using ATM as widely as industry. QoS offerings in commercial IP products are often vendor-specific, limiting their usefulness. An industry enterprise may choose to implement equipment from one vendor to gain the benefit of increased bandwidth efficiency; this is not an option for DoD.

DoD has requirements for precedence on networks (i.e., transport layer), to ensure that individual information units (such as messages) are handled in precedence order. This is a DoD unique requirement and has hindered the use of COTS applications for time-critical messaging systems. DoD personnel use COTS products for individual messaging and the organization message system, the Defense Message System (DMS), modifies COTS products to get precedence at the application layer.

9.4.3 Interoperability

The Defense Science Board noted: "…there is no established and accepted DoD database of Joint Information Exchange Requirements (JIERs)."[118] The lack of this database limits OSD and Joint Staff efforts to ensure interoperability through the Requirements Generation System. New ORDs are asserting JIERs, but prior to the publication of the GIG architecture[119] there has been no context for analysis of JIERs. CINC, Service, and Agency program advocates are free to assert unique JIERs for individual programs, and JROC has no analytic basis for finding and resolving duplication.

Current radio waveforms impose interoperability limitations. The Joint Tactical Radio System (JTRS) legacy waveform effort currently ongoing has the objective of making all legacy waveforms available to all force elements in a software definable radio.

Legacy secure voice protocols (such as Narrowband Subscriber Terminal) still impose interoperability limitations among ground force users, and the maritime forces that support

---

[118] Defense Science Board, p. vi.

[119] OASD (C3I) and Deputy CIO Director Architecture and Interoperability, *Global Information Grid Architecture Status Report,* undated (presented in June 2001).

voice equipment. This is an expensive work-around, especially in view of the fact that legacy secure voice equipment is out of production and in some cases is difficult to support.

Legacy multiplex equipment also limits interoperability. Army and Air Force tactical satellite multiplex equipment is still not interoperable. Navy satellite communication multiplex is interoperable with neither. ATM has been tested and found effective as a COTS replacement multiplex, but there is no imperative for investment to replace legacy equipment.

9.4.4 Security

Commercial sector members of the Defense Science Board asserted that industry is providing mechanisms for privacy, authentication, integrity, continuity of service, verification, and nonrepudiation. Those services that are being supported through Public Key Infrastructure (PKI) have been adopted by DoD and are mandated for implementation by the Global Information Grid IA and IA Implementation Guide. DoD has also approved[120] policy guidance in this area. Furthermore, PKI solutions, integrated with database systems and Intrusion Detection Systems (IDSs), have potential to be used as a mechanism to reduce the insider threat in the private sector.

Legacy encryptors are being replaced with TACLANE and FASTLANE encryptors that are capable of packet encryption instead of stream encryption. These encryptors do not, however, support QoS because they do not permit signaling from the "encrypted" side (transmission network) to the "unencrypted" side (applications that offer traffic to the network). This limitation will further slow use of QoS to improve efficient use of bandwidth.

9.4.5 Ongoing Integration Initiatives

The Defense Science Board noted that there is a "…significant lack of 'systems' perspective and independent system engineering organizations within DoD to provide the necessary studies and analyses…."[121] There are several initiatives to address this deficiency. GIG has issued the Version 1.0 Architecture document, providing an enterprise-wide reference for CINC, Service, and Agency warfighting and business system acquisition. The Version 1.0 ongoing work and additional detail will extend the Architecture and will be added to CINC, Service, and Agency systems that can be connected to the GIG Architecture. This work should enable the establishment of a JIER database and the architecture context to make the comparison of existing and proposed JIERs meaningful. The architecture can also

---

[120] Public Key Enabling of Applications, Web Servers, and Networks for the Department of Defense.

[121] Defense Science Board, p. vii.

provide an operational and system reference for the modeling of bandwidth requirements against validated CINC Operations Plans and Contingency Plans.

OUSD (AT&L) has established the Single Integrated Air Picture System Engineer (SIAP SE) to address deficiencies in Joint air operations. This effort must be integrated with GIG to assure the SIAP system engineer has an enterprise context for integrating air picture information processes with enterprise-wide processes. Navy (the Common Command and Decision program) and Air Force support the SIAP SE effort.

Section 10

NCW and DoD—Policies and Processes

10.1 Personnel

10.1.1 Need for an IT Literate and Knowledge-Based Work Force

People are our most important asset. Improved productivity in the Information Age depends, in large measure, upon our ability to attract, train, and retain a highly skilled workforce. This skilled workforce can then create the core business processes designed to capitalize upon available knowledge, and create and maintain the knowledge repositories (the reusable knowledge bases). DoD's ability to create and leverage the SSA necessary for NCW depends on individuals who are prepared to tackle Information Age problems with Information Technologies. DoD needs both a cadre of highly skilled IT professionals and a well-educated workforce that understands how to exploit information. Improving IT skills among our cadre of IT professionals and making our workforce more IT-literate will contribute significantly toward improving many of the "weak links" in the NCW value chain—specifically the protection of information and information processes, the creation and sharing of SSA, collaboration, and the development of network-centric mission capability packages.

A corps of appropriately trained and experienced IT professionals is the most critical component in protecting the Department's information resources against modern-day cyber attacks. Individuals using, administering, and maintaining these systems must be masters of proscribed protective procedures, and know how to operate the equipment designed to mitigate these threats.

In a *Federal Computer Week* article written in March 2000,[122] (at the end of the high-tech boom of 1999 and 2000), Service representatives identified problems in retaining mid-career military service personnel. In this article, IT personnel retention was cited as a problem, and a RAND Corporation researcher[123] cited an inability to target pay on skills that were in demand as a particular problem. The commercial IT sector slowdown could be expected to help DoD attract and retain required civilian and military personnel. Further, IT support contracts would be expected to help supply skills that the civilian and military personnel systems cannot.

---

[122] Colleen O'Hara, "Military Tech Workers Fall Out," *Federal Computer Week,* 20 March 2000.

[123] *Loc. Cit.*

To create, train, and retain a cadre of professionals that can help protect and exploit information, the critical enabler of NCW, DoD needs to accomplish the following:

- Create an adequate package of incentives
- Provide adequate training
- Provide career management.

10.1.2 Personnel Incentives

DoD is failing to attract promising candidates and losing many of its most experienced IT professionals to the higher paying jobs in private industry. A strong incentive program is required to enable, acquire, and retain a cadre of highly skilled IT professionals, both uniformed and civilian. The military has just begun to explore the authority to provide a pay differential for critical IT professional skills. Although there is more latitude with civilians to provide monetary awards, there is currently no professional pay differential for civilians either (like there is for doctors, lawyers, and pilots in other departments). One mechanism to mitigate this problem would be to provide pay differential to people assigned to positions that require IT skills/expertise. Another would be to provide signing bonuses to military IT professionals.

This package should also include proficiency pay; enlistment and retention bonuses; training in advanced technology; opportunities to work with industry, academia, and government laboratories on high technology; and the opportunity to work on modern state-of-the-art systems supporting national security. In addition to competitive financial incentives, DoD must give the soldiers and civilians who perform these crucial functions a high quality work environment, exciting challenges, and the opportunity to perform important missions for our National Defense. In short, we need a total package to attract and retain these critical skills.

The available pool of information technology civilian careerists is of great concern. To acquire and continuously sustain a pool of civilian and military IT professionals to carry out the diverse information technology based functions of the Department, we must act now to appropriately plan and implement the following initiatives:

- Development and creation of a specialty skill tracking system with pay incentives, while allowing upward mobility and further professional development
- Establishment of programs to pay for civilian schooling for IT professionals with retention stipulations that would require the student to stay within the government for a set number of years
- Promotion developmental assignments to sharpen executive and technical skills by leveraging the individual's knowledge and background

- Establishment and management of fellowship/cooperative programs with industry leaders, thus improving our competitive edge
- Creation of a "within-the-government" high-tech employee exchange program, again to leverage the information technology knowledge base

10.1.3 Training

Although training for all employees using DoD computer systems is already mandated by statute and Department regulation, many lack a sufficient level of technical and procedural knowledge to fully protect the DoD's information resources. However, even if all DoD personnel were up to speed, IT training is highly perishable. It is not a one-time event for employees to learn a specific skill. Rather it is a technology-driven continuum of knowledge that is ever changing.

Everyone—from the user in the foxhole to the intelligence analyst, from the weapons system developer to the professional network managers and system maintainer—must have some IT training. This not only provides the common knowledge base needed to leverage interoperable systems and networks, it also helps create the more knowledgeable workforce DoD needs to efficiently operate as the IT environment changes.

Furthermore, the DoD must keep its IT professionals at knowledge parity with their contemporaries in industry and must therefore provide continuous training opportunities to its professionals. As DoD's IT infrastructure evolves, IT training must evolve to allow the DoD workforce to sustain highly perishable IT knowledge, and cope with rapidly shifting work focuses. The DoD must evolve different IT training concepts, based on the military's different and unique systems' needs, to determine the best means of supporting and increasing our warfighting capabilities.

A modern curriculum of DoD-sponsored IT educational opportunities needs to be established and maintained. Appropriate training and opportunities must be made available via the latest distribution techniques. In some cases, the curricula will be commercially available, in others they will be modified versions of commercial products to meet the special needs of the DoD. The main point, however, is that for the first time, from a Department-level approach, a core of standardized skills and knowledge will be required learning for DoD IT professionals. That core will be the foundation of new IT certification requirements and will be augmented by special civilian and military Service training needs as necessary. The Department must also provide continuing training to IT professionals as well as the user community because both have a critical role to play in the protection of the content carried by DoD systems and networks.

10.1.4 Career Management

To complement a competitive incentive package, DoD must provide IT professionals with attractive career paths in order to retain its best and brightest. This should be done by creating clear and effective IT career management mechanisms. Additionally, the Department must determine the size of its IT population and know precisely what IT activities/functions it is performing. Today, the Department is unable to efficiently determine this information.

Appropriate career management databases and tools need to be designed and implemented to code and track civilian and military Service IT professionals. In many cases, existing personnel databases are devoid of appropriate IT categorizations and career descriptors. These descriptions need to be updated or modified with a standardized list of IT functions against which tracking can begin. The personnel databases should then be populated with the appropriate IT function codes. The information gleaned from this tracking would allow the Department to size its IT population in various categories and track the training achievements and adherence to certification requirements of those individuals assigned to that population. In short, it would allow career management of IT professionals in ways that are unachievable today.

Progress is being made in meeting the challenges of IT career management. As this report goes to press, the Navy is in the process of establishing a new Information Professional (IP) career field for its officer corps. This is being done to meet the growing Navy demand for officers with specialized skills in Information Technology. The Information Professional career field will provide officers with expertise in information, command and control, and space systems that support Navy operational and business practices. Additionally, the IP career field will provide officers with expertise in the information and space technologies that are the building blocks of command and control, communications, and computer architectures, as well as the information and knowledge elements that are essential for information and knowledge superiority. An in-depth discussion of how the Marine Corps is addressing the challenges of IT career management is provided in Appendix D, paragraph D.3.3.

10.2 Requirements

The DoD has updated the process for developing requirements to improve the responsiveness of the Defense Acquisition System to requirements for NCW and Information Superiority capabilities. This update has emphasized delineation of performance-based requirements by the operational (warfighter) community. The Requirements Generation System,[124] as called for by the Defense Acquisition System,[125] establishes the policies and

---

[124] *CJCSI 3170.01B*, signed 15 April 2001 vice 13 Feb 2001.

procedures for a uniform, department-wide process for the generation of requirements. The update to the Requirements Generation System instructs requirements developers to adhere to the guidance contained in Section 4.7.2 of DoDI 5000.2, Operation of the Defense Acquisition System. Selected policy from Section 4.7.2 of DoDI 5000.2 is summarized below:

In the process of refining requirements, the user shall adhere to the following key concepts:

- Keep all reasonable options open and facilitate cost, schedule, and performance trades throughout the acquisition process.
- Avoid early commitments to system-specific solutions, including those that inhibit future insertion of new technology and commercial or non-developmental items.
- Define requirements in broad operational capability terms.
- Develop time-phased requirements with associated objectives and thresholds (as appropriate).
- Evaluate how the desired performance requirements could reasonably be modified to facilitate the potential use of commercial or non-developmental items and components.
- Evaluate whether system will be able to survive and operate through the anticipated threat environment.
- Consider Critical Program Information needs, anti-tamper, and intelligence support requirements.
- Address cost in the Operational Requirement Document (ORD), in terms of a threshold and objective.
- Include requirements for security, information assuredness, and critical infrastructure protection with consideration of releasability criteria for multinational operational environments.
- Consider supportability, data sharing, and interoperability needs of the family of systems in the operational environment.
- Mandate interoperability as a key performance parameter (KPP) to be documented in all ORDs and Capstone Requirement Documents (CRDs) (reference (i)) and included in the Acquisition Program Baseline (APB) (reference (c)).

