USAWC STRATEGY RESEARCH PROJECT

NETWORK CENTRIC WARFARE – TRANSFORMING THE U.S. ARMY

by

Lieutenant Colonel Carl D. Porter
United States Army

Mr. Bill Waddell
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 MAY 2004		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Network Centric Warfare - Transforming the U.S. Army	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Carl Porter	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**42**	

ABSTRACT

AUTHOR: Lieutenant Colonel Carl D. Porter

TITLE: NETWORK CENTRIC WARFARE – TRANSFORMING THE U.S. ARMY

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 42 CLASSIFICATION: Unclassified

The old paradigms of U.S. military operations in the industrial age are dead. Military relevance in the information dominated 21st Century no longer comes from the industrial age concept of massing forces or attrition warfare. Rather, it comes from a new information age paradigm where access to information enables the rapid employment of the right force at the right place and time to achieve strategic objectives, while preventing any adversary from doing the same. To achieve this position of dominance, the Department of Defense has embraced the concepts of Network Centric Warfare (NCW) as a way to transform the force and achieve Joint Vision 2020 objectives. This information age concept provides a systems view of the battle space that can radically compress the strategic, operational and tactical levels of war and dramatically increase combat power through shared awareness and self-synchronization. The concept will not take hold in the U.S. Army, however, without a substantial effort to overcome impediments and a corresponding co-evolution of processes, organizations and technology infrastructure. This research paper provides a summary of network centric warfare concepts and highlights some of the challenges to applying it throughout a transformed Army force.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

NETWORK CENTRIC WARFARE – TRANSFORMING THE U.S. ARMY

> We need to make the leap into the information age, which is critical to the foundation of our transformation efforts, the ability of forces to communicate and operate seamlessly on the battlefield will be critical to our success.
>
> —Secretary of Defense Donald H. Rumsfeld, Jan 2002[1]

The old paradigms of U.S. military operations in the industrial age are dead. Military relevance in the information dominated 21st Century no longer comes from the industrial age concept of massing forces or attrition warfare. Rather, it comes from a new information age paradigm where access to information enables the rapid employment of the right force at the right place and time to achieve strategic objectives, while preventing any adversary from doing the same. To achieve this position of dominance envisioned by Joint Vision 2020, the U.S. Army must transform through the adoption of a new concept of operations and infusion of the right technologies to maintain relevance in the complex and dynamic global environment.

The predominant information age concept to facilitate Army transformation is Network Centric Warfare (NCW). In a 2001 report to Congress, the Department of Defense (DoD) stated that this concept is "no less than the embodiment of information age transformation."[2] Admiral Jay Johnson, former Chief of Naval Operations calls it a "fundamental shift from what we call platform-centric warfare."[3] Similarly Vice Admiral (Retired) Arthur Cebrowski, Director of the DoD Office of Force Transformation (OFT) declares that NCW is not just a "new concept of operations"[4] but a paradigm shift to a "new American way of war"[5] that will prove to be the most significant Revolution in Military Affairs (RMA) in 200 years.[6] These comments indicate many strategic leaders' beliefs that NCW will provide the ways to achieve Joint Vision 2020 objectives and revolutionize how the Army operates in a joint, capability-based environment.

Although these statements suggest a growing enthusiasm and commitment to applying this concept to force transformation, many are not as optimistic over its potential impact on military effectiveness. Marine General Paul Viper argues that most DoD personnel "have no clue what NCW is."[7] Still other defense analysts contend that NCW concepts will do little to fundamentally change the nature of warfare or support the achievement of strategic objectives.[8]

So what exactly is Network Centric Warfare and how will its application transform the Army? What are the impediments to achieving it, and what are the implications of NCW on the Army's transformation strategy? To address these questions, this research paper begins with an overview of NCW concepts and tenets. Next, it describes the transformational nature of NCW through a comparison of platform-centric and network-centric operational constructs.

Finally, this document details some of the technical and fiscal impediments to applying this information age concept and offers some implications this concept may have on transforming the Army into a dominate, information superior force.

THE CONCEPT OF NETWORK CENTRIC WARFARE – AN EXECUTIVE SUMMARY

A new American way of war has emerged – network centric operations

—Vice Admiral (Retired) Arthur Cebrowski, Director, OFT[9]

Much has been written over the past few years on the concept and potential benefits of NCW. This section summarizes some of this intellectual thought to provide a succinct description of the essence of this information age concept of operations.

A commonly accepted definition of NCW is that provided by David Alberts, John Garstka, and Fred Stein in *Network Centric Warfare, Developing and Leveraging Information Superiority.* This reference defines network centric warfare as:

> Network Centric Warfare
> "An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[10]

This definition postulates revolutionary changes to existing capabilities achieved through networking sensors, shooters and decision makers. Consideration of the potential power of networking and the underlying tenets of NCW aids in understating and applying this definition.

POTENTIAL POWER OF NETWORKING

Network Centric Warfare is not about the "network" but about the ability to share information through the power of networking.[11] One of the best ways to articulate this potential power is consideration the Internet-enabled information "explosion." The birth of the Internet occurred in late 1969 when government and academia connected four host computers to form a network known as ARPANET.[12] Over the succeeding two decades, the number of network nodes grew modestly, limited mainly by immature infrastructure and the lack of common user interfaces, protocols and applications. When advances in technology mitigated these factors, the Internet became "real." Today, there are millions of nodes connected to the Internet and the corresponding number of interactions has grown exponentially.

Although the ability to connect nodes is significant, the real value rests in the ability to exchange information and collaborate across the network. Roger Roberts suggests that the

value of the Internet is that it acts like "a living entity that is constantly receiving new data, cataloging it, and storing it so that those in search can find the most up to date information easily and quickly."[13] Roberts offers that NCW concepts provide the ways to "use the power of the network to access information from far reaching resources in order to make timely, effective, and sometimes life saving decisions."[14] This characterization highlights the fundamental value of networking – the ability to share relevant information quickly across the entire enterprise.

The commercial sector was one of the first to take full advantage of the Internet-enabled method of exchanging information. By leveraging the power of networking, new methods of doing business emerged where information superiority became the enabler of maintaining a competitive advantage in the market place. These concepts enabled electronic business, a revolutionary change that is now common place.

Some suggest that the terms "network-centric operations" and "network-centric warfare" describe military operations "in the same way that the terms 'e-business' and 'e-commerce' describe a broad class of business activities enabled by the Internet."[15] Review of NCW tenets and their application to the domains of warfare provides insight into this suggested relationship.

TENETS OF NETWORK CENTRIC WARFARE AND THE DOMAINS OF WAR

The 2001 DoD NCW Report to Congress provides four NCW tenets and describes their application to the domains of warfare.[16] These tenets (Table 1) and their underlying attributes provide insight into how the Army can achieve a competitive advantage through networking.

Tenets of Network Centric Warfare
• 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 • These, in turn, dramatically increase mission effectiveness

TABLE 1: TENETS OF NETWORK CENTRIC WARFARE

The first tenet builds on the power of information sharing as "a source of potential value."[17] A robust network implies an interoperable infrastructure that enables the force to share, access, and protect information quicker and more efficiently than its adversaries, thereby achieving information superiority. Army Vision 2010 defines information superiority as follows:

Information Superiority
"The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[18]

Information superiority is not an end state – but a relative state achieved when the ability to exploit information advantages creates a competitive advantage over any adversary.

