Report on Network Centric Warfare

Sense of the Report

Submitted to the Congress in partial fulfillment of Section 934 of the Defense Authorization Act for FY01 (Public Law 106-398)

March 2001

Arthur L. Money

Assistant Secretary of Defense (C3I)

Report on Network Centric Warfare

Sense of the Report

This “Sense of the Report” is submitted in partial fulfillment of Section 934 of the Defense Authorization Act for FY01 (Public Law 106-398). This section calls for the Secretary of Defense, in consultation with the Chairman of the Joint Chiefs of Staff, to develop a report on the development and implementation of network-centric warfare concepts within the Department of Defense. The Act stipulated that the following areas be addressed:

(A) A clear definition and terminology to describe the set of operational concepts referred to as “network-centric warfare.”

(B) An identification and description of the current and planned activities by the Office of the Secretary of Defense, The Joint Chiefs of Staff, and the United States Joint Forces Command relating to network-centric warfare.

(C) A discussion of how the concept of network-centric warfare 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.

(D) A discussion of 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."

(E) An identification and description of the current and planned activities of each of the Armed Forces relating to network-centric warfare.

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

(G) A discussion 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.

(H) A discussion of how Department of Defense activities to establish a joint network-centric capability are coordinated with other departments and agencies of the United States and with United States allies.

(I) 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.

(J) The methodology being used to measure progress towards stated goals.

These areas will be addressed comprehensively in two documents. The first document is this "Sense of the Report," which provides an initial perspective on where network-centric warfare is today and where it is going in the Department of Defense. A subsequent document, to be provided no later than 1 July, will cover all areas in detail. A coordinated outline of this subsequent document is provided at Appendix A. The Department is currently in the process of collecting and integrating information for this second document.

"Sense of the Report"

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. Information technology 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 – 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.

NCW as a Product of the Information Age

Warfare takes on the characteristics of its Age. Network Centric Warfare (NCW) continues this trend -- it is the military response to the opportunities created by the Information Age. The term network-centric warfare 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. It involves the development of distributed collaboration processes designed to ensure that all pertinent available information is shared and that all appropriate assets can be brought to bear to by commanders to employ dominant maneuver, precision engagement, full-dimensional protection, and focused logistics.

Consequently, the terms "network-centric operations" and "network-centric warfare" 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. Scott McNealy, Chairman and CEO of Sun Microsystems, recently stated: "the "e" in e-business is redundant.[1]" 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 network-centric warfare is very much about warfare – about warfare in the Information Age. 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 Department of Defense seeks similar disproportionate advantages in future conflicts as we develop and implement a strategy for transformation with network-centric warfare as a principal component.

NCW Defined

To first order, network-centric operations are military operations that are enabled by the networking of the force. When these military operations take place in the context of warfare, the term network-centric warfare is applicable. Warfare takes place simultaneously in and among the physical, the information, and the cognitive domains.

Physical Domain: The physical domain is the traditional domain of warfare. It is domain where strike, protect, and maneuver take place across the environments of ground, sea, air, and space.[2] 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. Two important metrics for measuring combat power in this domain, lethality and survivability, have been and continue to be benchmarks for measuring the effectiveness of combat operations.

Information Domain: The information domain is the domain where information lives. It is the domain 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. 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.

Cognitive Domain: The cognitive domain is the domain of the mind of the warfighter and the supporting populous. This is the domain where many battles and wars are 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 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.

A warfighting force that can conduct network-centric operations can be defined as having the following attributes and capabilities:

Physical Domain:

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

Information Domain:

The force has the capability to share, access, and protect information to a degree that it can establish and maintain an information advantage over an adversary.

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.

Cognitive Domain:

The force has the capability to develop high quality awareness and share this 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.

The central hypothesis of network-centric warfare is that a force with these capabilities can increase combat power, by:

- better synchronizing effects in the battlespace
- achieving greater speed of command
- increasing lethality, survivability, and responsiveness

Network-centric operations to date have tended to focus on the tactical and operational levels of warfare, but they impact all levels of military activity from the tactical to the strategic. 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.