---

[125] Paragraph 1.a, CJCSI 3170.01B.

- For purposes of interoperability and supportability, all IT (including National Security Systems—NSS) acquisition programs regardless of acquisition category, developed for use by U.S. forces are for Joint, combined, and coalition use. The intent is to develop, acquire, and deploy IT systems that meet essential operational needs of U.S. forces. Interoperability and integration of IT requirements shall be determined during the requirements validation process by the DoD Components and Joint Staff (through review of all Mission Needs Statement (MNSs) and ORDs) and shall be updated as necessary throughout the acquisition, deployment, and operational life of a system. Given the potential Joint nature of Automated Information Systems (AISs), all AIS MNSs and ORDs shall be submitted to the Joint Staff in accordance with CJCSC Instruction 3170.01B (reference (i)) to determine if there is Joint Requirements Oversight Council (JROC) special interest.

10.3 Acquisition

Over the last year, the Defense Acquisition System has undergone a series of changes in response to a variety of acquisition reform initiatives. These changes, including greater emphasis on acquisition management across families and systems-of-systems (SoS) within mission areas, has positioned the department to acquire NCW and Information Superiority capabilities.

10.3.1 Defense Acquisition System

System-of-systems policies and management processes must be developed in order to achieve an NCW Capability. Tradeoffs will be required among ASD (C3I) connectivity requirements, Warfighter requirements, and acquisition strategies and resources. The Office of the Undersecretary of Defense (Acquisition, Technology, and Logistics) (OUSD AT&L) will be at the center of performing these tradeoffs to ensure that adequate systems architectures are developed for these mission area capabilities while ensuring the use of commercial and industry technology to the maximum extent possible. As we incorporate a system-of-systems acquisition approach throughout DoD, there will also be a need to identify an acquisition transition from the existing legacy systems to the future NCW vision.

The Defense Acquisition System establishes a management process to translate user needs and technological opportunities into reliable and sustainable systems that provide capability to the user.[126] User needs and technological opportunities are defined as:

- **User needs:** Broadly stated mission needs responding to a postulated threat and developed in the Requirements Generation System or business needs responding to new ways of doing business and developed by the appropriate staff office.

---

[126] *DoDI 5000.2,* section 4.6.1.2.1.

- **Technological opportunities:** Developed or identified in the Science and Technology program based on user needs.

The Defense Acquisition System is a continuum composed of three activities with multiple paths into and out of each activity. First, technologies are researched, developed, or procured in pre-system acquisition (science and technology and concept development and demonstration). Second, systems are developed, demonstrated, produced or procured, and deployed in systems acquisition. The outcome of systems acquisition is a system that:

- Represents a judicious balance of cost, schedule, and performance in response to the user's expressed need
- Is interoperable with other systems (U.S., coalition, and Allied systems, as specified in the ORD)
- Uses proven technology, open systems design, available manufacturing capabilities or services, and smart competition
- Is affordable and supportable

Third, once deployed, the system is supported throughout its operational life and eventual disposal in post-system acquisitions using prudent combinations of organic and contractor service providers, in accordance with statutes.[127]

Information Superiority is defined and specifically addressed within the revised acquisition policies:[128]

> *Information superiority is defined as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority is achieved in a non-combat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives.*
>
> *Forces will attain information superiority through the acquisition of systems and families of systems that are secure, reliable, interoperable, and able to communicate across a universal IT structure, to include NSS. This IT infrastructure includes the data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities.*

---

127 *Ibid.*, section 4.6.1.2.2.

128 *Ibid.,* section 4.6.2.2.

For the DoD Components to provide these capabilities in a cost-effective manner, they must identify and evaluate IT (including NSS) infrastructure and supportability and interoperability from the beginning of each program's life cycle. This identification shall include appropriate system and family of systems requirements associated with critical infrastructure protection, IA, space control, and related missions that are consistent with DoD policies, standards (e.g., the Joint Technical Architecture), and mission-area integrated architectures. In addition, the evaluation of IT (including NSS) supportability and interoperability shall be documented in the C4ISP (reference (c)). The results of this planning shall be discussed in the system acquisition strategy.

As discussed above, the ability of the Defense Acquisition System to acquire NCW and Information Superiority capabilities is dependent upon the delineation of performance-based requirements. OUSD (AT&L) expects that requirements developers can improve the ability of the Defense Acquisition System to acquire NCW and Information Superiority capabilities, by adhering to use of performance-based requirements.

Recently, the OUSD (AT&L) engaged in the review and comment on selected requirements documents. One such document, directly related to the acquisition of NCW and Information Superiority capabilities, is the GIG CRD. Review of the GIG CRD by the Acquisition community, is one step taken to ensure that this capability is implementable from an acquisition perspective, and that the NCW and Information Superiority capabilities envisioned by *Joint Vision 2020* are achievable.

10.3.2 MCP Within Defense Acquisition System

The achievement of NCW and Information Superiority capabilities is also supported by other initiatives within the Acquisition community. As mission areas are defined within the department, the process for managing acquisition programs supporting the mission areas must be matured. Management of acquisitions across mission areas to achieve a capability implies the involvement of multiple systems developers and owners of legacy systems. The revised acquisition policy speaks, in multiple places, to this management, across Military Departments, Defense Agencies, and OSD Principal Staff Assistants (PSAs), of family-of-systems and SoS within mission areas. SoS acquisition management approaches are being developed and documented through review of existing SoS activities within the department and through selected pilot programs. An example is the Ballistic Missile Defense Organization (BMDO) and Joint Theater Air and Missile Defense Office (JTAMDO) Theater Missile Defense as a Family of Systems and SoS program. These programs include the Family of Interoperable Pictures (FIOP) activity and the TCT/Time Critical Strike (TCS)/Attack Operations (AO) Pilot. The FIOP and TCT/TCS/AO Pilot are discussed in greater detail in Appendix A5 to this report. The SoS management processes and templates to be developed from this effort will be available for use across the Department in the management of the acquisition of a capability for a given mission area. The processes

developed will support the MCP concept described earlier in this report and thereby contribute to the achievement of the *Joint Vision 2020* NCW and Information Superiority capabilities envisioned.

10.4 Science and Technology

Investments within the DoD and the Intelligence Community are being coordinated and directed toward Joint capabilities through a number of mechanisms. These include the coordination of research and development investments to ensure they are complementary and consistent with one another. These investments are targeted at Joint warfighting and national decision making needs and priorities. They also include Joint visibility and participation in warfighting experiments and demonstrations, research studies, advance technology laboratory efforts, and ACTDs that involve the Services, Agencies, and Unified Commands.

10.4.1 Defense S&T Coordination

In 1996, the Director of Defense Research and Engineering (DDR&E) improved the Defense S&T Reliance planning process by establishing a coordinating body that helps eliminate unnecessary duplication and seeks out opportunities for synergy, integrating the various Components programs into a corporate Defense S&T program. This new coordinating body is known as the Defense S&T Advisory Group (DSTAG). It provides advice to the Deputy Under Secretary of Defense (Science & Technology) on strategic planning, programming, budgeting, review, assessment, and oversight of the DoD S&T program. The three major tasks of the DSTAG are: (1) to guide the development of the Defense S&T planning documentation; (2) to review the results of the annual Technology Area Review and Assessments (TARA); and (3) to assist the DDR&E in formulating guidance for the S&T program in the Program Objective Memorandum (POM) and budget process. The DSTAG Committee consists of the following members:

- Deputy Under Secretary of Defense (Science and Technology), Chair
- Deputy Under Secretary of Defense (Advanced Systems and Concepts)
- Deputy Assistant Secretary of the Army (Research and Technology)
- Chief of Naval Research
- Deputy Assistant Secretary of the Air Force (Science, Technology, and Engineering)
- Deputy Director, Defense Advanced Research Projects Agency (DARPA)
- Chief Scientist, Ballistic Missile Defense Organization
- Deputy Director, Defense Threat Reduction Agency
- Deputy Director, Force Structure, Resources, and Assessment, Joint Staff (J-8)

The DSTAG Committee is comprised of organizations that oversee or execute the Defense Department's 6.1, 6.2, and 6.3 budget activities.

Four planning documents, depicted in Figure 10-1, detail how to implement the Defense S&T program: The Defense S&T Strategy, the Basic Research Plan (BRP), the Defense Technology Area Plan (DTAP), and the Joint Warfighting S&T Plan (JWSTP). These documents are a collaborative product of the Office of the Secretary of Defense, Joint Staff, CINCs, Military Services and Defense Agencies. The plans are provided annually to Congress and are fully responsive to the National Science and Technology Council's National Security Science and Technology Strategy and the Chairman of the Joint Chiefs of Staff's *Joint Vision 2020*. Although these plans do not assemble or display projects under the heading of NCW, many of the research and technology projects are key to the Department's quest to achieve NCW capabilities for our future defense forces.

Figure 10-1. Four OSD Planning Documents

10.4.2 Director for Central Intelligence's (DCI's) Advanced Research & Development Committee (AR&DC)

In 1998, the DCI established a process for ensuring that intelligence community's research and development investments are linked to mission needs and Information Superiority. The processes also ensure that the programs of its member agencies are coordinated and that sharing occurs across related efforts. The AR&DC is the formal

mechanism for this purpose and includes as members the Community Management Staff, OASD (C3I), DARPA, and the directors of research programs at each of the thirteen agencies of the Intelligence Community.

The AR&DC has established four thrust areas which serve to focus the National Foreign Intelligence Program's advanced research and development on key needs, and to exploit opportunities available through technical and scientific advances in academia, the national laboratories, and the private sector:

- Accessing Data and Information Anywhere, Anytime
- Producing Intelligence from Collected Data
- Enabling a Secure, Seamless Intelligence Information Infrastructure
- Revolutionizing the Intelligence Business

These thrust areas support the concept of NCW for the Defense Department's warfighters and decision makers.

10.4.3 Advanced Battlespace Information System (ABIS)

In 1996, the Joint Staff Director for C4 Systems (VADM Arthur Cebrowski) and the DDR&E (Dr. Anita Jones) led the Advanced Battlespace Information System study. The ABIS study report documented how emerging information technologies could be used to provide the warfighter with the significant new capabilities articulated in *Joint Vision 2010*. This report acknowledged the fact that achieving success in future combat relies upon our ability to rapidly acquire, disseminate, and utilize knowledge of the three-dimensional battlespace at all echelons by means of a global information system with assured services. The Information Superiority chapter of the JWSTP reflects current S&T activities that originated as a result of the ABIS report. In addition, many Information Superiority-related activities are contained in other chapters on Combat Identification, Space Protection, Hard and Deeply Buried Target Defeat, and Theater Missile Defense.

10.4.4 Implications of NCW on Science and Technology

The NCW concept emerged shortly after the ABIS report, underscoring time as the essential fourth dimension to future battlespace information. The fundamental components of NCW—GIG, networked sensors, and networked intelligent forces with competent and motivated people—extended beyond the ABIS report by introducing the need for technology and equipment, doctrine and tactics, and organizational structures to evolve together (co-evolution) to leverage information to generate increased combat power. NCW challenges science and technology to more closely integrate human engineering into traditional system and equipment development. From an NCW perspective, Defense Department science and technology efforts need to leverage applicable commercial technology and commercial

practices, invest in both social science and physical science research and technology that commercial sector won't provide, and engage with the user community in experimentation, demonstrations, and accelerated fielding initiatives.

10.4.5 Current DoD S&T Investment Strategy

The DoD S&T investment strategy has been structured in order to achieve the capability of information superiority as defined by the Joint Staff in *Joint Vision 2020* and the Joint Warfighting Capability Objectives. The S&T challenges that face the DoD in achieving information superiority were evolutionary enhancements of the Advanced Battlespace Information System (ABIS) study, and are currently defined in three operational capability elements in the JWSTP: battlespace awareness, effective employment of forces, and the GIG. See Figure 10-2.