The second tenet suggests that networking the force provides a higher level of situational awareness that subsequently enables the Army to "deploy a more focused and lethal force by providing frontline war fighters with critical information, including a near real time view of the battlefield."[19] Networking enables the force to gather raw data, transform it into relevant information that creates a shared understanding of the "threats and assets"[20] in the battle space where both the enemy and friendly forces are seen as "complex, adaptive systems, composed of many systems and subsystems."[21] As such, information superiority provides the means to generate decision superiority to achieve desired results. Joint Vision 2020 defines decision superiority as "better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission."[22]

The third tenet highlights the value of collaboration and self synchronization. One NCW goal is to reach a collaborative state by having all operations networked, with "the right item at the right place at the right time."[23] Some NCW advocates declare that NCW comes down to "harnessing the collaborative behavior that results from ever-faster access to information."[24] Clearly, NCW provides an environment where "collaboration between platforms, systems and devices is possible."[25] This environment supports the doctrinal imperative that "the commander who can gather information and make decisions faster and better will generate a quicker tempo of operations and gain a decided military advantage."[26]

The final tenet implies that the information superiority achieved through application of NCW concepts provides the means to achieve full spectrum dominance[27] by supporting the capabilities of dominant maneuver, precision engagement, focused logistics, and full dimensional protection envisioned in Joint Vision 2020.[28] Through collaboration and self-synchronization, a network centric force can rapidly maneuver a lethal force to the decisive point on the battlefield and achieve the desired effect with unparalleled precision. Network centric operational concepts elevate the value of information over mass to enable employment of a lighter force that is easier to support logistically. As a result, network enabled logisticians can provide the fighting force the resources it needs when it needs them without relying on vast logistic stocks in theater. Finally, through radically improved understanding of both the friendly and enemy situations, the force can achieve full dimensional protection by dramatically reducing incidents of fratricide and avoiding enemy strengths on the battlefield.

Applying these tenets to the domains of warfare yields additional insight into where NCW "fits" in the overall conduct of military operations. The DoD NCW Report to Congress provides that warfare occurs simultaneously in the physical, cognitive and informational domains. The physical domain is the "traditional domain of warfare…where strike, protect, and maneuver takes place."[29] The cognitive domain is the "domain of the mind of the war fighter… where many battles and wars and won and lost."[30] The information domain is the domain where "information is created, manipulated and shared."[31] Intersections between these domains shown graphically in Figure 1 present opportunities for transforming the conduct of warfare.

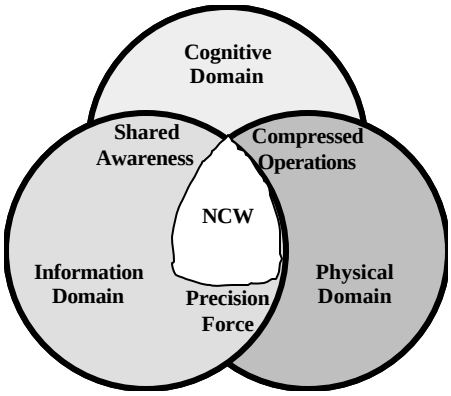

FIGURE 1: RELATIONSHIP BETWEEN NCW AND THE DOMAINS OF WARFARE[32]

Defense analysts in the DoD Office of Force Transformation (OFT) contend that the intersection of the physical and informational domains of warfare enables the application of a joint, precision force.[33] The intersection of the information and cognitive domains enables shared awareness and tactical innovation.[34] And finally, the intersection between the physical and cognitive domains is where time compression occurs and where tactics achieve operational and strategic effects. This intersection is also where high rates of change are developed and achieved. [35] NCW "exists at the center where the three warfare domains intersect."[36]

Finally, NCW advocates postulate that the information age creates a new rule set for the conduct of warfare, where NCW plays a significant role and where the things that are valued shifts.[37] Table 2 provides a summary of this proposed new rule set.

The New Rules	Network Centric Warfare
• Fight first for information superiority • Speed of command • Access to information; shared awareness • Dispersed forces; noncontiguous operations • Demassification • Self-synchronization • Deep sensor reach • Alter initial conditions at higher rates of change • Compress the levels of war	High rates of change Closely coupled events Lock in/out Speed of command Self-synchronization
	What's Valued
	Networking Sensing Envelope Management Speed/endurance Numbers Risk tolerance Staying power

TABLE 2: CHANGING RULE SET IN THE INFORMATION AGE [38]

The potential power of networking and conceptual theory behind NCW clearly underscores our strategic leaders' enthusiasm for this new concept. The challenge, however, is translating this conceptual framework into a coherent application across the Army to achieve the potential benefits it offers.

FROM PLATFORM CENTRIC TO NETWORK CENTRIC – APPLYING THE NCW CONCEPT

> To fight and win our nation's wars, the 21st century U.S. Army must rapidly transform to a net-centric, knowledge based force.
>
> —LTG Steven Boutelle, U.S. Army Chief Information Officer/G-6[39]

Practical application remains the key to understanding the transformational nature of NCW. This section offers a comparison of platform centric and network centric operations to reveal opportunities for transforming the force. Analysis of this comparison with examples from recent combat operations provides insight into the potential of NCW concepts.

The 2003 Defense Transformation Planning Guidance defines transformation as a "process that shapes the changing nature of military competition and cooperation through new combinations of concepts, capabilities, people and organizations that exploit our nation's advantages and protect against our asymmetric vulnerabilities to sustain our strategic position, which helps underpin peace and stability in the world"[40] As such, the transformational nature of NCW rests in the degree to which it shapes the nature of military competition and cooperation.

The Joint Staff publication entitled *An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution in the 21st Century*[41] provides areas for comparison between current, platform centric operations and those conducted under a network centric construct. For the purposes of

this comparison, platform centric operations are characterized by traditional military platforms linked by voice or data link that detect and identify targets, decide whether to engage the target, convey the decision to a weapons platform, and employ weapons on the target.[42] Network centric operations entail the networking of sensors, decision makers, and shooters to achieve the potential benefits of NCW.

Platform Centric Operations	Network Centric Operations
Closed, service-centric architecture systems	Fully integrated / networked joint C4ISR architecture and modular "plug and play" capabilities that tie military and civilian architectures
A long and involved sensor-to-shooter decision making sequence	Information, subsequent decisions, and actions are near simultaneous.
Material Node-centric system with emphasis on vertical connectivity	A joint capabilities-based system with emphasis on horizontal connectivity.
Service Platforms employed in a de-conflicted and coordinated manner to accomplish the operational or strategic objectives	Joint platforms integrated with common systems and a shared picture designed to provide a synergistic capability to achieve effects desired
Requires translation from Information Superiority into combat power through deconfliction process to ensure clearance, no duplication and commanders intent are met	Rapidly translates Knowledge superiority into combat power by effectively inter-linking knowledgeable entities with C2 structure throughout the battle space.

TABLE 3: COMPARISON OF PLATFORM AND NETWORK CENTRIC OPERATIONS[43]

The first point of comparison is the command, control and communications (C^3) architectures used to support operational requirements. Platform centric operations typically involve service-centric architectures that, because of their proprietary nature, do not communicate effectively with external entities. They are inherently hierarchal and linear, following traditional chains of command. Under a network centric operational construct, C^3 systems are integrated into an enterprise-wide C4ISR architecture[44] that includes both traditional military platforms as well as non-traditional DoD civilian entities. The envisioned C4ISR architecture is achieved through employment of open systems architectures with common user interfaces and protocols that enable all nodes on the network to connect and communicate efficiently. This architecture enables new entities to "plug" into the network and "play" in the same way that computers and peripheral devices can plug into an existing network and operate immediately with little reconfiguration or user effort. This "plug and play" approach is not limited to military forces; it includes potential integration of interagency and multinational collaboration and operational employment.[45]

A critical enabler to achieve the fully integrated C4ISR architecture necessary to support NCW is the Global Information Grid (GIG). The 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 war fighters, policy makers, and support personnel."[46] In some respects, the GIG is the "entry fee" for network centric operations and is essential for maintaining a fully integrated network that provides the "environment for decision superiority."[47]

Application of NCW capabilities in the form of an integrated C4ISR architecture was evidenced by the success of special operations forces (SOF) during Operation Enduring Freedom (OEF) in Afghanistan. Brigadier General James Parker, director of Special Operations Command (SOCOM) Center for Intelligence and Information Operations offers that SOF forces in Afghanistan were "empowered by shared situational awareness and robust communications" infrastructure.[48] He explains that the "adoption of network-centric capabilities laid the groundwork for success in Afghanistan…giving SOF greater access to vital information and creating an environment that allowed greater flexibility of SOF personnel and those equipping and supporting them."[49]