NCW as an Emerging Perspective

The term network-centric warfare is, as yet, not universally accepted in the Defense community nor are network-centric warfare concepts well understood. The term network-centric warfare was first introduced to a wide audience in 1998 in the article "Network Centric Warfare: It's Origins and Future," in *Proceedings of the Naval Institute*.[3] 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 tens of articles, hundreds of briefings, the distribution of tens of thousands of copies of the book *Network Centric Warfare: Developing and Leveraging Information Superiority*.[4] Additional factors that have contributed to this understanding include the reprinting of the book by leading information technology 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. 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 network-centric warfare.

Therefore, the second document in this report will go beyond the labels to the ideas behind them to pull together those DoD activities and initiatives that reflect the central hypothesis of network-centric warfare whether or not the term network-centric warfare is or is not used.

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.[5] 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 build-out, 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.[6] 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-business to date, the initial intuition of its Founder and Chairman, Pierre Omidyar, was borne out in eBay's subsequent success.[7] 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 could not predict exactly how many people would want to use eBay to buy and sell items.

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 ever 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 experimented with network-centric concepts in the counter special operations forces (CSOF) mission and validated the power of network-centric warfare.[8]

NCW – The Source of Combat Power

The extent to which networking a force can directly contribute to increased combat power in a broad range of mission areas is not immediately apparent. Yet it is supported by emerging evidence from recent military operations and a broad range of experimentation. A close analysis of the evidence has highlighted that new tactics, techniques, and procedures (e.g., new "warfighting models) – enabled by dramatically improved capabilities for information sharing – play a key role in increasing combat power.[10]

Perhaps the most significant example of the power of network-centric operations to date occurred when FBE Delta was conducted in conjunction with Combined Forces Command Korea. This command faces major warfighting challenges in three mission areas: Counter Fire, Counter Special Operations Forces, and Theater Air and Missile Defense. Each of these missions was addressed in Fleet Battle Experiment 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 counter special operations force mission area, where the seemingly intractable problem of countering hundreds of North Korean special operations boats (a counter special operations forces (CSOF) mission) was dealt with on a timeline previously not thought possible.

The application of network-centric concepts enabled elements of the Army's 2nd Infantry Division, AH-64 Apache helicopters, Air Force AC-130s, as well a range of Navy and Marine Corps units to share information and develop common operational picture. This resulted in a very high level of shared situational awareness that, when combined with new tactics techniques, and procedures, allowed these forces to synchronize their efforts from the bottom up to achieve dramatically increased combat power and to accomplish their mission in the half the time required with traditional platform-centric operations.[11]

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.[12]"

Clearly, networking a force dramatically improves its capabilities for information sharing. This does not mean that all elements of the force are sharing information with each other all the time – but rather that all involved have the capability to share and access needed information. Sharing information is a prerequisite for a force to be able to develop shared situational awareness and to yield the warfighting benefits associated with enhanced collaboration and synchronization.

Some of the most compelling evidence for the power of information sharing in enabling network-centric operations is provided by an Operational Special Project conducted by the U.S. Air Force to evaluate the military utility of tactical data links employed by F-15Cs. Data collected during over 12,000 sorties and 19,000 flying hours demonstrated that the kill ratios for Joint Tactical Information Distribution System (JTIDS) equipped aircraft over non-JTIDS equipped adversaries were extremely high, increasing by over 2.5 x in offensive and defensive counter air missions.[13]

The digitization and networking of the F-15Cs enabled digital information to be shared between platforms, resulting in a significantly improved information position for the JTIDS equipped F-15Cs. It is clear that when compared to the information position of fighters operating with voice only, that the pilots flying F-15Cs with data-links were able to establish a relative information advantage that translated to a significantly higher level of shared situational awareness. The pilots were then able to exploit this awareness advantage to significantly increase their operational effectiveness.

Dramatically improved capabilities for information sharing enable a warfighting force to bring different kinds of expertise and perspectives to bear to better understand complex and dynamically changing operational situations. It also allows commanders to communicate their intent more rapidly, accurately, and completely, to change intent, and to monitor execution dynamically as an operational situation evolves knowing that all forces will be kept in the loop. With everyone on the team "in the know," they are better able to share an understanding of the operational situation, both locally and globally, and are able to stay abreast of changes in the situation. A significant benefit of information sharing is the enabling of new approaches to command and control that capitalize on shared awareness to achieve a high degree of synchronized effects while being able to rapidly adapt to changes in the operational situation.