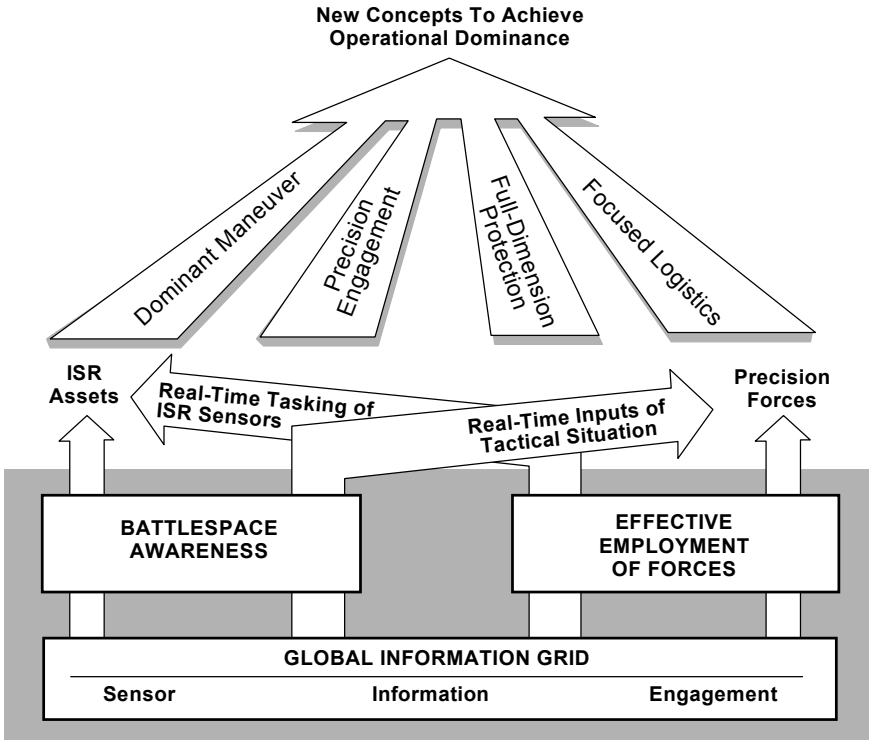


Figure 10-2. The Concept of Information Superiority as Described in the JWSTP

Within those broad capability areas, the crucial elements needed for the integrated, dynamic decision making and execution for Network Centric Operations are:

- Vastly improved and SSA and understanding

- Dynamically adaptive and coordinated planning and decision making
- Dispersed, self-synchronizing forces swiftly achieving desired effects

10.4.6 Science and Technology Challenges

Major science and technology challenges must be met to provide the technology to equip NCW forces of the future, including the following:

- Research/Technical/Operational
  - Establish the network to serve all users
  - Move information as required, within the constraints of the network
  - Help users cope with the enormous increase in quantity and variety of available information
  - Manage the grid resources to meet priorities
  - Provide adequate protection and accessibility of information and services to the diverse set of users
  - Support applications that users need to accomplish their tasks
- Leadership/Management
  - Synchronizing the development of military strategy and doctrine with the advances in technology and with the technology insertion process
  - Connection to NCW experimentation
  - Connection to mission capability packaging
  - Faster, synchronized technology insertion

10.4.7 Beyond Science and Technology: Co-Evolution of Technology, Doctrine, and Organization

It should be noted that continued S&T investment in the areas identified in Section 10.4.8 is necessary to bring the DoD closer to NCW, but insufficient in and of itself. Technology and concepts derived from focused NCW research must be accompanied by changes in the doctrine, procedures, training, and organizations involved in planning and conduct of Joint operations. To implement NCW, the DoD needs to focus on NCW co-evolution experimentation in the areas of SSA and self-synchronization, accompanied by richly integrated Intelligence, Surveillance, and Reconnaissance (ISR), and directly connected to

streamlined fielding and implementation. The concept[129] of NCW permits a new, more holistic view of both strategic and tactical level of operations, rather than single platform, weapon, or sensor views. This unified perspective means you don't have to do everything on every platform, every sensor, or every system. In addition, there will not be one physical "network" used to provide this holistic view of the battlespace, but rather a mix of many separate networks, data sources, and processes. The fine balance of obtaining, interpreting, and disseminating the right information, to the right warfighters and decision makers, in a timely manner, is the challenge facing both the technologist and the operator.

10.4.8 NCW S&T Focus Areas

To be able to achieve these capabilities and to implement NCW, the Department will need to focus.

- **Seamless, robust connectivity and interoperability.** Developing the technologies and procedures to assure a warfighter's access to all forms of information whenever needed, and for any type of mission, mounted or dismounted. Focus is on antennas, networking technologies, network management, and wireless technology developments.
- **Information management and distribution.** Developing the technologies and procedures for providing the right information at the right time to help the warfighter and their support organizations carry out missions and tasks. Focus is on intelligent information management and interaction products for use of multimedia information from heterogeneous sources.
- **Information Assurance.** Developing the technologies and procedures that provide high confidence that information available to the warfighter is protected, available when needed, and can be trusted (includes capabilities for defensive information warfare and access control based on agreed security and need-to-know requirements). Focus is on (1) the ability to protect DoD information, systems, and networks from attack, (2) the capability to detect information warfare attacks in real-time, and (3) the ability to react quickly to ensure mission critical information is available, correct, and secure.
- **Operationally responsive and reliable network resources and services.** Developing the technologies and procedures for the control of computing and

---

[129] Vice Admiral Arthur K. Cebrowski, and Roger W. Barnett; "Network Centric Warfare: An Emergent Military Response to the Information Age," presentation to the 1999 C2 Research and Technology Symposium, Naval War College, Newport, R.I., June 29, 1999. "As a concept, it [NCW] cannot have a precise definition, because concepts and definitions are like matter and anti-matter. Thus if a concept can be defined, it is no longer a concept."

communications resources for optimal performance in support of operational needs and priorities, including graceful degradation and ability to view the grid capabilities in terms of operational implications. Focus is on autonomous software, advanced software technology, embedded computing architectures, and persistent power supplies for the mobile user.

- **Information integration, presentation, and decision support.** Developing the technologies and procedures for processing raw sensor data, other intelligence information, and own information into a form that facilitates rapid and accurate decision making and the rapid formulation, updating, and direction of action plans. Focus is on the ability to provide for continuous predictive planning and the interoperability between simulations and live C4ISR systems for supporting mission planning, rehearsal, and training.
- **Distributed collaborative support.** Developing the technologies and procedures that provide the applications and services that allow dispersed users to share information, to consult and agree on information, and to develop courses of action. Focus is on common, modular elements that connect Joint mission planning, rehearsal, execution monitoring, and common pictures of the battlespace that support real-time operations.

10.4.9 S&T Projects Addressing NCW

Appendix F contains a sample list of Defense Technology Objectives (DTOs) that address each NCW focus area. Appendix G contains a sample list of analyses, experimentation, and ACTD activities that address multiple NCW focus areas. These activities are being conducted by Services, Agencies, and Unified Commands of the DoD.

10.4.10 Investment Areas Needed for NCW

Science and Technology is needed to allow network-centric concepts and processes to be implemented for integrated force battle command, including vertical and horizontal coordination and self-synchronization within and across warfighting and support functional areas.

- Data transport technology
  - Transmission systems/data links
  - Networking
- Information dissemination management technology
  - Interoperability software
  - Information access and delivery software

  - Computer-aided reasoning for task/simulation oriented dissemination
  - Adaptive, value-based, distributed data base replication
  - Information discovery
  - Optimization in dynamic environments
- Distributed computing infrastructure
  - Electronic devices and components
  - Networking computing services
  - Power devices
- Co-operative processing/decision support technology
  - Sensemaking processing
  - Information integration (i.e., fusion & correlation) software
  - Computer-aided reasoning
  - Co-operative software agents
  - Heterogeneity mediation agents
  - Optimization software (for QoS)
- Human-machine interface
  - Fundamental functions
  - Visualization
  - Natural language interface
  - Explanation agents
  - Alerting and cueing agents
  - Knowledge elicitation agents
  - Hands-free human-system interface
  - Input/output for a stressing environment
- IA/security technology
  - Network security software and protocols
  - Network security hardware for mobile users

  - Adaptive, polymorphic information access
  - Intrusion detection, assessment, and response
  - Insider threat detection and response
- Information integrity technology
  - Estimation and inference engines
  - Presentation/understanding of integrity
  - Confidence & uncertainty
- Rapid, distributed modeling and simulation for "what if" analysis and information management
  - Robust stochastic algorithms and processes
  - Automated learning
  - Distributed intelligent agents
- Information representation technology
  - Processes
  - Data
  - Metadata
  - Architectures
  - Policy
  - Pedigree
  - Ontologies
  - Semantic relationships

10.4.11 Leveraging Commercial IT

The S&T investment areas identified in Section 10.4.10 are leveraging state-of-the-art commercial products and developments while simultaneously developing and operationalizing next-generation militarily essential technologies. The results can be brought to bear on DoD problems through co-operative and participatory efforts to set standards and establish policy. Costly DoD-specific development can be avoided with the amortization of costs across government and commercial communities. However, there are unique military aspects of C4ISR and modeling & simulation that must be strongly influenced or directly

developed by DoD. In particular, developing the capability to reliably communicate among numerous, widely dispersed mobile sites operating in actively hostile environments, identifying friend and foe, achieving information security, and meeting the requirements for military-unique processing and decision support systems will not be achieved without signification DoD support. The information systems technology acquisition strategy is necessarily a pragmatic one—identify the pivotal issues, capitalize on commercial development whenever possible, leverage development in areas with special military aspects, and sponsor programs in technologies with unique DoD interest that would otherwise not be available to meet DoD needs.

10.5 Investment Strategy

Achieving a NCW capability will require changes in the patterns of DoD investments and expenditures. While the specifics of the changes required will not be fully understood for quite some time (some of these changes are currently being debated in the ongoing QDR and will be considered in future QDRs), the nature of the changes necessary are understood today.

First, these changes will not be confined, or even primarily focused, on the things we acquire. An NCW capability requires changes in all three domains of warfare, changes in how we think about accomplishing missions as much as changes in the material we employ. Changes, processes, information flows, organizational structures, and command approaches are central to NCW. These are enabled by (1) the skills and expertise of the men and women of DoD, (2) the availability of high quality information, and (3) the capabilities of our platforms, weapons, and logistics systems. Thus, to achieve an NCW capability, attention needs to be paid to warfighting concepts and organizations, education and training, information, and material. In other words, all of the components of a mission capability package. Not all of these changes involve more dollars.

Second, these changes are interrelated and inter-dependant in the effects they have on mission effectiveness. For example, how one might best approach a situation depends, in large measure, upon the nature of the uncertainty involved. The suitability of a particular form of organization depends upon what information is available, when it is available and to whom it is accessible. In terms of mission effects, investments spent on gathering information will not yield significant returns unless corresponding investments are made in a number of other areas; e.g., training and information distribution.

Third, synchronized changes will be required in both “investment” and “operating” accounts and investments will be needed in both “infostructure” and “force structure.” Putting together a mission capability package will require a balanced and coordinated set of investments/expenditures that transcend the traditional “colors” of money. Thus, in addition to all of the changes discussed above, changes in the way we think about budgeting and

oversight may be needed to facilitate visibility into these heterogeneous collections of investments/expenditures associated with specific mission capability packages.

Fourth, the enablers of NCW will need to receive increased attention, and in some cases, increased levels of investment/expenditures. The infostructure is the "entry fee" to NCW. Experimentation and research are needed to provide the intellectual foundation.

Fifth, platforms and weapons systems need to be "net ready" and may evolve in significant ways as new warfighting concepts emerge.

While it is clear that these changes will eventually involve or affect everyone and every organization and system in DoD, history shows that only a small fraction of the total force needs to be transformed to achieve dramatic effects. This makes it possible to achieve historic results in the near to mid-term with only a fraction of the resources needed to transform the whole force. The ongoing QDR and those that will follow in the coming decades will make the specific decisions regarding where actual dollars will go, but NCW has and will continue to shape the questions and serve as an organizing logic for the analyses of the alternatives.