Operation Iraqi Freedom (OIF) in Iraq provides similar insights of the transformational benefits achieved through C4ISR integration. Brigadier General Dennis Moran, U.S. Central Command (CENTCOM) J6 argues that CENTCOM "validated the concept of NCW and the need for communication, command and control (C2) and ISR systems to be hooked up to, and interoperable with, the Global Information Grid and to be adaptable to whatever circumstances are on the battlefield."[50] He offers that "CENTCOM had a common operating picture of both friendly and enemy forces that could be shared at all levels of command, from strategic to operational and tactical. Each of the services brought its full family of intelligence, surveillance and reconnaissance systems to the battle which produced mountains of intelligence."[51]

The second point of comparison between platform centric and network centric operations is the speed of the observe, decide, act and assess cycle,[52] commonly referred to as the observe, orient, decide, act (OODA) loop. This cycle begins with sensor observation and target characterization, and subsequent decisions on whether or not to engage them. Shooter selection ensues based on target type and known shooter availability. In the platform centric environment, this cycle is linear with considerable latency. In some cases, excessive time requirements limit the potential number of targets engaged. Additionally, the platform centric environment with inherent communication architecture constraints precludes access to sensor information and application of shooter resources between the levels of command. As such, the

OODA loop is essentially limited to application at the tactical level of sensors, shooters and decision makers.

The network centric operational environment radically transforms the OODA loop. Although fundamental concepts remain, the efficient networking of sensors, decision makers and shooters enables these processes to occur in near simultaneous fashion. Through enhanced situation awareness provided by the GIG, hostile targets are easily identified, reducing the time required for target characterization. Sensors networked to decision makers and networked shooters enable the near simultaneous execution of targets contained in the engagement grid.[53] The robust C4ISR architecture greatly expands access to sensor information and provides the means to employ the full range of shooters to include strategic resources. Similarly, it allows leaders at all levels of command, from tactical up to national command authority level, to engage in the decision making process for strategic and time sensitive targets without significant latency in the process. As such, NCW essentially compresses the levels of command.

Figure 2 provides a logical model of the relationship between networked sensors, decision makers and shooters. The entities displayed in this figure are not limited to any level of war; they may include tactical, operational or strategic sensors, shooters and decision makers engaged simultaneously.

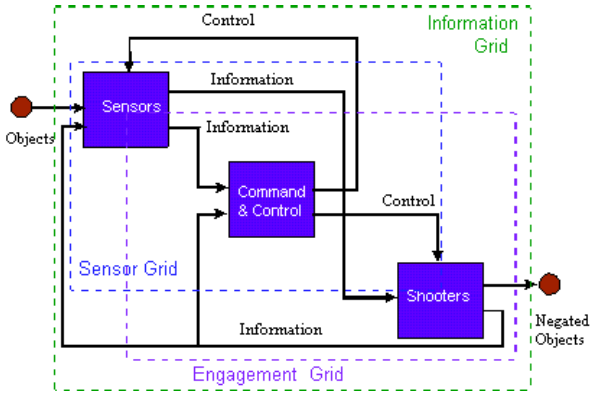

FIGURE 2: LOGICAL MODEL OF NCW RELATIONSHIPS[54]

Application of NCW concepts in accelerating the OODA loop and compressing the levels of command was evident during OEF and used extensively throughout the battlefield during Operation Iraqi Freedom (OIF). A Jane's Defence Weekly article offers that "the ability to transmit, receive and view data in real time across the coalition spectrum was practiced in an embryonic capacity in Afghanistan and honed in Iraq."[55] The article highlights the events and

short timelines involved with the pre-invasion attempt to decapitate the Iraqi dictator. Intelligence of Saddam's location was transmitted rapidly and simultaneously to strategic leaders at the national level and allied air planners in theater. A strategic B-1B bomber then engaged the target within about 12 minutes of the initial sensor report. [56] This rapid application of force to achieve the desired effect was possible through the networking of sensors, shooters and decision makers at the all levels of command.

The transformational change in dramatically reduced latency and enhanced effectiveness of the OODA loop "demonstrated just how effective a network-centric force can be on the battlefield."[57] Vice Admiral Cebrowski contends that OIF lessons learned will reveal that "good sensors, networked with good intelligence, disseminated through a robust network of systems"[58] increased the pace of operations leading to the rapid defeat of numerically superior Iraqi forces.

The final point of comparison is the method used to generate combat power and the underlying decision making processes involved. The platform centric approach generates combat power through a deconfliction process that clears operations, eliminates duplication, and ensures the commander's intent is met through hierarchal organizational arrangements. This construct requires the movement of information collected at the edges toward the center for decision making.[59] Generating combat power in an NCW environment, by comparison, is "all about changing decision making processes and topologies. It relies on an information age model where the edge is empowered to make decisions based on command intent and high quality situational awareness."[60] This radical shift in decision making processes and topologies and renewed emphasis on collaboration is clearly at the heart of the NCW concept. This shift generates considerable combat power and shapes the nature of competition.

SOF elements deployed during OEF achieved significant decision making enhancements through the application of NCW concepts. Specifically, they employed a "collaborative tool suite, known as the SOF Digital Environment (SDE)" in Afghanistan to provide "situational awareness, collaboration and mission planning."[61] As a result, they were able to "plan future missions and monitor ongoing missions from several locations."[62]

Similarly, use of a blue force tracking mechanism known as Force XXI Battle Command, Brigade-and-Below (FBCB2) was "one of the success stories of OIF."[63] This system enhanced decision making and the speed of command for ground forces during OIF by providing the means to interlink knowledgeable entities throughout the battle space with command and control structures. The resulting situational awareness enabled the application of overwhelming combat power that led to the rapid destruction of belligerent Iraqi forces.

NCW - IMPEDIMENTS AND IMPLICATIONS FOR ARMY TRANSFORMATION

> US forces must leverage information technology and innovative network-centric concepts of operations to develop increasingly capable joint forces. New information and communications technologies hold promise for networking highly distributed joint and multinational forces…
>
> —Secretary of Defense Donald H. Rumsfeld[64]

Although recent operational experience suggests that NCW is a viable concept for transforming the Army, the full potential has not been realized and significant impediments to implementing it remain. Not all of the NCW experiences were ideal and the "situational awareness picture was not available to everyone"[65] who needed it. Similarly, some senior leaders contend that "network-centric projects are still not ready for battle."[66]

Applying the concept of NCW relies on the infusion of new capabilities and technologies, and corresponding changes in tactics, techniques and procedures that have not fully matured. This section summarizes some of impediments to achieving the vision of NCW and considers the implications this concept has on Army force transformation.

IMPEDIMENTS TO ACHIEVING THE BENEFITS OF NCW

There are several known and emerging[67] impediments to achieving the potential benefits of NCW and realizing enhanced capabilities through networking the force.[68] For brevity, discussion of impediments is limited to some technical and resource-oriented challenges that may inhibit progress in applying NCW concepts throughout the Army. These impediments include the lack of robust network connectivity and interoperability, information security issues, and competition for resources to fund C4ISR investments in a fiscally constrained force.

The greatest impediment to achieving NCW is that the Army lacks the robust network connectivity and interoperability necessary to fully implement it. By design, NCW requires a robust network with common user access throughout a fluid battle space. Even the most avid NCW enthusiasts submit that "the information infrastructure will not be ready to support network-centric operations." [69] They content that "we are becoming more dependent on a fragile and vulnerable infrastructure"[70] and argue that there is a "disconnect between the future concepts being developed and planned reality of the infrastructure in the same time frame."[71]

The Army is heavily reliant on Mobile Subscriber Equipment (MSE) and other primarily terrestrial based communications systems to support its tactical networks in theater. Initially fielded in the late 1980's, MSE does not have the mobility required or bandwidth available to support the pace of operations envisioned in a NCW environment.[72] As offered by Colonel Tom

Cole from the U.S. Army Communications Electronic Command (CECOM), “right now, we have to stop, put a stake in the ground and put an antenna up, which slows our capability.” [73]

Shortfalls in terrestrial based systems generate increased demand for satellite communications (SATCOM) to make up the difference in bandwidth requirements. The relative demand for space-based bandwidth during OEF and OIF were over 50 times more than used during Operation Desert Storm in the early 1990’s.[74] By 2020, the anticipated bandwidth demand may exceed current requirements by more than 600 percent.[75] Although the military satellite community is working to meet this growing demand through organic, military SATCOM (MILSATCOM), it is unlikely that the military will be able to “deliver a functional worldwide system until sometime in the second decade of this century.”[76] As a result, the Army must rely on commercial satellites that may not be available when needed to support bandwidth requirements during combat operations.