The power of the network-centric operations in enabling collaboration was demonstrated by the U.S. Army in the fall of 2000 during the Joint Contingency Force Army Warfighting Experiment. During this experiment, an airborne sensor collected information that was rapidly distributed to the Joint Task Force Joint Operations Center and elements of an early entry force that was airborne and enroute. The capability to collaborate in real-time allowed commanders to rethink and change their execution plan. The employment of this network-centric concept enabled the warfighters participating in this experiment to significantly improve their operational effectiveness.

NCW and Joint Vision 2020

Joint Vision 2020 articulates a vision of future Joint warfare that is enabled by the competitive advantages of Information Superiority and Decision Superiority.

Information Superiority is a condition in the information domain that is created when one competitor is able to establish a superior information position vis-à-vis an adversary.[14] 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. *Joint Vision 2020* highlighted the central role that Information Operations can play in enabling a force to develop and maintain an information advantage.

Decision Superiority is a competitive advantage in the cognitive domain. It describes the capability of a warfighting team to collectively make better-informed decisions more quickly than an adversary. Decision Superiority is facilitated by Information Superiority.

Network-centric operations provide a force with access to a new, previously unreachable region of the information domain. The ability to operate in this region provides warfighters with a new type of information advantage**,** an advantage that when leveraged dramatically increases combat power.

NCW and the Global Information Grid

Joint Vision 2020 identified the Global Information Grid (GIG) as a key enabler of Information Superiority. An objective of the Global Information Grid is to attain a more fully integrated, joint command, control, communications, and computer capability. The Global Information Grid will provide warfighters with secure global access to information. The Global Information Grid will play a key role in networking the force and extending and securing the warfighters' information domain to enable network-centric operations. The success of network-centric operations is directly tied to the reliability, integrity, and timeliness of information sharing.

Currently, the Joint Forces Command is developing a capstone requirements document (CRD) for the GIG based on tasking by the Joint Requirements Oversight Council. When approved, the GIG CRD has the potential for impacting a broad range of service requirements for C4 and ISR capabilities.

The integrated information infrastructure of the GIG will leverage research and development results from both the commercial and the defense sectors.

NCW and Transformation

Network-centric warfare is the military analogue of the new business models that are replacing their industrial age predecessors in the private sector. Like its counterparts in the commercial world, network-centric warfare provides the warfighter with improved precision, agility, and efficiency necessary to maintain a competitive advantage. In the sense that the transformation of DoD is its adaptation to Information Age concepts and technologies, then network-centric operations is a manifestation of DoD's transformation. Network-centric operations can not be restricted to combat units or functions that take place on the battlefield because the success of these units depends upon a host of combat support and other services. Thus, the pursuit of network-centric warfare as a Revolution in Military Affairs must go hand in hand with a corresponding revolution in the DoD's business affairs. These revolutions and the synergy between them are what DoD transformation is all about. A key insight that has emerged from the commercial sector is that three key factors influence what a company can and cannot do when it comes to supporting innovation and transformation. These factors are resources, processes, and values.[15] These same factors can be used broadly characterize the challenges that DoD faces in transforming the force.

Transformation Challenges and Innovation

Going from network-centric concepts to fielded capabilities that can both create and leverage Information and Decision Superiority is a complex undertaking. This undertaking must take place within the context of the Department's resources, processes, and values. To be effective, transformation must take place along each of these dimensions.