Section 11

Current and Planned NCW-Related Initiatives and Programs

Making NCW a mature operational warfighting capability for the CINCs requires that the maturing NCW capabilities of the Services, as well as Allied/coalition partners, be effectively developed and integrated. The military Services describe their vision, concept development activities, and NCW development in terms of the requirements of *Joint Vision 2020*. Concept of Operation (CONOPS) development is necessary to transition from the physical and information domains of warfare to the cognitive. People may be able to fight and work more quickly, more efficiently, and more accurately if we automate the way they do their current job. They can fight and work **differently** if they develop new concepts for fighting or working. There is often a gap between stating requirements and developing systems, and the development of concepts. Different communities are involved, and people prioritize their resources differently. Currently, interoperability is an impediment to the development of mature NCW CONOPS.

There are a number of significant developments and ongoing initiatives within the Office of the Secretary of Defense, the Joint Staff, the Services, and the Unified CINCs that directly address interoperability, the foundation for information sharing, and a key enabler of NCW. In addition, there are key important developments and ongoing activities that specifically relate Allied/coalition interoperability and NCW.

This section provides an overview of:

- Significant developments and ongoing initiatives within the Office of the Secretary of Defense, the Joint Staff, Joint Forces Command, and the CINCs relating to interoperability and NCW
- Important initiatives and developments relating to Allied/Coalition Interoperability and NCW.

11.1 OSD Initiatives

Within the Office of the Secretary of Defense, there are a number of significant developments and ongoing initiatives that directly support interoperability and are directly related to NCW. An overview of key developments and initiatives is provided in this section. The Appendices also contain an extensive discussion of Service and Agency initiatives and programs.

- Global Information Grid (GIG): A detailed discussion of the GIG and ongoing GIG policies formulated to implement DoD Chief Information Officer responsibility under

the Clinger-Cohen Act was provided in Section 9. Service and Agency activities in support of GIG are described in detail in Appendix D.

- Family of Interoperable Pictures (FIOP): FIOP addresses the lack of an integrated and coordinating effort that goes beyond SSA to battle management, to include fire support, logistics, maneuver, intelligence, and other capabilities. Currently, no coherent view of the battlespace from the CINC level to the firing unit exists, which creates an inability to prosecute a coordinated strategy. Individually conceived and developed systems, along with constantly changing missions, new coalition partners and stove-piped intelligence dissemination, have created a disorderly web of corresponding systems. FIOP addresses the needed horizontal and vertical system interoperability across the service lines and between command echelons. FIOP is a coordinated initiative between OUSD (AT&L), the Office of the DoD CIO, and a multi-Service working group to define and establish a program governance structure for Joint interoperability. The FIOP initiative is relatively new, and must be well coordinated with GIG to assure they are mutually supportive. Air Force reports (Appendix C, paragraph 4.3) Joint Service efforts that implement three phases of FIOP Increment One and recommends the Multi-Service C2 Flag Officer Steering Committee (described in Appendix E, paragraph1.5) assume ongoing responsibility for FIOP implementation.

- Single Integrated Air Picture System Engineer (SIAP SE): The Department has substantial evidence from operations and exercises that significant warfighting capability shortfalls exist in the Joint counter-air mission area. In October 2000, the USD (AT&L), the JROC Chairman, and the DoD Chief Information Officer chartered a SIAP SE Task Force responsible for the systems engineering needed to build and maintain a SIAP capability. SIAP provides the warfighter the ability to better understand the battlespace and employ weapons to their designed capabilities. SIAP will support the spectrum of offensive and defensive operations used by U.S., Allied, and coalition partners in the airspace within a theater of operations.

  The direct involvement of Service personnel in the SIAP SE indicates a level of commitment to find ways within the Service Title 10 responsibilities to improve the quality of the Joint air picture. Navy activity supporting SIAP is described in Appendix E, paragraph 3.8.3. Air Force activity is described in Appendix E, paragraph 5.2.5. This initiative has strong Service participation through Navy's Common Command and Decision program described in Appendix E, paragraph 3.8.2. Air Force interoperability work described in Appendix E, paragraph 5.3.3 supports SIAP definition and implementation. Navy Cooperative Engagement Capability described in Appendix E, paragraph 3.8.6, is conducting Joint testing to explore the benefits of these systems in a Joint Composite Tracking Network, described in Appendix B, paragraph 5.4. Marines report a coordinated acquisition program with Air Force to develop and field a Theater Battle Management Core System. U.S.

Marine Corps activity is described in Appendix E, paragraph 4.5.3.3. Air Force work is described in Appendix E, paragraph 5.3.1.1.

- SoS Pilot for TCS/TCT: The lessons learned during *Operation Allied Force* indicate a critical shortcoming in the U.S. and Allied forces' capability to field enough C2 assets to decisively attack elusive mobile targets. Each of the Services is actively acquiring service-specific TCS/TCT capabilities. At present, there is no single, integrating effort to address a Joint systems architecture for TCS/TCT and to align/synchronize those systems from an SoS acquisition standpoint to achieve a Joint TCS/TCT capability. The SoS pilot for TCS/TCT will develop and refine the processes for managing the acquisition and development of a Joint TCS/TCS capability in a SoS context.

11.2 Joint Staff Initiatives

- Joint Mission Areas/Joint Operational Architecture: The Joint Operational Architecture: The Chairman of the Joint Chiefs of Staff (CJCS) approved[130] a fully coordinated definition of JMAs for the Joint Operational Architecture (JOA). This document provides high-level direction for development, in conjunction with the Services and Agencies, of an operational architecture that establishes a framework for understanding and Agency support and can become the basis of Joint Mission Capability Packages.
- Joint Warfighting Capability Assessments (JWCAs): The Joint Staff conducts Joint Warfighting Capability Assessment studies that address key interoperability issues. Three studies that will be initiated in FY02 include: GCCS Interoperability, OCONUS Bandwidth, and Network Consolidation.
- JTF C2 Strategic Initiative: The JTF Command and Control Initiative is one of the CJCS's Strategic Initiatives and is focused on developing an enhanced operational architecture for JTF Command and Control.
- Focus on Interoperability: As cited in the Appendices, CJCS Instructions and Memoranda focus the attention of the Services on interoperability. A significant recent development was the approval of CJCS Instructions and Memoranda that place an increased emphasis on Key Performance Parameters (KPPs) for interoperability based on top level information exchange requirements.
- GIG Architecture Version 1.0. This architecture describes the operational and systems architecture for a selected Joint Task Force scenario. It also includes

---

130 General Henry Shelton, "Joint Mission Areas to Organize the Joint Operational Architecture", *CM-1014-00*, dated 6 September 2000.

scenario-independent systems architecture "templates" that can improve interoperability by encouraging common technical approaches at the interfaces between organizations, networks, and technologies.

- Network Operations (NetOps): The Joint Staff J6 is leading a network operations (NetOps) initiative to provide CINCs with SSA and management oversight of networks within their Area of Responsibility. This effort provides synergy between critical aspects of network management, information assurance and information dissemination management to give CINCs the ability to visualize their C4 battlespace, achieve positive control and greater security.

11.3 Joint Forces Command (JFCOM) Initiatives

- JFCOM Designation as the Joint Force Integrator: JFCOM was designated as the Joint Force Integrator on 1 Oct 1999 to support development and integration of fully interoperable system capabilities, including C4ISR for Joint warfighting.
- Joint Experimentation: The Commander in Chief, Joint Forces Command (JFCOM), is conducting Joint Experimentation. The relationship between Joint Experimentation and NCW was reported in their March 2001 report to Congress (attached as Appendix H).
- Joint Battle Center: JFCOM is also utilizing experimentation and testing by the Joint Battle Center to address CINC prioritized interoperability issues.
- Information Distribution and Management (IDM) CRD: JFCOM has developed the IDM CRD, which was approved by the Joint Requirements Oversight Council in January of 2001.
- Global Information Grid CRD: JFCOM has developed the Global Information Grid Capstone Requirements Document that is currently being staffed for Joint Requirements Oversight Council approval. Additional detail is provided in Section 10.
- All Service Combat Identification Evaluation Team (ASCIET): Through the ASCIET series of interoperability tests, JFCOM has identified critical deficiencies in the Services' C2 systems. This rigorous testing and critical reporting has resulted in the formation of the SIAP SE organization.

Other CINCs, notably USCINCPAC, have addressed interoperability issues that must be solved in order to move forward with NCW. USCINCPAC has established an Information Capabilities Framework that guides their investment strategy (PACWARNET). The investment strategy views Information Superiority as being enabled through network-centric enterprise, knowledge-centric infosphere, and Information Assurance to deliver SSA, Collaborative Planning and Execution, and Improved Decision Support.

In the Appendices, the Services and Agencies report extensive activity that focuses upon interoperability. The following paragraphs summarize this activity and provide reference to the location of the information in the appendices.

11.4 Service Experimentation and Interoperability

The Services report interoperability as a major thrust of their experimentation activity. Table 11.1 provides reference to the location of this information in the Appendices, with a brief note concerning the nature of interoperability experimentation reported. Appendix H contains JFCOM's report to Congress, noting the experimentation activity related to Joint Experimentation.

Table 11-1. Interoperability Focus in Service Experimentation

Appendix and Para	Activity Reported
B.1.4.2	Interoperability experimentation in Joint Contingency Force Army Warfighting Experiment
C.2.3.8	Interoperability as a focus in Navy Fleet Battle Experiments
E.3.2	Navy experimentation, initiatives, and programs report a consistent emphasis on interoperability as a major objective
F.1	Defense Technology Objectives emphasize interoperability in Objective #1
G.2	Airborne Overhead Interoperability Office experimentation
G.3	Joint Continuous Strike Environment experimentation by Army addresses strike systems interoperability
G.6	Hostile Forces Integrated Targeting System experimentation
G.7	JIVA Collaborative Environment/Joint Targeting Toolbox experimentation sponsored by U.S. Central Command
G.8	Joint Expeditionary Digital Information System & Mobile Satellite Systems experimentation by Marine Corps Warfighting Lab
G.12	PACOM Network Initiative
G.16	Precision Targeting Workstation/REDS experimentation by National Imagery and Mapping Agency and Navy

11.5 Systems Engineering and Interoperability

Services and Agencies report extensive systems engineering activity with interoperability as a major focus. The table below provides reference to the location of this information in the Appendices, with a brief note concerning the nature of systems engineering activity reported.

Table 11-2. Interoperability Focus in System Engineering

Appendix and Para	Activity Reported
B.1.4.3	Army C2 system interoperability initiative
B.4.2	U.S. Air Force acquisition transformation
B.5.2	Ballistic Missile Defense Office engineering and integration to support interoperability
B.5.4	System of Systems approach to facilitate interoperability of heterogeneous systems
D.2.3.3.2	Navy focus on interoperability in implementing GIG policies
D.3.2.2	U.S. Marine Corps use of Defense Information Infrastructure Common Operating Environment and Joint Technical Architecture to assure interoperability
E.2.2	Army design of Joint Tactical Internet to facilitate interoperability
E.2.3	Navy acquisition programs focus on interoperability
E.3.3.3	Navy initiative in Allied Interoperability
E.5.2.2	U.S. Air Force support for Family of Interoperable Pictures initiative
E.5.2.5	U.S. Air Force support for Single Integrated Air Picture initiative
E.5.3.3	U.S. Air Force programs support interoperability
E.6.3	Ballistic Missile Defense Organization support to Joint Interoperability Initiative
E.6.5	Ballistic Missile Defense Organization interoperability programs
F.1	Defense Technology Objective #1: Seamless, Robust Connectivity, and Interoperability

Appendix and Para	Activity Reported
G.1	Joint C4ISR Decision Support Center NCW Analysis
G.5	Hyper-spectral Imaging for Battle Damage Information and Battle Damage Assessment
G.10	Naval Fires Network
G.17	Joint Targeting Workstation

11.6 Service and Multi-Service Initiatives

A selected set of Service and Multi-Service Initiatives are highlighted below, with references to more detailed discussions in the Appendices.