The lack of robust network connectivity has led to increased investments and development of the GIG and new tactical communications systems, including the Warrior Information Network – Tactical (WIN-T) and the Joint Tactical Radio System (JTRS).[77] Some defense analysts predict that major increases in DoD C4ISR-related investments, combined with anticipated progress in the private sector, will eliminate bandwidth constraints “in about a decade.”[78] Although these predictions are somewhat optimistic, it is clear that greater C4ISR investments and private sector advances will resolve some current shortfalls. However, delays in technology development timelines will frustrate the process.

The second major impediment is the inability to address network security issues generated by increased reliance on a networked C4ISR infrastructure. The envisioned GIG and C4ISR infrastructure that connects tactical, operational and strategic nodes will only be as secure as its weakest link. As such, the Army must contend with a new set of network security issues in order to maintain a secure and reliable network.

Although the vast majority of network nodes in the envisioned C4ISR infrastructure will reside inside a relatively secure network environment, they may not be completely immune to internal or external actors who seek to disrupt operations, corrupt data, steal sensitive information, deny access or exploit network vulnerabilities.[79] For example, a rapidly propagating computer virus intentionally or unintentionally introduced into the C4ISR infrastructure may have devastating results. Additionally, the connection of relatively secure tactical C4ISR nodes to potentially less secure domestically based nodes required to create the end-to-end architecture of the GIG may provide a point of entry for hostile actors. As such, security concerns may limit the application and use of the infrastructure necessary to support NCW requirements.

The final impediment is the competition for resources to fund the investments required to build and maintain a robust C4ISR infrastructure. In a resource constrained force, greater C4ISR investments will generate "reduced investments in traditional platforms."[80] As such, weapon systems currently under development that do not integrate well into the conceptual C4ISR framework will receive "less attention, less funding, and may sometimes be cancelled."[81] The successful application of NCW concepts during OIF and OEF has already led DoD to consider a shift of over $1 billion from current programs to C4ISR during fiscal years (FY) 05 to FY 09.[82] It is probable that this shift of resources will increase over time.

Some contend that during the Rumsfeld era, "all new weapon systems will be evaluated primarily on the degree to which they further the…ability to conduct NCW."[83] This is based on the belief that NCW investments will generate a "greater influence…on total battlefield performance, whereas development of traditional platforms (in measures of fire-power, speed and range) is likely to create less operational impact."[84] Although this assertion has some merit, there is considerable risk in overestimating the impact of C4ISR investments over more traditional platforms. Additionally, if the advocates and system developers get it wrong, it can lead to a transformed force that is "completely unbalanced"[85] in required capabilities.

Finally, although investment strategies may support a networked force within the next 10 to 15 years, resource constraints will delay full employment throughout the Army and the joint force for a much longer period. According to Colonel Toomey, the "current situation of digital haves and have-nots is creating a force that cannot communicate with itself."[86] He contends that the "risk of fratricide to unseen units makes an already challenging force protection and survivability problem on a complex and confusing battle field even more acute."[87] As experienced during OEF and OIF,[88] we will experience interoperability issues and gaps in common situational understanding both internal to the Army and throughout the joint force.

IMPLICATIONS FOR ARMY TRANSFORMATION

> As we prepare for the future, we must think differently and develop the kinds of forces and capabilities that can adapt quickly to new challenges and unexpected circumstances. We must transform not only the capabilities at our disposal, but also the way we think, the way we train, the way we exercise and the way we fight.
>
> —Secretary of Defense Donald H. Rumsfeld[89]

The *Army Transformation Roadmap* states that Army transformation is about "changing the way we deploy, fight, sustain, and use information that will make us more strategically responsive and dominant across the spectrum of operations."[90] As such, the ultimate goal of

the Army's transformation strategy is to "provide relevant and ready current and future forces organized, trained and equipped for joint, interagency and multi-national full spectrum operations."[91] Transformation involves "more than technologies – it requires deep cultural shifts from traditional practices to collaboration, teamwork, and innovations; from information hording to knowledge sharing; from stovepipe to enterprise processes; and from traditional skills to internet-age competencies."[92] Applying the NCW operational construct yields insight into some of the implications this new concept will have on the Army's transformation strategy concerning doctrine, organizations, and training.

The first implication is the impact on the doctrinal application of decision making. Achieving NCW objectives necessitates doctrinal shifts from centralized decision making to a more distributed process where each entity on the battlefield is "empowered to make decisions based on command intent and high quality situational awareness."[93] Joint Vision 2020 states that "decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation…and the proper command and control mechanisms and tools are equally necessary."[94] As such, the Army must radically transform current command and control doctrine to create the environment necessary to translate information into decision superiority and support empowerment. Table 4 offered by David Alberts highlights some doctrinal changes in decision making evidenced in a net-centric force.[95] This listing is not exhaustive, but summarizes some of new doctrinal realities gained through application of NCW concepts and subsequent changes in doctrine as compared to current doctrinal conceptions.

Decision Making Requirements	Platform Centric (Industrial Age)	Network Centric (Information Age)
Dealing with the Future	• Predict/Plan • Perfect Tasks	• Prepare/Adapt • Develop agility
Developing Capabilities	• Define Requirements • Engineer • Insert Technology • Test Systems	• Experiment • Grow • Co-evolve capabilities • Assess operations
Command and Control	• Do what I tell you • Synchronize • Control • Constrain subordinates • Staff	• Do what makes sense • Self-synchronize • Converge • Enable subordinates • Collaborate
Dealing with Information	• Push • Use and distribute • Server-client • Clear people	• Pull • Post before process • Peer-to-peer • Sanction transaction

TABLE 4: COMPARISON OF DECISION MAKING REQUIREMENTS

Applying the NCW concept similarly necessitates a paradigm shift in how and when we apply information technology (IT) to existing doctrinal processes to achieve a competitive advantage across the full spectrum of operations. Some suggest that the Army transformation strategy is "all about accelerated processes."[96] The military routinely leverages IT as a means to gain efficiencies and accelerate processes. Unfortunately, the focus of IT application is on automating existing processes without substantially changing them.

A case in point is the doctrinal targeting process used at theater level and below to synchronize and de-conflict the application of air, sea and ground-based weapons platforms.[97] Although application of IT to automate this process has enhanced it effectiveness and reduced latency, the underlying process remain fairly linear and unchanged. Transforming to a network centric force requires a complete reengineering of the targeting process and many other existing tactics, techniques and procedures to achieve measurable results. Additionally, IT resource application must be consistent with the overall reengineering effort in order to gain measurable mission enhancements through IT and C4ISR investments.

The second implication for Army transformation is the potential impact NCW will have on the organizational structure of the force. A networked environment, by design, exists without significant regard to existing organizational hierarchy or institutional boundaries. As such, Army organizations will need to "co-evolve to take full advantage of the enhanced capabilities"[98] provided through the application of NCW concepts. The Army's transformation plan recognizes that "as platforms, units, and headquarters at all levels become information enabled, operations at both the tactical and operational levels will change."[99]

Some NCW advocates postulate that "as information moves down echelon, so does combat power, meaning smaller joint force packages wield greater combat power."[100] This point implies that transformed Army units must co-evolve into smaller, joint force package entities that can provide capabilities equal to the larger current force. It supports the premise that our future organization will be "fully joint: intellectually, operationally, organizationally and technically."[101]

A related implication is the impact NCW will have on the existing concept of the levels of war. Networking distributed entities that exist at all levels of command may generate fundamental changes to the current concept of the tactical, operational and strategic levels of war. Because NCW provides the ability to move information rapidly between all levels of command, some contend that it will "collapse the strategic, operational, and tactical levels of war."[102] Although this claim may be somewhat overstated, NCW clearly provides the ways to compress strategic, operational and tactical levels of war through radically improved situational awareness and understanding, knowledge management and self-synchronization.