For example, simply inserting new technology into existing organizations and processes may be the path of least resistance, but will inexorably lead to incremental or marginal improvement. Technology insertion leads to “sustaining” innovations, those that involve faster, better, and/or cheaper ways to accomplish the same set of tasks. Thus, choosing a purely technology-focused approach to transformation may appear attractive because it is comfortable but it carries with it a huge opportunity cost. This opportunity cost is, of course, giving up the potential benefits associated with a more innovative approach. And the “safe” choice is not without risk. Changing the nature of available information and the ways that information can be used while not adapting our organizations and processes encourages the growth of informal processes and organizations that develop to make the most of what is available. Informal organizations are not exercised or tested and may create problems that do not surface until the organization is under stress. The larger the mismatch between the formal way of doing something and the way it could be done by virtue of improved information capabilities, the greater the chance that informal arrangements will proliferate.[16]

To reap the rewards that can accompany the Information Age another path must be chosen. This path involves the conscious co-evolution of mission capability packages (sometimes referred to as Doctrine, Organization, Training, Material, Leadership & Education, Personnel, and Facilities (DOTMLPF)). A mission capability package begins with a network-centric operational concept, a concept of how a particular mission could be accomplished if everyone on the team were "on the net." Next an approach to command and control, organization, and doctrine that is designed for this "networked environment" is needed. Following this, the network-centric environment must be created. To complete the package, the education and training required to make it all function smoothly need to be specified. Taken together the mission capability package contains everything necessary to implement a network-centric concept. This approach enables a network-centric warfighting force.

The development of mission capability packages inherently involves disruptive innovation because it involves simultaneous changes in multiple dimensions and changes that cut across existing stovepipes and fiefdoms and brushes up against existing resource constraints, organizational processes, or values. This path, however, has the potential to reap dramatic improvement. It carries with it its own set of risks, but these can be minimized by a deliberate process that integrates experimentation with the co-evolution of network-centric mission capability packages. The DoD is engaged in developing and experimenting with network-centric concepts that tend to involve sustaining rather than disrupting innovation.[17] The good news is that there is mounting evidence that applications of network-centric warfare offer significant improvements in mission performance. The very good news is that these sustaining innovations are just scratching the surface of the possible. The potential of network- centric warfare is, indeed, enormous.

While DoD is proud of our accomplishments to date, we are not putting in place quickly enough the "infostructure" necessary to support network- centric warfare and to facilitate and encourage further innovation. Now is the time to move beyond harvesting low hanging fruit to make a concerted effort to remove the remaining impediments to progress. Under the leadership of ASD(C3I) and with the assistance of the Department's warfighters and technologists, a plan for the implementation of network-centric concepts will be developed to both consolidate the gains made thus far and to establish an integrated DoD process that will both encourage and facilitate innovation and will be capable of bringing these innovations to fruition in the form of proven mission capability packages in a timely manner.

Progress will not be made as quickly as many would hope because while the vision is clear, we must be take great care in managing the transition to new concepts of operations and the changes to our organization, doctrine, and force structure given that our National Security is at stake. We believe that the very process of collaboration needed to complete our response to Section 934 will help enable us to develop a more coherent approach to network-centric operations and accelerate progress.

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

[2] *Measuring the Effects of Network-Centric Warfare,* Office of the Secretary of Defense (Net Assessment), Pentagon, Washington, D.C.

[3] 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.

[4] David S. Alberts, John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised).* Washington, D.C., CCRP Press, 1999.

[5] Christensen, et el., "After the Gold Rush: Patterns of Success and Failure on the Internet," www.innosight.com, p. 22-24.

[6] Ibid.

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

[8] Personal conversation with VADM Walter Doran, 5 Feb 2001, Washington, DC.

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

[10] John J. Garstka, "Network Centric Warfare: An Overview of Emerging Theory," *PHALANX*, December, 2000.

[11] Vadm Arthur K. Cebrowki, USN, 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. February 23, 1999.

[12] ADM Dennis Blair, CINCPAC, Remarks during Keynote Address at WEST 2001, January 23rd, San Diego, CA.

[13] JTIDS Operational Special Project (OSP) Report To Congress, Dec 1997, Mission Area Director for Information Dominance, Office of the Secretary of the Air force for Acquisition, Headquarters U.S. Air Force, Washington, D.C.

[14] *Information Superiority: Making the Joint Vision Happen*, Office of the Assistant Secretary of Defense (Command, Control, Communications, & Intelligence), Pentagon, Washington, D.C., November, 2000.

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

[16] David S. Alberts. *The Unintended Consequences of Information Age Technologies*. Washington, DC: National Defense University Press, 1995.

[17] Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, MA, 1997.

<< Table of Contents