- The Army's Ground Force Level Control CONOPS is designed to achieve interoperability through the automated exchange of infor mation at the tactical level in support of multinational, combined, and Joint operations. It creates the necessary operational architecture that bridges interoperability gaps by identifying Information Exchange Requirements for the Joint Mission Areas and subordinate Uniform Joint Task Lists. It will substantially improve force-level SSA and will support the definition of Communications and Information System materiel requirements that will transport this data and information. The Ground Force Level Control initiative is described in Appendix E, paragraph 1.5.
- The Multi-Service Command and Control Flag Officer Steering Committee described in Appendix E, paragraph 1.5, addresses interoperability among ground component elements. Involvement by general and flag officers indicates Service interest, and Joint Interoperability testing processes being worked in the FIOP initiative may provide metrics for progress.
- Joint Command Control Ship Payload work by Navy described in Appendix E, paragraph 3.2.11, is a ground-up effort to develop requirements, and operational and system architectures, for Joint requirements on a future Joint Command Control Ship. This effort is coordinated with GIG Architecture version 1.0, and should also be coordinated with the FIOP initiative.
- The Naval Fires Network described in Appendix E, paragraph 3.7.4, is a Navy program to automate the process of requesting and delivering fire support. Army Advanced Field Artillery Tactical Data System (AFATDS), described in Appendix E, paragraph 2.2, and Marine AFATDS described in Appendix E, paragraph 4.5.3.1, indicate work in progress on a similar capability. The Navy work should be coordinated with Army and Marine Corps work.

- Navy Command and Control Processor (C2P), described in Appendix E, paragraph 3.4.12, reports that the program is using the DoD Core Data Model. The Navy program does not specifically identify Joint Test and Evaluation events that will ensure interoperability of data translated by the C2P.
- Navy reports that the Multifunction Information Distribution Terminal (MIDS), described in Appendix E, paragraph 3.4.19, Low Volume Terminal (LVT) is being procured for many U.S. platforms, as well as Allied systems. MIDS program testing includes Link 16 interoperability testing, and is coordinated with the SIAP SE effort.
- BMDO reports in Appendix E, paragraph 6.3, ongoing support for Joint Initiatives involving air and missile defense capabilities.
- The Defense Intelligence Agency reports the establishment of the Interoperability Senior Steering Group (Appendix E, paragraph 10.3.2).

11.7 Allies, Partners, and Interoperability

11.7.1 Multinational Operations

NCW is, and will be, the most advanced form of interoperability for some time to come. However, when it comes to our Allies and partners, we must work basic interoperability first. Under the title of Multinational Operations, *Joint Vision 2020* captures the strategic challenges we face improving interoperability with our Allies and partners.

> *Since our potential multinational partners will have varying levels of technology, a tailored approach to interoperability that accommodates a wide range of needs and capabilities is necessary. Our more technically advanced allies will have systems and equipment that are essentially compatible, enabling them to interface and share information in order to operate effectively with U.S. forces at all levels. However, we must also be capable of operating with allies and coalition partners who may be technologically incompatible—especially at the tactical level. Additionally, many of our future partners will have significant specialized capabilities that may be integrated into a common operating scheme. The overall effectiveness of multinational operations is, therefore, dependent on interoperability between organizations, processes, and technologies.*

One of the fundamental issues confronting commanders in multinational operation is the sharing of information among participants. During *Operation Desert Storm,* the most likely method of communicating with an adjacent commander was through a liaison officer with a U.S. communications package. Some feel that, as we push forward to greater heights of harnessing Information Technologies to achieve Information Superiority, we may continue to outpace our Allies. We have a lot of work to do to improve basic interoperability with our Allies at every level, but interoperability is critical as a precondition for NCW. Two

principle aspects of information sharing in the context of interoperability are what to share and how to share it. Requirements for alliance information sharing are often based on treaty relationships and are difficult to generalize; however, there is significant effort to improve Allied interoperability that is focused on both aspects of information sharing. The Combined Communications Electronics Board (CCEB) and the NATO C3 Board provides steady and consistent pressure to improve Allied and coalition interoperability. Engagement by the operations communities (Joint Staff J-3 and similar Allied organizations) has assured that progress addresses substantive change as well as technical innovation. OSD and the Joint Staff are pursuing many strategic initiatives to improve Combined C4 interoperability. A few of the key ones are listed below:

- NATO's Defense Capability Initiative represents a major effort to accelerate the mobility, flexibility, lethality, sustainability, and survivability of Nations and NATO-committed forces. Ten of these initiatives focus on C4 interoperability.
- Joint Warrior Interoperability Demonstration 99 demonstrated CWAN enabling the U.S. to operate on a network with Allies employing GCCS with their national C2 systems.
- Chairman-directed JWID CWAN transition to the Combined Federated Battle Labs Network (CFBLNET) to conduct year-round CINC, Service, and Allied experiments and demonstrations and create a template for an operational CWAN for the CINCs.
- Work continues with key Allies on the Joint Tactical Radio Systems (JTRS), a family of digital, modular, and software-programmable radios, which will range from a low-cost Joint tactical radio to a higher-capability, Joint Multi-band, Multi-mode radio with Link 16 and Variable Message Format (VMF) Capability.
- DOD funded the Joint Interoperability Test Command to establish a combined interoperability test and standards program.
- The Joint Staff Directorate for C4 Systems is leading an effort to codify the security accreditation process for Multinational network connectivity to support warfighter requirements.
- In NATO, the NATO C3 Board's Interoperability Sub-Committee (ISC) is developing policy which mirrors U.S. DoD's "architectural" approach used to enhance interoperability, and the Information System Sub-Committee (ISSC) is developing a NATO C3 Technical Architecture along the lines of the DOD's JTA.
- Successful VTC between the five member nations of the CCEB (UK, NZ, CA, AS & U.S.). Non-secured multipoint VTC achieved. Secure Point-to-Point VTC testing partially completed and Secure multipoint VTC in progress. Additionally, a nonsecure alternate VTC bridge is under examination.

The services also are working on Allied and coalition interoperability. These efforts tend to be focused on Service missions or existing Service-to-Service relationships (AF, Navy, or Army).

11.7.2 CINC Interoperability

CINCs have also established initiatives for Allied interoperability that are employing a number of technical solutions to address key interoperability challenges that exist within each CINCs area of responsibility. Examples include U.S. European Command's Linked Ops/Intel Centers Europe (LOCE), U.S. Central Command's Proof of Concept for a Coalition Wide Area Network (CWAN), U.S. Southern Command's fielding of the Caribbean Information Sharing Network (CISN) in conjunction with twenty Caribbean nations, and U.S. Pacific Command's implementation of the Multi-Domain Dissemination System (MDDS), which is discussed in some detail below.

The MDDS is being developed for the Commander in Chief, United States Pacific Command (USCINCPAC) and the Joint Intelligence Center Pacific (JICPAC) to provide an accreditable multilevel system suitable to disseminate processed intelligence information at different sensitivity levels throughout the Pacific theater. The MDDS is intended to be an intelligence product repository widely accessible by U.S. and coalition partners in the Pacific Theater via multiple networks. MDDS will consolidate as many as possible of the multiple Web servers currently being used into one server. In addition, the MDDS will support the dissemination of information to newly formed partnerships (e.g., to coalitions). JICPAC intends to use the MDDS as a repository and dissemination point for processed intelligence products.

Within U.S. Pacific Command, United States Forces Korea (USFK) has developed the capability to provide GCCS-K access to the Republic of Korea (ROK) Army, which provides a common operating picture (COP) for multinational operations in the Korean AOR. This results in critical new efficiencies during planning and execution of the USFK mission to defend South Korea.

11.7.3 Tactical Communications Post 2000—A Future NATO Initiative

International peacekeeping operations in the Persian Gulf, Somalia, Bosnia, and Kosovo repeatedly demonstrated that future military operations need to be multinational efforts. As a result, support is increasing for improved interoperability among NATO and Coalition partners.

A group of NATO nations realized that improving the level of interoperability among their tactical communications systems was essential for the success of future military operations. Achieving interoperability has been costly and inefficient due to lack of standardization and cooperation among the NATO nations during the development of their

communication systems. Interoperability can best be achieved if addressed early in the development cycle, before being locked into a specific system or architecture.

The Tactical Communications (TACOMS) Post 2000 project began as an effort to identify common standards that could be implemented by the NATO nations during system development and save costs needed to retrofit legacy systems. The project objective is to produce the next generation of NATO Standardization Agreements (STANAGs) for land combat zone tactical communications.

Current switched tactical communications systems of NATO nations obtain the majority of their interoperability via communications gateways such as defined in STANAG 5040 for the analog gateway and the STANAG 4206 series for the digital gateway. Due to the cost and technical limitations, the interoperability provided by these gateways is generally restricted to basic voice and data services.

NATO nations need tactical communications systems that use new technologies and are fully interoperable without the use of gateways. This has been the objective of the TACOMS Post 2000 project since its inception: seamless interoperability without gateways, using commercial standards to the maximum extent possible, not only between tactical networks, but also with strategic networks and, where possible, civilian networks.

The problem facing NATO is how to integrate national systems that have significantly different implementation time scales. To overcome this problem, PG/6 developed a concept in which the NATO nations would jointly produce new communication standards that would provide sufficient technical detail to allow national industries to produce their own compliant systems. Each nation would then evolve their existing and soon-to-be-fielded systems toward common standards, thus progressively enhancing NATO's communications interoperability.

The TACOMS P2K System Architecture is composed of four subsystems, the Local Area Subsystem (LAS), Wide Area Subsystem (WAS), Mobile Subsystem (MS), and the System Management and Control Subsystem (SMCS). Both the wide area and local area subsystems share a common transport network layer.

The LAS is designed to support local communications of a self-sustained community in a geographically restricted area. The topology is that of a local area network as a backbone, with the use of asynchronous transfer mode technology (ATM) for switching via private automatic branch exchanges (PABX) or on the local area network. The transmission media will be fiber optic cable with transmission rates in the gigabit-per-second range, and also via wireless technologies. For the transition period, standard twisted pair cable will be used. For access to the network, the user will have a wide range of voice (digital and analogue), data, and multimedia terminals from which to choose.

The WAS provides a transit function to LAS users over the long-haul tactical transport system using fiber optic cable, radio, and satellite links. The topology is a mesh of nodes at greater distances than in the LAS, with ATM as the switching technology. The transmission media will be combinations of fiber optic cable, terrestrial radio, and satellite communications. Access to the WAS will be from direct subscriber terminals as in the LAS, or from the LAS directly, the mobile subsystem, the NATO strategic network, and national and commercial networks. The WAS will support both the Integrated Services Digital Network (ISDN) and the Broadband ISDN.

The MS is designed with radio links supporting mobile operations and is, essentially, a network built on combat net radio (CNR) nets, Single Channel Radio Access (SCRA) points, Packet Radio Networks (PRN), and cellular phone technology. The PRN will use Internet Protocols for packet data services. Radio access points (RAP) provide the connectivity between the MS and both the WAS and the LAS. The use of ATM switching in the RAP provides connectivity from any user to any user, regardless of intervening transmission media or user terminal. The MS will operate in the VHF, UHF, and SHF frequency bands.

The SMCS performs the network management function, to include fault management, performance management, accounting management, configuration management, security management, and compliance to International Telecommunications Union (ITU) Standards for interoperability and compatibility with other networks.

A Multilevel Security Subsystem will be implemented that will provide for end-to-end encryption for transmission of information above the NATO Confidential level. Bulk encryption will be used on all trunks, and link-by-link encryption will be used in the mobile subsystem.

In summary, this project will lead to the development of a seamless network that will allow any user on any terminal to connect to and interoperate with any other user in the system. Mobile subscribers can connect into the network from any location via a wide distribution of radio access points, much like the ubiquitous cell phone towers. The system design remains open and thus amenable to the employment of new technologies. Furthermore, the architecture allows nations to transition into the new system by providing for backward interoperability with current national systems and technologies.

11.7.4 Summary

There are many initiatives in progress to improve multinational operations at tactical, operational, and strategic levels. These efforts are managed by organizations, such as the Multinational Interoperability Council (MIC), Combined Communications Electronics Board (CCEB), NATO C3 Board, and many more. Interoperability is the number-one focus, but for some of our closest Allies, we will achieve some degrees of NCW. Other examples of interoperability and aspects of NCW with our Allies will be seen throughout this report.