The final implication is the impact NCW will have on Army training and leader development programs. An article published in *Armor* magazine suggests that the Army's transformation to a network enabled force requires a "deliberate front-end analysis that will define the doctrine, training, and personnel implications for the Army. This analysis…is critical for focusing resources and accelerating the U.S. Army's transition"[103] to an information superior force. Application of NCW concepts clearly implicates the need for potentially intensive systems training as well as radically new approach to leader development.

Operating in an NCW environment requires a new combination of technical and conceptual skills that exceed current Army training skill sets. Experience gained by the Army Transformation Task Force suggests that "digital skills are neither easily acquired nor retained and require a steep learning curve for both soldiers and leaders."[104] Other reports indicate that "it takes a long time for human crews to learn how to intuitively operate" these complex systems-of-systems.[105] These statements imply the need for radically different training regimes as a means to achieve Army's transformation objectives throughout a networked enabled force. Additionally, future training strategies and programs must be inherently joint to identify and mitigate interoperability issues that exist between services.

The training strategy necessary to support doctrinal changes to decision making, C2 and other processes implicate the need for greater emphasis on innovation and collaboration in our leader development programs. Information superiority, by itself, does not achieve desired effects on the battlefield. Rather, it requires the ability of leaders at all levels to translate information superiority into decision superiority through collaboration and the innovative application of all capabilities in the battle space. Similarly, empowering smaller, geographically dispersed units to decide and act without the control mechanism current in place requires a new level of risk tolerance. As such, our leader development programs must emphasize a paradigm shift away from risk aversion.

CONCLUSION

> Faith in the unproven potential of technology is not a solid basis for strategy
>
> —General Dennis J. Reimer, CSA, 1997[106]

It is obvious that our strategic leaders believe in the transformational nature of NCW and the potential value of networking. Network-enabled mission enhancements realized during recent combat operations tend to underscore the belief that applying NCW operational concepts provides the ways to achieving full spectrum dominance envisioned in Joint Vision 2020 in an

information dominated 21st Century environment. As General Reimer's statement suggests, however, there is risk in building the Army's transformation strategy around a new concept that, in many respects, is still in its infancy. Similarly, it is clear that the Army has not realized the full potential of this information age concept and does not fully appreciate the impediments or impact it will have on force transformation.

Some contend that the concept of NCW is "already having a profound effect on military operations, and will continue to do so."[107] However, the theory and successful application of NCW concepts are still developing and the known and emerging impediments to realizing its full potential are real and cannot be overcome easily.

Applying the concepts of NCW requires significant investments in C4ISR infrastructure and the maturation of emerging technologies that may not develop at the pace required to support rapid force transformation. Additionally, increased C4ISR investments will reduce funding for other programs. As such, overemphasis on C4ISR without appropriate funding for other programs may result in a transformed force that is not properly balanced to meet the demands of the dynamic global environment. Similarly, increased emphasis on C4ISR will generate a new set of network security issues that the force must content with during the conduct of operations.

Application of NCW has significant implications for Army transformation. It requires the co-evolution and development of radically new doctrine, organizations and training processes and strategies, supported in part by fundamental changes in the application of information technology. Failure to co-evolve these processes will limit the real value gained in a network centric force.

The realities and opportunities of the information age clearly demand that the force transform to maintain readiness and relevance. The potential of NCW operational concepts may provide the ways to revolutionize how the Army operates in a joint, capability-based environment. Maturation of this concept and appropriate attention to mitigating known and emerging impediments, however, is crucial to realizing the full potential of it.

WORD COUNT=6448

ENDNOTES

[1] Donald H. Rumsfeld, Secretary of Defense, Remarks delivered at National Defense University, Fort McNair, Washington, D.C., 31 January 2002; available from <http://www.defenselink.mil/speeches/2002/s20020131-secdef.html>; Internet, accessed 17 October 2003

[2] Department of Defense, *Network Centric Warfare, Report to Congress* (Washington, D.C.: U.S. Department of Defense, 21 July 2001), i. available from <http://www.defenselink.mil/nii/ncw/ncw_main.pdf> Internet, accessed 8 November 2003.

[3] "Network Centric Warfare: Exploiting an Information Edge," *Defence Research and Development Canada* October 2002 [journal on-line], available from <http://www.drdc-rddc.dnd.ca/publications/issues/issues14_e.asp>; Internet, accessed 16 November 2003. The article quotes an address provided by Admiral Jay Johnson at the U.S. Naval Institute Annapolis Seminar and 123rd Annual Meeting, Annapolis, MD, 23 Apr 1997.

[4] "Cebrowski: Joint Philosophy Fosters Network Centric Warfare"., *C4I News* (25 April 2002): 1 [database on-line]; available from ProQuest; accessed 7 November 2003.

[5] Arthur K. Cebrowski, "New Rules for a New Era," White Paper (Washington D.C., Department of Defense Office of Force Transformation), 5.

[6] Arthur K. Cebrowski and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Proceedings* January 1998: 2 [journal on-line]; available at <http://www.usni.org/ proceedings/ articles98/PROcebrowski.htm>; Internet, accessed 16 November 2003.

[7] Dan Caterinicchia and Matthew French, "Network-centric warfare: Not there yet", *Federal Computer Week* 9 June 2003 [journal on-line]; available from <http://www.fcw.com/fcw/ articles/2003/0609/cov-netcentric-06-09-03.asp>; Internet, accessed 24 October 2003.

[8] See Frederick W. Kagan article, "The Art of War," *The New Criterion*, available at <http://www.newcriterion.com/archive/22/nov03/kagan.htm>; Internet, accessed 11 November 2003. Although Kagan acknowledges that NCW provides the means to enhance some military operations, he argues against over emphasizing it as a new way of war. His article highlights some of the challenges with this information age concept – and concludes with the believe that it will do little to fundamentally alter the nature of warfare.

[9] Cebrowski, "New Rules for a New Era": 5.

[10] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* 2nd ed. (Washington, DC: CCRP Publication Series, February 2000), 88.

[11] Robert Metcalfe, the primary architect of the Ethernet protocol, postulated that the potential power of a network is "proportional to the square of the number of people using it." Simply put, each user that is added to a network creates significant growth in potential interactions between existing network nodes. As such, the more users that are connected to the network – the more information you can exchange.

[12] Internet Society, "A Brief History of the Internet," available from <http://www.isoc.org/internet/history/brief.shtml#Origins>; Internet, accessed 22 Nov 2003.

[13] Roger Roberts, "Network Centric Operations", Speech given at the Network Centric Operation 2003 Conference, 2003, Apr 16 2003, available from <http://www.boeing.com/news/speeches/2003/Roberts_030416.html>; Internet, accessed 10 November 2003. Roger Roberts is Senior Vice President, Boeing IDS Space and Intelligence Systems.

[14] Roger Roberts, "Network Centric Operations" Speech, available from <http://www.boeing.com/news/speeches/2003/Roberts_030416.html>; Internet, accessed 10 November 2003.

[15] Arthur L. Money, *Report on Network Centric Warfare Sense of the Report*, March 2001. Available from <http://www.defenselink.mil/nii/NCW/ncw_sense.doc>; Internet, accessed 10 November 2003.

[16] Department of Defense, *Network Centric Warfare, Report to Congress*, iv.

[17] Money, 9

[18] Department of the Army, *Army Vision 2010*, (Washington D.C.; Department of the Army), 1, available from <http://www.army.mil/2010/information_superiority.htm>; Internet, accessed 10 November 2003.