Requirements for alliance information sharing are often based on treaty relationships and are difficult to generalize. Science and Technology investment will provide improved technology, but a change in system engineering focus is required. GIG Architecture Version 1.0 addresses coalition interoperability in the context of an approved Commander in Chief, U.S. Forces Central Command Operation Plan, and may provide the system engineering focus for future progress in this area.

11.8 Assessment

The foregoing discussion in this section indicates there is reason for optimism that OSD is providing effective mechanisms to promote CINC, Service, and Agency cooperation in developing NCW capabilities as an enterprise. However, there is also room for improvement. Specifically:

- MCP Development. DoD will develop MCP definitions that align with Joint Mission Areas, but does not have MCP definitions for Services and Agencies to use in ongoing development. This is required to give a system view of requirements and architecture.
- Infrastructure. Infrastructure is of concern to the Services and Agencies; they all have modernization programs. DoD efforts to bring infrastructure modernization within the Defense Information System Network (DISN) do not appear to have much traction in Service program planning. Air Force reports (Appendix B.4.2) that the Electronics Systems Center has been given responsibility for integrating the fielding of the Air Force C2 Enterprise, implementing a concept of network-centric acquisition. Navy reports (Appendix E.3.4.7) the development of an Expeditionary C5 Grid as a mission capability package for C4 and Combat System programs, integrating existing programs of record to enhance Battle Force C2.
- Personnel. Army reports (Appendix A.1.1) ongoing work on remote training. Navy reports (Appendix D.2.3.3.4) restructuring of an end-to-end approach to enlisted personnel training and organization to respond to changing operational and technology needs. Marines report (Appendix D.3.3.2) realignment of enlisted Military Occupational Specialties and officer categories for the same purpose. Otherwise, people programs are not an important theme in Service and Agency initiatives. Navy's Web-Enabled Navy (WEN) initiative (reported in Appendix E.3.3.5) addresses improvements in Navy civilian and military personnel systems, but this is not a central focus of the initiative.
- Joint Test and Evaluation. Each Service and Agency describes their test and evaluation process, both in connection with process and systems. None of the

Service or Agency inputs mentions the role of the Joint Interoperability Test Command.[131]

[131] *Chairman of the Joint Chiefs of Staff Instruction 6212.01B*, *DoD Directive 4630.5*, and *DoD Instruction 4630.8* establish requirements for JICT to certify interoperability of C3I systems.

Section 12

Findings and Conclusions

This section presents DoD's findings and conclusions with respect to our current and future ability to understand and conduct Network Centric Operations. To put things into perspective, NCW is no less than the embodiment of DoD transformation. It is a monumental task that will likely span a quarter of a century or more. It will involve ways of operating that have yet to be conceived. It will employ technologies yet to be invented. It will increase warfighting capabilities more than all the advances that have been made in the history of warfare to date. In this context, the many and varied activities that are currently underway in the pursuit of network-centric capabilities may seem clumsy and lacking in sophistication, but these activities represent an enormous acceleration in the short period of time since the concept of NCW began circulating within DoD and the Defense community. Compare this with how long it took for the capabilities inherent in the ARPANET to gestate before catching hold and resulting in the Internet. The gestation period for Network Centric Warfare has been far shorter then that of the ARPANET and the head of steam that is building promises accelerating progress for years to come.

This is not to say that there are no impediments to progress; in fact, there are some significant impediments that need to be removed from the road ahead. Nor is it to say that there is nothing we can do better to foster more creativity and synergy; there most certainly is. Rather, it is meant to put the findings and conclusions of this report into proper context—to realize that the glass is filling and that the fill rate is increasing. It is also to communicate the fact that the glass itself is growing larger with every passing day and that continued focus and commitment will be needed if we are to be able to fully take advantage of the opportunities that network-centric concepts and advancing information technologies offer.

DoD is committed to removing the impediments to progress and to developing a culture that will encourage, nurture, and protect potentially disruptive innovation to enable a network-centric transformation of the Department.

12.1 Findings

The following findings speak to the status of our efforts to make NCW a reality.

1. There is compelling evidence that supports the theory of NCW.

   Joint and Service experiments, exercises, analyses, and simulations have compiled an impressive amount of data that supports hypotheses that link a robustly networked force to various attributes of mission success. Evidence points to the ability to:

   (a) Increase the quality of the information available by networking sensors

(b) Better understand a situation as a result of the sharing of information

(c) Respond more rapidly because of increased awareness

(d) Synchronize actions both by more dynamic planning and execution and by self-synchronization

(e) Achieve higher levels of lethality and survivability with less risk and fewer resources

2. Progress has been made in developing an understanding the basics of network-centric concepts and their ability to contribute to mission success.

   Although NCW currently means different things to different people, these differences, more often than not, involve different forms of Network Centric Operations (e.g., networking of sensors, collaborative planning, dynamic planning and execution) rather than disagreements about the basic concepts. When one goes beyond the labels, one finds more agreement than that is sometimes apparent. Given that the theory of NCW is only a couple of years old, the level of awareness within DoD and the Defense community is remarkably high, the theory is developing nicely, and applications abound.

3. Applications to date of NCW theory have barely scratched the surface of what is possible. However early experimentation by JFCOM and the Services have provided significant justification for Congress to continue investing in the development of NCW as the cornerstone enabler of future combat forces.

   There are two interrelated reasons for the limited nature of the NCW applications today. The first is the fact that DoD has yet to field an infostructure with sufficient interoperability to foster synergies among organizations that do not traditionally work together. This is analogous to the situation that kept the possibilities inherent in ARPANET technology at bay for over 20 years before they were transformed into the Internet. The second is that, despite a theory that has far reaching implications for DoD CONOPS and organization, the applications to date represent “safe” excursions from existing processes and relationships. They resemble the first applications of computers in the 1960s that automated then-existing processes by making minimal modifications to existing processes within the real or perceived constraints imposed by organizational boundaries and doctrine. With rare exception, they avoid threatening institutional arrangements. Service applications are primarily focused inward; those that include other Services are facilitating existing roles rather than exploring new ones. They represent an embrace of sustaining innovation rather than a pursuit of what is possible.

4. There are significant impediments to progress.

The lack of adventure displayed to date in developing network-centric concepts and applications may be traced to the existence of a formidable collection of impediments to progress. These include:

(a) Lack of appreciation for what is possible technologically

(b) Lack of existing interoperability to serve as an example and harbinger of future interoperability

(c) Lack of progress toward an infostructure that achieves the levels of connectivity and interoperability needed to support Network Centric Operations

(d) Acquisition processes and practices that are unable to keep pace with advancing technology or fully exploit commercial capabilities

(e) Disconnect between the requirements and experimental processes

(f) Disconnect between experimental and acquisition processes

(g) Process that does not adequately support the co-evolution of mission capability packages

(h) Lack of incentives and plenty of disincentives to disruptive innovation

(i) Lack of understanding of the basics of experimentation, including the design, conduct, and collection and analysis of experimental results

(j) Lack of a strategic plan expressed in terms of network-centric hypotheses

(k) Lack of organizational focal points in OSD, the Services, Agencies, and the Joint community to promote and assist with the attainment of network-centric capabilities

12.2 Conclusions

The following are the conclusions drawn from an assessment of progress to date and the impediments to progress that have been identified.

1. In the future, the network will be the single most important contributor to combat power.

   The nature of the NCW applications will mature with increasing focus being paid to "born-Joint" operations, new command concepts, and self-organizing forces.

2. There is considerable and growing urgency associated with removing any impediments to progress.

   In sum, the impediments identified constrain us in two ways. They limit our ability to conceive of truly transformational applications and they limit our ability to turn

ideas into real capability. It has taken just over two years to create widespread awareness about the possibilities inherited in NCW. Initial applications have and will continue to provide the concrete evidence needed to convince the rest of DoD that NCW is the future. We have already progressed to the point where the leading edge of ideas has outstripped our ability to implement them because of one or more of the impediments. As time goes by, the backlog of good ideas will grow and, with them, increased frustration at a lack of progress. The ranks of the discontent will continue to grow by a continuing stream of evidence. As more and more ideas are placed on hold, the seed corn of the transformation is wasted, and the production of future seed corn is adversely affected. This makes removing or mitigating existing impediments to progress of increasing importance and urgency.

3. Timely removal (or mitigation) of the impediments to progress will be greatly facilitated by an OSD-level Office of Transformation to develop, and then help implement, a "transformation" of DoD business practices to enable a network-centric transformation of the Department.

   The process of assembling this report and a review of the visions, initiatives, and activities of Services and Agencies highlights the uneven nature of NCW awareness and progress on NCW applications. In addition, the lack of an obvious focal point in many organizations and the lack of shared SSA of similar and related activities, point to the need for a mechanism to promote the coalescence of organizational visions; the identification of appropriate focal points; the exchange of information; and the fostering of collaborative research, analysis, experimentation, and development of network-centric MCPs.

4. A goal to achieve a specific network-centric capability by a specific date is needed.

   Even a cursory reading of the annexes to this report shows the large disparities in progress among organizations and the lack of progress on truly Joint network-centric concepts of operation. With nothing but a general vision to guide them, each organization will develop its own sense of urgency and its own priorities. The result will be that the force will take a long time to achieve a mature network-centric capability. DoD needs to establish mission specific goals for both the infostructure and the nature of network-centric capabilities to be achieved by a certain date. Working back from this date, interim milestones could be established and progress tracked.

5. NCW offers unprecedented promise to achieve long-sought-after capabilities without corresponding increases in resources *in the long run.*

   Being able to use all of the available information and being able to bring all available assets to bear rapidly in response to a dynamic situation directly affects the efficiency of operations. Increased lethality and survivability combine in a positive feedback

loop to achieve greater levels of productivity. The multiplicative nature of the NCW value function represents increasing returns on investments made in networking the force and in learning how to capitalize upon a networked force with its SSA and ability to collaborate and self-synchronize. All of this offers us the opportunity to get more out of our investments in "net-ready" platforms. Rapid deployments, small in-theatre footprints, and low collateral damage are all by-products of network-centric concepts and network-centric capabilities. There is a legitimate question about whether or not there is a need, in the short run, for increases in the budget to affect this transformation of the force. In theory, one might argue that a realignment of priorities is all that is needed. However, in practice, additional investments in the short run may be required to achieve a critical mass of network-centric capabilities sufficient to demonstrate the power of joint NCW capabilities and, therefore, affect a realignment of investment patterns. Given the evidence to date, it is clear that a given level of warfighting effectiveness can be obtained with fewer resources if the force embodies mature network-centric concepts and capabilities. Thus, in the long run, it should not cost more to operate a network-centric force than a platform-centric one. A lot will depend upon developing new approaches to persistent military problems (e.g., critical mobile targets) that leverage the power of a networked force rather than the power of stand-alone platforms. Certainly an appropriately focused increase in the top line would help remove key impediments to transformation more quickly.

6. NCW and NCO should be the cornerstone of the Department's strategic plan for the transformation of the forces.

   NCW and NCO offer order-of-magnitude improvements in almost every importance dimension of interest. The success of these concepts is not dependent upon a particular geopolitical future or a particular set of scenarios. NCW and NCO go to the heart of how well an organization is equipped to handle uncertainty, dynamically unfolding situations, asymmetrical attacks, and day-to-day operations. NCW and NCO allow DoD to reap the full benefits of its more importance resource—its people—by giving them what they need to do their job; i.e., high-quality awareness and the freedom to utilize this awareness to accomplish the varied tasks at hand.

Glossary

AADC	Area Air Defense Commander
AAFIF	Automated Air Facilities Information File
AAMDC	Air Assault Missile Defense Command
AAW	Anti-Air Warfare
ABA	Adaptive Battlespace Awareness
ABCCC	Airborne Battlefield Command & Control Center
ABCS	Army Battle Command System
ABIS	Advanced Battlespace Information System
ABL	Airborne Laser
AC2ISRC	Aerospace Command and Control & Intelligence, Surveillance, and Reconnaissance Center
ACA	Airspace Control Authority
ACADA	Automatic Agent Detector Alarm
ACAT	Acquisition Category
ACETEF	Air Combat Environment Test and Evaluation Facility
ACS	Aerial Common Sensor
ACTD	Advanced Concept Technology Demonstrations
ADA	Air Defense Artillery
ADOCS	Automated Deep Operations Coordination System
ADRP	Army DISN Router Program
ADSI	Air Defense System Integrator
ADUA	Administrative Directory User Agent
AEA	Airborne Electronic Attack
AEF	Expeditionary Aerospace Force
AESA	Active Electronic Scanned Array
AFATDS	Advanced Field Artillery Tactical Data System
AFOTEC	Air Force Operational Test and Evaluation
AIS	Automated Information System
AMC	Advanced Mission Computers
AMC&D	Advanced Mission Computer & Display
AMDWS	Air and Missile Defense Work Station
AME	Air Mobility Element
AMHS	Automated Message Handling System
AMU	Air Mobility Unit
ANGEL	Active Network Guidance and Emergency Logic
ANS	Advanced Narrowband System
AO	Attack Operations
AoA	Analysis of Alternatives
AOACMT	Attack Operations Against Critical Mobile Targets

AOC	Aerospace Operations Center
AODA	Attack Operations Decision Aid
AOR	Area of Responsibility
APB	Acquisition Program Baseline
AR&DC	Advanced Research & Development Committee
ASAS	All Source Analysis System
ASC	Aeronautical Systems Center
ASCIET	All Service Combat Identification Evaluation Team
ASUW	Anti-Surface Warfare
ASW	Anti-Submarine Warfare
ATACCS	Airborne Targeting and Cross Cueing System
ATC/ATR	Automatic Target Correlation/Recognition
ATD	Advanced Technology Development
ATDLS	Advanced Tactical Data Link System
ATR	Atlantic Test Range
ATRB	Advanced Technology Review Board
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
ATSC	Army Training Support Center
AWACS	Airborne Warning and Control System
AWE	Advanced Warfighting Experiment
AWS	Advanced Wideband System
BCA	Business Case Analyses
BCT	Brigade Combat Teams
BCTP	Battle Command Training Program
BDA	Battle Damage Assessment
BFM	Basic Flight Maneuver
BLII	Base Level Information Infrastructure
BLOS	Beyond Line of Sight
BMC3	Battle Management, Command, Control and Communications
BMC4I	Battle Management, Command, Control, Communications, Computers, and Intelligence
BMD	Ballistic Missile Defense
BMDO	Ballistic Missile Defense Organization
BMIC	Battleforce Management Information Center
BOS	Battlefield Operating System
BP1	Big Picture 1
BRP	Basic Research Plan
C2	Command and Control

C2I	Command, Control, and Intelligence
C2IPS	Command and Control Information Processing System
C2IS	Component Command and Control Information Systems
C2P	Command Control Processor
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4ISP	Command, Control, Communications, Computers, and Intelligence Support Plan
C4ISR	Command Control, Communication, and Computer, Intelligence, Surveillance and Reconnaissance
CAD	Component Advanced Development
CAF	Combat Air Forces
CAMP	Core Avionics Master Plan
CAOC	Combined Aerospace Operations Center
CAOC-X	Combined Aerospace Operations Center—Experimental
CAS	Collaboration at Sea; Close Air Support
CBIRF	Chemical Biological Incident Response Force
CCEB	Combined Communications Electronics Board
CCRB	C4ISR Cooperative Research Program
CDL	Common Data Link
CE	Command Element
CEC	Cooperative Engagement Capability
CFBLNet	Combined Federated Battle Laboratory Network
CGS	Common Ground Station
CID	Combat Identification
CIL	Command Information Libraries
CINC	Commander in Chief
CIO	Central Information Office
CIOMB	CIO Management Board
CIRT	Computer Incident Response Team
CITS	Combat Information Transport System
CIX	COP Interface eXchange
CJCS	Chairman of the Joint Chiefs of Staff
CMA/COM	Collection Management Authority/Collection Operational Management
COMTHIRDFLT	Commander Third Fleet
COSMOS	C4ISR Space and Missile Operations Simulator
CNAI	Critical Named Areas of Interest
CNO	Chief of Naval Operations
CNR	Combat Radio Nets
COA	Course of Action

COE	Common Operating Environment
COMAFFOR	Commander Air Force Forces
CONOPS	Concept of Operations
COMSEC	Computer Security
CONUS	Continental United States
COP	Common Operational Picture
COTS	Commercial-Off-the-Shelf
CPAM	Chairman's (of the JCS) Program Assessment Memorandum
CPIGS	Coalition Portal for Imagery and Geospatial Services
CPX	Command Post Exercise
CRC	Control and Reporting Center
CRD	Capstone Requirement Document
CRE	Control and Reporting Element
CROP	Common Relevant Operating Security
CS	Combat Support
CSDE	Combat Support Data Environment
CSE	Combat Support Enhanced
CSOF	Counter Special Operations Forces
CSS	Combat Service Support
CSSCS	Combat Service Support Control System
CST	COP Synchronization Tools
CTP	Common Tactical Picture
CUITN	Common User Installation Transport Network
CWAN	Coalition Wide Area Network
CXP	Common Transponder
DAA	Distributed Analytic Architecture
DAC	Designated acquisition commander
DACT	Data Automated Communications Terminal
DAL	Defended Asset List
DAMA	Demand Assigned Multiple Access
DARPA	Defense Advanced Research Projects Agency
DATP	Defense Technology Area Plan
DCGS-A	Distributed Common Ground System-Army
DCI	Director for Central Intelligence
DCIIS	Defense Counterintelligence Information System
DCX	Division Capstone Exercise
DD2-N	Digital Divisions 2 thru N
DDR&D	Director of Defense Research and Engineering
DEP	Distributed Engineering Plant
DII	Defense Information Infrastructure

DISA	Defense Information System Agency
DISN	Defense Information System Network
Dnet	Defense Network
DoD	Information Technology Security Certification and Accreditation Plan
DMS	Defense Message System
DoD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
DREN	Defense Research and Engineering Network
DRPM	Design Reference Performance Missions
DSAWG	DISN Security Accreditation Work Group
DSCS	Defense Satellite Communication System
DSP	Defense Support Program
DSTAG	S&T Advisory Group
DTAP	Defense Technology Area Plan
DTC	Digital Technical Control Facility
DTES	Division TES
DTIG	Deployable Theater Information Grid
DTLOMS	Doctrine, Training, Leader development, Organizations, Materiel, and Soldier
DTO	Defense Technology Objectives
DTRA	Defense Treat Reduction Agency
DTSS	Digitized Topographic Support System
DVMC	Digital Video Map Controller
EAC	Echelon Above Corps
EAF	Expeditionary Aerospace Force
EB/EC	Electronic Business/ Electronic Commerce
EBO	Effects-Based Operations
E-business	Any Internet initiative—tactical or strategic—that transforms business relationships, whether those relationships be business-to-consumer, business-to-business, intra-business, or even consumer-to-business
EC	Enabling Capabilities
EC5G	Expeditionary C2, Communications, Computing, and Combat Systems Grid
ECOC	Experimental Combat Operations Center
E-commerce	A particular type of e-business initiative that is focused around individual business transactions that use the Internet as a medium of exchange, including business-to-business as well as business-to consumer.
EFDS	Expeditionary Force Development System

EHF	Extremely High Frequency
EIPT	Executive Integrated Process Team
ELB	Extending the Littoral Battlespace
ELINT	Electronic Intelligence
EMW	Expeditionary Maneuver Warfare
EOTDA	Electro-Optical Tactical Decision Aid
EPLRS	Enhanced Position Location Reporting System
ERP	Enterprise Resource Planning
ESA	Electronically Scanning Array
ESC	Electronic Systems Center
ESG	Expeditionary Sensor Grid
ESTEL	E-2C Simulation Test and Evaluation Laboratory
EUT	End User Terminal
EW	Electronic Warfare
EXCOM	Executive Committee
EXFOR	Experimental Force
F2T2EA	Find, Fix, Target, Track, Engage, Assess
FAA	Federal Aviation Administration
FAC	Forward Air Controllers
FAST	Fleet Anti-Terrorism Security Team
FBCB2	Force XXI Battle Command Brigade and Below
FBE	Fleet Battle Experiments
FCS	Future Combat Systems
FIOP	Family of Interoperable Pictures
FIST-V	Fire Support Team Vehicle
FLEEDO	Focused Logistics Enabling Early Decisive Entry Operations
FNC	Future Naval Capability
FO/GO	Flag Officer/General Officer
FoS	Family of Systems
FOTP	Fleet Operational Telecommunications Plan
FTI	Fixed Target Indicators
FYEP	Five-year Experimental Plan
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCCS-A	Global Command and Control System-Army
GCCS-K	GCCS-Korea
GCCS-M	GCCS-Maritime
GCSS	Global Combat Support System
GCSS-A	GCSS-Army

GCSS-AF	GCSS-Air Force
GFE	Government-furnished Equipment
GFLC	Ground Force Level Control
GI3IPT	Geospatial Information Infrastructure Implementation IPT Team
GIG	Global Information Grid
GLTER	Geo-Location of Threat Emitters
GMF	Ground Mobile Forces
GMT	Ground Mobile Terminal
GPS	Global Positioning System
GRS	Global Reconnaissance Strike
GSORTS	Global Status of Resources and Training
GTACS	Ground Tactical Air Control System
GTN	Global Transportation Network
GUI	Graphic User Interface
HARM	High-speed Anti-Radiation Missile
HCLOS	High Capacity Line of Sight Radio
HITL	Human-in-the-Loop
HLA	High-level Architecture
HMDA	High Mobility Digital Group Multiplex Assemblage
HMI	Human-Machine Interface
HMMWV	High Mobility Multipurpose Wheeled Vehicle
HIS	Human Systems Interface
HOL	High Order Language
HTS	Harm Targeting System
HWIL	Hardware-in-the-Loop
I3A	Installation Information Infrastructure Architecture (Army)
I3MP	Installation Information Infrastructure Modernization Program (Army)
IA	Information Assurance
I&W	Indication and Warning
IAVA	Information Assurance Vulnerability Alerts
IBAR	Integrated Battlespace Arena
IBCT	Interim Brigade Combat Teams
IBS	Integrated Broadcast Service
ICD	Interface Control Documents
ID	Information Distribution; Identification
IDL	Interoperable Data Link
IDM	Information Dissemination Management
IDS	Intrusion Detection Systems
IEW	Intelligence and Electronic Warfare

IF	Integration Framework
IFF	Identification, Friend or Foe
IIW	Information-in-Warfare
IMETS	Integrated Meteorological System
IMINT	Imagery Intelligence
IO	Information Operations
IOC	Initial Operational Capability
IP	Internet Protocol
IPB	Intelligence Preparation of the Battlespace
IPT	Integrated Product Team
IS	Information Superiority
ISC2	the Integrated Space Command and Control
ISDN	Integrated Services Digital Network
ISM	ISR Sensor Manager
ISR	Intelligence, Surveillance, and Reconnaissance
ISR-M	ISR Manager
ISSC	Information System Sub-Committee
ISSM	Information System Security Managers
IT	Information Technology
IT-21	Information Technology for the 21st Century
ITSDN	Integrated Tactical-Strategic Data Network
ITSG	Information Technology Steering Group
ITU	International Telecommunications Union
ITW/AA	Integrated Tactical Warning and Attack Assessment
IW	Information Warfare
IWAR	Integrated Warfare Architecture
J2EE	Java 2 Enterprise Edition
JAOC	Joint Aerospace Operations Center
JBI	Joint Battlespace Infosphere
JBPDS	Joint Biological Point Detection System
JCALS	Joint Computer-aided Acquisition and Logistics Support
JCAS	Joint Collaboration at Sea
JCC(X)	Joint Command and Control Ship
JCSE	Joint Communications Support Element
JCTN	Joint Composite Tracking Network
JDA	Japan Defense Agency
JDN	Joint Data Network
JDP	Joint Defensive Planner
JFACC	Joint Forces Air Component Commander
JFC	Joint Force Commander