[19] Caterinicchia, 2.

[20] Bradley C. Logan, "Technical Reference Model for Network-Centric Operations," *Crosstalk* , August 2003 [journal on-line]; available from <http://www.stsc.hill.af.mil/crosstalk/2003/08/ 0308logan.html>; Internet, accessed 24 October 2003

[21] Joint Chiefs of Staff, *Joint Operations Concepts* (Washington, D.C.: Joint Staff J-7, November 2003): 9, available from <http://www.defenselink.mil/nii/ncw/ncw_main.pdf> Internet, accessed 8 November 2003.

[22] Joint Chiefs of Staff, *Joint Vision 2020*, (Washington, D.C.: Joint Staff, J-5, June 2000): 11, available from <http://www.dtic.mil/jointvision/jvpub2.htm>; Internet, accessed 10 November 2003.

[23] "Information Superiority Drives Network-Centric Operations," Sun Microsystems Boardroom Minutes, available from <http://www.sun.com/br/government_312/feature_info.html>; Internet, accessed 24 October 2003.

[24] Department of Defense, *Transforming America's Military: Net-Centric Warfare,* White Paper (Washington D.C., Assistant Secretary of Defense Command, Control, Computers and Intelligence) available from <http://www.don-ebusiness.navsup.navy.mil/pls/portal30/docs/folder/DoD_content/documents/asd_C3I_ncw_brochure.pdf>; Internet, accessed 16 November 2003.

[25] "About Network Centric Operations," *Strategic Architecture*, [journal on-line]; available from <http://www.boeing.com/ids/stratarch/about_nco.html>; Internet, accessed 24 October 2003.

[26] Joint Chiefs of Staff, *Unified Action Armed Forces,* Joint Pub 0-2, (Washington, D.C.: Joint Staff J5, 10 July 2001): xiii.

[27] Full spectrum dominance is the defeat of any adversary or control of any situation across the full range of military operations.

[28] Department of Defense, *Joint Vision 2020*, 2.

[29] Department of Defense, *Network Centric Warfare, Report to Congress*, iv.

[30] Ibid, v.

[31] Ibid.

[32] Department of Defense, *Network Centric Warfare - Creating a Decisive War fighting Advantage*, Brochure (Washington, D.C., Director, Force Transformation, Office of the Secretary of Defense, Winter 2003): 1, available from <http://www.oft.osd.mil/library/ library_files/ document_318_NCW_GateFold-Pages.pdf>; Internet, accessed 10 January 2004.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Ibid

[39] Steven W. Boutelle, "Global and Pervasive Information for Joint Warfighters," *Army,* October 2003, 143. Lieutenant General Boutelle is the U.S. Army G6.

[40] Department of Defense, *Transformation Planning Guidance* , (Washington, D.C., Department of Defense, April 2003): 3.

[41] Joint Chiefs of Staff, *An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution In the 21st Century*, White Paper (Washington, DC, Joint Staff, J7: 28 January 2003), 33, available from <http://www.dtic.mil/jointvision/jwcr_screen.pdf>; Internet, accessed 10 November 2003.

[42] Alberts, Garstka, and Stein, 94.

[43] Joint Chiefs of Staff, *An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution In the 21st Century*, 33.

[44] C4ISR is a Department of Defense acronym that stands for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance. Its definition is generally equivalent to the term “enterprise architecture” used in the commercial sector.

[45] Joint Chiefs of Staff, *Enabling the Joint Vision* (Washington D.C.: Department of Defense, Joint Staff, C4 Systems Directorate, May 2000): 12. available at <http://www.dtic.mil/jcs/j6/enablingjv.pdf>; Internet, accessed 22 November 2003.

[46] Ibid, 2.

[47] Jim Garamone, “Joint Vision 2020 Emphasizes Full-Spectrum Dominance”, *DefenseLink* News Article, 2 June 2000, available from <http://www.defenselink.mil/news/june2000/n06022000_20006025.html>; Internet, accessed 10 November 2003.

[48] Robert K. Ackerman, “Special Operations Forces Become Network-Centric”, *Signal Magazine,* March 2003 [journal on-line]; available from <http://us.net/signal/archive/march03/special-march.html>; Internet, accessed 7 December 03.

[49] Ibid

[50] Robert K. Ackerman, “Iraq War Operations Validate Hotly Debated Theories,” *Signal Magazine*, (July 2003): 31, [database on-line]; available from ProQuest; accessed 2 November 2003.

[51] Ibid.

[52] David C. Hardesty, “Fix net centric for the operators,” *Proceedings*, (September 2003): 68, [database on-line]; available from ProQuest; accessed 2 November 2003.

[53] Cebrowski, ”Network Centric Warfare: Its Origin and Future.”

[54] Fredrick P. Stein, “Observations on the Emergence of Network-Centric Warfare”, Information Paper: 3, available from <http://www.dtic.mil/jcs/j6/eduction/warfare.html>; Internet, accessed 16 November 2003.

[55] Kim Burger, “What Went Right,” *Jane’s Defence Weekly* (30 April 2003) [database on line]; available from Jane’s Defence Magazines; accessed 10 January 2004.

[56] Ibid.

[57] Robert K. Ackerman, “Tactical Operations Enable and Benefit from Network-Centric Warfare”, *Signal Magazine*, 15 Oct 2003 [journal on-line], available from <http://www.imakenews.com/signal/e_article000189552.cfm>; Internet, accessed 16 November 2003

[58] Hunter Keeter, “Cebrowski: Iraq Shows Network Centric Warfare Implementation”, *Defense Daily* (23 April 03) [database on-line]; available from ProQuest; accessed 7 November 2003.

[59] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC: CCRP Publication Series, June 2003), 35.

[60] David S. Alberts, *Information Age Transformation: Getting to a 21st Century Military* (Washington, DC: CCRP Publication Series, June 2002): 32.

[61] Ackerman, "Special Operations Forces Become Network-Centric."

[62] Ibid.

[63] Roxana Tiron, "Army's Blue-Force Tracking Technology was a Tough Sell," *National Defense*, (December 2003): 20 [database on-line]; available at ProQuest; accessed 10 January 2004.

[64] Department of Defense, *Network Centric Warfare - Creating a Decisive War fighting Advantage*, 2.

[65] Robert Ackerman, "Special Operations Forces Become Network-Centric."

[66] Matthew French, "Iraq shows IT work needed," *Federal Computer Week* , 5 September 2003: 1 [journal on-line]; available at <http://www.fcw.com/fcw/articles/2003/0901/web-navy-09-05-03.asp>; Internet, accessed 26 October 2003. French credits this statement to Marine Major General James Nattis, commanding general of 1st Marine Division during Operation Iraqi Freedom.

[67] One emerging impediment is the practical matter of increasing the number of Internet Protocol (IP) addresses available for routing on the network to support NCW. Routing (controlled movement of data packets) across the network currently relies on node-unique IP addresses known as IP version 4 (IPv4). IPv4 is a 32-bit addressing scheme that supports approximately 4 billion unique addresses. Most of these are already permanently assigned to specified users. According to the Assistant Secretary of Defense for Networks and Information Integration (ASD-NII) John Steinbit, DoD will need to migrate to IPv6 to support the transition to network centric operations. IPv6 uses a 128-bit addressing scheme that will provide a virtually unlimited number of IP addresses. Although DoD intends to transition to IPv6 by 2008, there will likely be some "speed bumps" along the way that will push this transition out to 2010 or beyond. Similarly, systems that are not compatible with this new protocol will have to be replaced.

[68] Thomas P.M. Barnett provides a good summation of impediments and risks associated with applying NCW in "The Seven Deadly Sins of Network Centric Warfare" published in the U.S. Naval Institute's *Proceedings*, January 1999: 36-39, available from <http://www.geocities.com/researchtriangle/thinktank/6926/7deadly.html>; Internet, accessed 16 November 2003.

[69] David S. Alberts et al., *Understanding Information Warfare* (Washington, DC: CCRP Publication Series, July 2002): 286.

[70] Ibid.