JFCOM	Joint Forces Command
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
JFTOC	Joint Force Tactical Operations Center
JI&I	Joint Integration and Interoperability
JICPAC	Joint Intelligence Center Pacific
JIER	Joint Information Exchange Requirements
JIP	Joint Interactive Planning
JMA	Joint Mission Areas
JMPS	Joint Mission Planning System
JMSWG	Joint Multi-TADIL Standards Working Group
JNMS	Joint Network Management System
JOA	Joint Operational Architecture
Joint C2	Joint interoperability
JOPES	Joint Operational Planning and Execution System
JPN	Joint Planning Network
JRE	Joint Range Extension
JROC	Joint Requirements Oversight Council
JSEAD	Joint Suppression of Enemy Air Defense
JSOTF	Joint Special Operations Task Force
JSOW	Joint Stand Off Weapon
JSTARS	Joint Surveillance Target Attack Radar System
JSWS	Joint Service Work Station
JTA	Joint Technical Architecture
JTAMDO	Joint Theater Air and Missile Defense Office
JTAT	Joint Terrain Analysis Toolkit
JTAV	Joint Total Assets Visibility
JTF	Joint Task Force
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
JUSE	Joint User Switch Exercises
JWARN	Joint Warning and Reporting Network
JWICS	Joint Worldwide Intelligence Communications System
JWID	Joint Warrior Interoperability Demonstration
JWSTP	Joint Warfighting S&T Plan
JV	Joint Vision
KSA	Knowledge Superiority and Assurance
KPP	key Performance Parameter
LAS	Local Area Subsystem

LAWS	Land Attack Warfare
LVT	Low Volume Terminal
LMST	Lightweight Multi-Band Satellite Terminal
LOCE	linked Ops/Intel Centers Europe
LoS	Line of Sight
MAGTF	Marine Air-Ground Task Force
MAMS	Military Airspace Management System
M&S	Modeling and Simulation
MARFOR INO	Marine Corps Forces Integrated Network Operations
MASINT	Measurement and Signatures Intelligence
MB	Megabyte
Mbps	Megabits per second
MCEN	Marine Corps Enterprise Network
MCP	Mission Capability Package
MCS	Maneuver Control System
MCSC	Marine Corps Systems Command
MCTDN	Marine Corps Tactical Data Network
MCTSSA	Marine Corps Technical Systems Support Activity
MCWL	Marine Corps Warfighting Laboratory
MDAPS	Major Defense Acquisition Programs
MDDS	Multi Domain Dissemination System
MEADS	Medium Extended Air Defense System
MEB	Marine Expeditionary Brigades
MEF	Marine Expeditionary Forces
MEU SOC	Marine Expeditionary Units (Special Operations Capable)
MIDAS	Marine Intrusion Detection Analysis Section
MIDS	Multifunction Information Distribution Terminal
MILSATCOM	Military Satellite Communications
MILSTAR	Military Strategic, Tactical, & Relay
MIP	MAGTF Integrated Process
MIT	Marine Corps Information Technology (IT)
MNS	Mission Needs Statement
MMA	Multi-Mission Maritime Aircraft
MOE/MOP	Measures of Effectiveness/Performance
MOS	Military Occupational Specialties
MOSAIC	Multifunctional On-the-Move Secure Adaptive Integrated Communications
MPEG	Multi-Platform Emitter Geolocation
MRC	Major Regional Contingencies
MROC	Multicommand Required Operational Capability

MS	Mobile Subsystem
MSC2FOSC	Multi-Service Command and Control Flag Officer Steering Committee
MSE	Mobile Subscriber Equipment
MSFE	Multi-Source Fusion Engine
MTI	Moving Target Indicators
MTT	Mobile Training Teams
MTW	Major Theater of War
MUOS	Mobile User Objective System
NAS	National Airspace System
NATO	North Atlantic Treaty Organization
NAVFOR	Naval Force Component Commander
NCA	National Command Authority
NCCS	New Central Command System
NCCT	Network Centric Collaborative Targeting
NCE	Network Control Element
NCIC	Network-centric Innovation Center
NCO	Network Centric Operations
NCTAMS	Naval Computer and Telecommunications Area Master Station
NCW	Network Centric Warfare
NETOPS	Network Operations
NFN	Naval Fires Network
NIL	NIMA Information Library
NIMA	National Imagery and Mapping Agency
NIPRNet	Non-secure Internet Protocol Network
NMCI	Navy / Marine Corps Intranet
NMD	National Missile Defense
NNC	NCCT Network Controller
NOC	Network Operations Center
NOSC	Network Operations and Security Centers
NPG	Network Participation Group
NSA/CSS	National Security Agency/Central Security Service
NSS	National Security Systems; Naval Simulation System
NSFS	Naval Surface Fire Support
NTC	National Training Center
NTDR	Near-Term Digital Radio
NTM	National Technical Means
NTW	Navy Theater Wide
NWDC	Navy Warfare Development Command
O& M	Operations and Maintenance

OCI/DCI	Offensive and Defensive Counter-Information operations
OFP	Operational Flight Program
OMFTS	Operational Maneuver from the Sea
ONA	Operational Net Assessment
ONIR	Overhead Non Imaging IR
ONR	Office of Naval Research
OODA	Observe, Orient, Decide, Act
OOTA	Operations Other Than War
OPAM	Observe, Predict, Assess, and Maneuver
OPCON	Operational Control
OPFOR	Opposing Force
OPSEC	Operations Security
OPSIT	Operational Situation
OPTEMPO	Operational Tempo
ORD	Operational Requirement Document
OSCAR	Outside Cable Rehabilitation
OSD	Office of the Secretary of Defense
OSP	Operational Special Project
OTH	Over the Horizon
OUSD (AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
OWG	Operational Work Group
PABX	Private Automatic Branch Exchanges
PBA	Predictive Battlespace Awareness
PD	Program Director
PDAS-BIM	Principal Deputy Assistant Secretary, Business and Information Management
PDM	Program Decision Memorandum
PED	Process, Exploit, and Disseminate
PEO	Program Executive Office
PEO-C3S	Program Executive Officer for C3 Systems
PGM	Precision-Guided Munitions
PIM	Platform Interface Module
PKI	Public Key Infrastructure
PMMV	Passive Millimeter Wave**
POM	Program Objective Memorandum
PoR	Program of Record
PRISM	Photo Reconnaissance Intelligence Strike
PRN	Packet Radio Networks
PS	Project SUTER

PSA	Principal Staff Assistants of OSD
PSAB	Prince Sultan Air Base
PSTN	Public Switched Telephone Network
QDR	Quadrennial Defense Review
QoS	Quality of Service
RAP	Radio Access Points
RBA	Revolution in Business Affairs
RDT&E	Research, Development, Test & Evaluation
REDS	Real-time Execution Decision Support
RMA	Revolution in Military Affairs
RNOSC	Regional Network Operations Support Centers
ROC	Residual Operational Capability
ROE	Rules of Engagement
ROK	Republic of Korea
RPTS/TDM	Rapid Precision Targeting System/ Tactical Dissemination Module
R/SAOC	Region/Sector Air Operation Centers
RSTA	Reconnaissance, Surveillance, and Target Acquisition
RTIC	Real Time in the Cockpit
RTSDL	Real Time Surveillance Data Link
SABI	Secret and Below Interoperability
S&TI	Science and Technology Intelligence
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SBIRS	Space Based Infrared System
SCAMP	Single Channel Anti-Jam Manportable Terminal
SCI	Secure Compartmented Information
SCRA	Single Channel Radio Access
SDH	Synchronous Digital Hierarchy
SDREN	Secret Defense Research & Engineering Network
SE	Systems Engineering
SE&I	Systems Engineering & Integration Division
SET	Systems Engineering Team
SHARP	Shared Reconnaissance Pod
SHF	Super High Frequency
SIAP SE	Single Integrated Air Picture Systems Engineer
SIE	Systems Integration Environment
SIGINT	Signals Intelligence
SINCGARS	Single Channel Ground and Airborne Radio System

SIPRNet	Secure Internet Protocol Network
SLA	Service Level Agreements
SLAM ER	Standoff Land Attack Missile Expanded Response
SMART-T	Secure Mobile Anti-Jam Reliable Tactical Terminal
SMCS	System Management and Control Subsystem
SMOOS	Shipboard Meteorological and Oceanographic Observation System
SMTP	Simple Message Transfer Protocol
SoS	System of Systems
SOSUS	Sound Surveillance System
SPAWAR	Space and Naval Warfare Systems Command
SPMAGTF	Special Purpose MAGTF
SSA	Shared Situational Awareness
SSC	Senior Steering Council
SSG	Strategic Studies Group (Navy)
SSS	Single Shelter Switch
STAMIS	Standard Army Management Information System
STANAG	NATO Standardization Agreement
STAP	Space, Time Adaptive Processing
STAR-T	SHF Tri-band Advanced Range Extension Terminal
STE	Standard Telephone Equipment
STEP	Standardized Tactical Entry Point
STK	Strike Warfare
STOM	Ship to Objective Maneuver
STRAP	System Training Plan
SUA	Special Use Airspace
SWAN	Secret Wide Area Network
TACAN	Tactical Air Control and Navigation
TACC	Tanker Airlift Control Center
TACOMS	Tactical Communications
TACON	Tactical Control
TADIL	Tactical Digital Information Links
TALCE	Theater Airlift Control Element
TAMD	Theater Air and Missile Defense
TAMMAC	Tactical Aircraft Moving Map Display Capabilities
T&E	Test and Evaluation
TAOC	Tactical Air Operation Center
TARA	Technology Area Review and Assessments
TBMCS	Theater Battle Management Core System
TBMD	Theater Battle Management Defense
TCCC	Theater C4ISR Coordination Center

TCO	Tactical Combat Operation
TCP	Transmission Control Protocol
TCS	Time Critical Strike
TCT	Time Critical Targeting
TCTA	Time Critical Target Aid
TDDS	Tactical Data Dissemination System
TEDS	Tactical Environmental Database System
TEL	Transporter Elevator Launcher
TENCAP	Tactical Exploitation of National Systems
TES	Tactical Exploitation System
TEWA	Threat Evaluation and Weapon Assignment
TFT	Tri-band Field Terminal
THAAD	Theater High Altitude Air Defense
THSDN	Tactical High-Speed Data Network
TIBS	Tactical Intelligence Broadcast Service
TIE	Technology Insertion Environment
TMD	Theater Missile Defense
TMET	Transportable Medium Earth Terminal
TOC	Tactical Operations Center
TPED	Tasking, Processing, Exploitation and Dissemination
TRADOC	Training and Doctrine Command
TRANSCOM	Transportation Command
TRI-TAC	Tri-Service Tactical Communications
TST	Time Sensitive Targeting
TTP	Tactics, Techniques, Procedures
TUAV	Tactical Unmanned Aerial Vehicle
UAV	Unmanned Aerial Vehicles
UCAV	Unmanned Combat Air Vehicles
UHF	Ultra High Frequency
ULCS	Unit-level Circuit Switch
URL	Universal Reference Library
USCENTCOM	U.S. Central Command
USCINCCENT	Commander in Chief, U.S. Central Command
USCINCPAC	Commander in Chief, U.S. Pacific Command
USEUCOM	U.S. European Command
USFJ	U.S. Forces—Japan
USFK	U.S. Forces—Korea
USIGS	U.S. Imagery and Geospatial Information Service
USJFCOM	U.S. Joint Forces Command
USPACOM	U.S. Pacific Command

USSOCOM	U.S. Special Operations Command
USSOUTHCOM	U.S. Southern Command
USSPACECOM	U.S. Space Command
USSTRATCOM	U.S. Strategic Command
USTRANSCOM	U.S. Transportation Command
USW	Undersea Warfare
UHF	Ultra High Frequency
VCNO	Vice CNO
VIPER	Virtual Intelligent Pilot for Enhanced Reactivity
VMF	Variable Message Format
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network; Voice Product Network
VTC	Video Teleconferencing
VWC	Virtual Warfare Center
W3C	World Wide Web Consortium
WAN	Wide Area Network
WAS	Wide Area Subsystem
WeCAN	Web-Centric ASW Network
WEN	Web-enabled Navy
WGM	Work Group Management
WIN-T	Warfighter Information Network
WMA	Warfare Mission Area
WMD	Weapons of Mass Destruction
WOC	Wing Operations Centers (U.S. Air Force)
WSSA	Weapon System Support Activity
WWI	World War I
WWMCCS	Worldwide Military Command and Control System
XML	Extended Markup Language
XMLMTF	Extended Markup Language Message Text Format
Y2K	Year 2000 acronym

For this report on line go to: www.c3i.osd.mil/NCW/

For more information on NCW go to: www.dodccrp.org/ncw.htm