[71] Ibid.

[72] Megan Scully, "Communications Snags Plagued U.S. Troops," *Defense News*, 19 Jan 2004: 8, available from <http://ebird.afis.osd.mil/ebfiles/s20040120250175.html>; Internet, accessed 28 January 2004.

[73] Dawn S. Onley, "Army Reviews Bid for Tactical Net,", *Government Computer News*, 20 May 2002 [journal on-line], available from <http://www.gcn.com/21_11/news/187000-1.html>; Internet, accessed 14 January 2004.

[74] Patrick Rayermann, "Exploiting Commercial SATCOM: A Better Way", *Parameters*, Winter 2003-2004: 54-55.

[75] Ibid.

[76] Ibid.

[77] The Joint Tactical Radio System (JTRS) is a family of software programmable radios that will provide reliable multi-channel voice, data, imagery and video communications, virtually eliminating communications problems caused by stovepipe legacy systems. It is designed to support the attainment of information superiority. A fact sheet on the JTRS is available from <http://jtrs.army.mil/sections/overview/overview.html>; Internet, accessed 3 December 2003.

[78] Alberts, *Information Age Transformation: Getting to a 21st Century Military*, 32.

[79] Network security threats to the envisioned C4ISR infrastructure include both internal and external actors ranging from unsophisticated "script kiddies" to more technologically advanced hackers, terrorists or state sponsored actors. The CRS Report to Congress on Cyber warfare lists China, Russia, France and Germany as examples of state sponsored actors who may use cyberspace to conduct industrial espionage or disrupt the operation critical infrastructure to their advantage. These actors seek to gain unauthorized access to disrupt operations, corrupt data, or steal sensitive information. They employ malicious code to disable networks and use tools to map and exploit vulnerabilities in Microsoft and Unix-based software applications and operating systems that were unintentionally created during software program development. According to statistics provided by the Carnegie Mellon sponsored Computer Emergency Response Coordination Center (CERTCC), over 4,100 such vulnerabilities were reported last year, with the top 10 known vulnerabilities being the most exploited.

[80] "Success in Iraq May Affect Defense C4ISR Investment Plan, New Report Says," *C4ISR News*, 24 June 2003, [database on-line]; available from ProQuest; accessed 7 November 2003.

[81] Frederick W. Kagan, "The Art of War," *The New Criterion*: 8, available at <http://www.newcriterion.com/archive/22/nov03/kagan.htm>; Internet, accessed 11 November 2003.

[82] "Near Term Budget Decisions to Map NCW Approach for DoD," *C4I News*, (30 October 2003) [database on-line]; available from ProQuest; accessed 7 November 2003.

[83] Kagan, 8.

[84] Folke Rehnstrom, "Moving Towards network centric warfare," *Military Technology*, (August 2002) [database on-line]; available from ProQuest; accessed 7 November 2003.

[85] Kagan, 9.

[86] Christopher J. Toomey, "Army Digitization: Making it Ready for Prime Time", *Parameters,* Winter 2003-2004: 49. Colonel Toomey served as Chief, C4ISR and Battle Command, Army Transformation Task Force at Fort Lewis, Washington.

[87] Ibid.

[88] French, 1.

[89] Department of Defense, *Transformation Planning Guidance* , 1.

[90] Department of the Army, *Army Transformation Roadmap*, (Washington D.C.: Department of the Army, 2002): 7, available from <http://www.oft.osd.mil/library/library_files/document_201_army_transformation.pdf>; Internet, accessed 10 January 04

[91] Department of the Army, *The Way Ahead, Our Army at War…Relevant and Ready*, White Paper, (Washington D.C.: Department of the Army, Army Strategic Communications, 2003): 12.

[92] Department of the Army, *Army Knowledge Management Version 2.1, A Strategic Plan for an Agile Force*, White Paper, (Washington D.C.: Department of the Army, 2001): 3.

[93] Alberts, *Information Age Transformation: Getting to a 21st Century Military*, 32.

[94] Department of Defense, *Joint Vision 2020*, 11.

[95] Alberts, *Information Age Transformation: Getting to a 21st Century Military*, 55.

[96] Ted Hendrickson, "Evolution of Technology Aids Cost Estimating," 2 May 2003, available from <http://www.monmouth.army.mil/monmessg/newmonmsg/may022003/m18costing.htm>; Internet, accessed 17 January 2004.

[97] Joint Chiefs of Staff, *Command and Control for Joint Air Operations* Joint Pub 3-30, (Washington D.C.: Joint Staff, 5 June 2003): III-19 – III-21. This reference provides a summary of the current Air Tasking Order (ATO) cycle and targeting processes. It is interesting to note that this doctrinal reference was published after the NCW concept was adopted by DoD as the focus for transformation – suggesting that current doctrine is out of step with the application of NCW concepts.

[98] Joint Chiefs of Staff, *Enabling the Joint Vision*, White Paper, (Washington D.C.: Joint Staff, J-6, May 2000): 16, available from <http://www.dtic.mil/jcs/j6/enablingjv.pdf>; Internet, accessed 22 November 2003.

[99] Department of Defense, *Network Centric Warfare, Report to Congress*, B-1.

[100] Arthur K. Cebrowski and Thomas P.M. Barnett, "The American Way of War," *Proceedings*, January 2003: 42 [database on-line]; available from ProQuest; accessed 16 January 2004.

[101] Jim Garamone, “Joint Vision 2020 Emphasizes Full-spectrum Dominance,” *Defenselink* News Article, 2 June 2000, available at <http://www.defenselink.mil/news/jun2000/n06022000_20006025.html>; Internet, accessed 10 November 2003.

[102] Curt Copley, “A Commander’s Network-Centric Odyssey,” *Proceedings*, January 2003, [database on-line]; available from ProQuest; accessed 16 January 2004.

[103] Clyde T. Wilson, “Training Transformation to Future Combat System (FCS),” *Armor*, (Jan/Feb 2003): 24 [database on-line]; available from ProQuest; accessed 17 January 2004.

[104] Toomey, 43.

[105] Defense and the National Interest discussion board, “Will Army Digitization Work? – Mud Soldiers Sound Off,” available at <http://www.d-n-i.net/fcs/comments/c416.htm>; Internet, accessed 16 January 2004.

[106] Dennis J. Reimer, “Dominant Maneuver and Precision Engagement,” *Joint Forces Quarterly,* Winter 1996-97: 13.

[107] William S. Scott and David Hughes, “Nascent Net-Centric War Gains Pentagon Toehold,” *Aviation Week & Space Technology*, (27 Jan 2003): 50 [database on-line]; available from ProQuest; accessed 16 January 2004.

BIBLIOGRAPHY

"About Network Centric Operations." *Strategic Architecture*. Journal on-line. Available from <http://www.boeing.com/ids/stratarch/about_nco.html>. Internet. Accessed 24 October 2003.

Ackerman, Robert K. "Iraq War Operations Validate Hotly Debated Theories," *Signal* (July 2003): 31. Database on-line. Available from ProQuest. Accessed 2 November 2003.

_____. "Special Operations Forces Become Network-Centric," *Signal* March 2003. Journal on-line. Available from <http://us.net/signal/archive/march03/ special-march.html>. Internet. Accessed 7 December 2003.

_____. "Tactical Operations Enable and Benefit from Network-Centric Warfare," *Signal* 15 Oct 2003. Journal on-line. Available from <http://www.imakenews.com/signal/ e_article000189552.cfm>. Internet. Accessed 16 November 2003.

Alberts, David S. and Hayes, Richard E. *Power to the Edge: Command and Control in the Information Age.* Washington, DC: CCRP Publication Series, June 2003.

Alberts, David S. et al. *Understanding Information Warfare*. Washington, DC: CCRP Publication Series, July 2002.

Alberts, David S., Garstka, John J. and Stein, Frederick P. *Network Centric Warfare: Developing and Leveraging Information Superiority* 2nd ed. Washington, DC: CCRP Publication Series, February 2000.

Alberts, David S. *Information Age Transformation: Getting to a 21st Century Military* Washington, DC: CCRP Publication Series, June 2002.

Barnett, Thomas P.M. "The Seven Deadly Sins of Network Centric Warfare" *Proceedings*, January 1999. Available from <http://www.geocities.com/researchtriangle/ thinktank/6926/7deadly.html>. Internet. Accessed 16 November 2003.

Boutelle, Steven W. "Global and Pervasive Information for Joint Warfighters," *Army* (October 2003).

Burger, Kim "What Went Right," *Jane's Defence Weekly* (30 April 2003). Database on-line. Available from Jane's Defence Magazines. Accessed 10 January 2004.

Caterinicchia, Dan. "Pentagon Identifying Net-Centric Core." *Federal Computer Week* 30 January 2003. Journal on-line. Available from <http://www.fcw.com/ fcw/articles/2003/0127/web-core-01-30-03.asp>. Internet. Accessed 26 October 2003.

Caterinicchia, Dan and French, Matthew "Network-centric warfare: Not there yet", *Federal Computer Week* 9 June 2003. Journal on-line. Available from <http://www.fcw.com/ fcw/articles/2003/0609/cov-netcentric-06-09-03.asp>. Internet. Accessed 24 October 2003.

Cebrowski, Arthur K. *New Rules for a New Era*, White Paper. Washington D.C., Department of Defense Office of Force Transformation.

Cebrowski, Arthur K. and Barnett, Thomas P.M. "The American Way of War," *Proceedings* (January 2003): 42. Database on-line. Available from ProQuest. Accessed 16 January 2004.

Cebrowski, Arthur K. and Garstka, John J. "Network Centric Warfare: Its Origin and Future," *Proceedings* (January 1998): 2. Database on-line. Available from <http://www.usni.org/proceedings/articles98/PROcebrowski.htm>. Internet. Accessed 16 November 2003.

Copley, Curt. "A Commander's Network-Centric Odyssey," *Proceedings* (January 2003). Database on-line. Available from ProQuest. Accessed 16 January 2004.

Defense and the National Interest Discussion Board. "Will Army Digitization Work? – Mud Soldiers Sound Off," available from <http://www.d-n-i.net/fcs/comments/c416.htm>. Internet. Accessed 16 January 2004.

"DOD Suggests Acquisition, Force Structure, Industry Base Be Based on Operational Effects." Defense Daily (11 February 2003). Database on-line. Available from ProQuest. Accessed 7 November 2003.

French, Matthew. "Iraq shows IT work needed," *Federal Computer Week* 5 September 2003. Journal on-line. Available from <http://www.fcw.com/fcw/articles/2003/0901/web-navy-09-05-03.asp>. Internet. Accessed 26 October 2003.

Garamone, Jim. "Joint Vision 2020 Emphasizes Full-Spectrum Dominance", *DefenseLink* 2 June 2000. Journal on-line. Available from <http://www.defenselink.mil/news/june2000/n06022000_20006025.html>. Internet. Accessed 10 November 2003.

Hardesty, David C. "Fix net centric for the operators," *Proceedings* (September 2003). Database on-line. Available from ProQuest. Accessed 2 November 2003.

Hendrickson, Ted. "Evolution of Technology Aids Cost Estimating," 2 May 2003. Available from <http://www.monmouth.army.mil/monmessg/newmonmsg/may022003/m18costing.htm>. Internet. Accessed 17 January 2004.

Huldreth, Steven A. *Cyberwarfare, Congressional Research Service Report to Congress*, 15 December 2000.

"Information Superiority Drives Network-Centric Operations." Sun Microsystems Boardroom Minutes. Available from <http://www.sun.com/br/government_312/feature_info.html>. Internet. Accessed 24 October 2003.

Internet Society. "A Brief History of the Internet." Available from <http://www.isoc.org/internet/history/brief.shtml#Origins>. Internet. Accessed 22 November 2003.

"Joint Philosophy Fosters Network Centric Warfare." *C4I News* (25 April 2002): 1 Database on-line. Available from ProQuest. Accessed 7 November 2003.

"Joint Tactical Radio System Fact Sheet." Available from <http://jtrs.army.mil/sections/overview/overview.html>. Internet. Accessed 3 December 2003.

Kagan, Frederick W. "The Art of War," *The New Criterion*. Journal on-line. Available from <http://www.newcriterion.com/archive/22/nov03/kagan.htm>. Internet. Accessed 11 November 2003.

Keeter, Hunter "Cebrowski: Iraq Shows Network Centric Warfare Implementation." *Defense Daily* (23 April 03). Database on-line. Available from ProQuest. Accessed 7 November 2003.

Kenyon, Henry S. "Large Data Pipes Link Vital Military Centers." *Signal* (October 2003). Database on-line. Available from ProQuest. Accessed 26 December 2003.

_____. "Tactical Web Takes Shape." *Signal* (November 2003). Database on-line. Available from ProQuest. Accessed 26 December 2003.

Leopold, George. "Networks: DOD's First Line of Defense." Electronic Engineering Times 13 October 1997. Journal on-line. Available from <http://www.techweb.com/wire/1997/10/1013dod.html>. Internet. Accessed 16 November 2003.

Logan, Bradley C. "Technical Reference Model for Network-Centric Operations," *Crosstalk*, August 2003. Journal on-line. Available from <http://www.stsc.hill.af.mil/crosstalk/2003/08/0308logan.html>. Internet. Accessed 24 October 2003

"Metcalfes Law." Available from <http://c2.com/cgi/wiki?MetcalfesLaw>. Internet. Accessed 16 November 2003.

Money, Arthur L. *Report on Network Centric Warfare Sense of the Report*, March 2001. Available from <http://www.defenselink.mil/nii/NCW/ncw_sense.doc>. Internet. Accessed 10 November 2003.

"Near Term Budget Decisions to Map NCW Approach for DoD." *C4I News* (30 October 2003). Database on-line. Available from ProQuest. Accessed 7 November 2003.

"Network Centric Warfare: Exploiting an Information Edge." *Defence Research and Development Canada* October 2002. Journal on-line. Available from <http://www.drdc-rddc.dnd.ca/publications/issues/issues14_e.asp>. Internet. Accessed 16 Nov 2003.

"Next-Generation Internet Protocol to Enable Net-Centric Operations." *DefenseLink* 13 June 2003. Available from <http://www.dod.mil/releases/2003/nr20030613-0097.html>. Internet. Accessed 16 November 2003.

Onley, Dawn S. "Army Reviews Bid for Tactical Net,", *Government Computer News*, 20 May 2002. Journal on-line. Available from <http://www.gcn.com/21_11/news/187000-1.html>. Internet. Accessed 14 January 2004.

"Pentagon Ponders Fully Integrated Global Information Grid to Integrate C4ISR Assets." *C4I News* (21 August 2003). Database on-line. Available from ProQuest. Accessed 26 December 2003.

Rayermann, Patrick. "Exploiting Commercial SATCOM: A Better Way", *Parameters*, Winter 2003-2004.

Rehnstrom, Folke. "Moving Towards network centric warfare," *Military Technology*,(August 2002). Database on-line. Available from ProQuest. Accessed 7 November 2003.

Reimer, Dennis J. "Dominant Maneuver and Precision Engagement," *Joint Forces Quarterly*, Winter 1996-97.

Roberts, Roger. "Network Centric Operations" Speech. Available from <http://www.boeing.com/ news/speeches/2003/Roberts_030416.html>. Internet. Accessed 10 November 2003.

_____. "Network Centric Operations." Speech given at the Network Centric Operation 2003 Conference, 16 April 2003. Available from <http://www.boeing.com/news/ speeches/2003/Roberts_030416.html>. Internet. Accessed 10 November 2003.

Rumsfeld, Donald H. Remarks delivered at National Defense University, Fort McNair, Washington, D.C., 31 January 2002. Available from <http://www.defenselink.mil/ speeches/2002/s20020131-secdef.html>. Internet. Accessed 17 October 2003.

Scott, William S. and Hughes, David. "Nascent Net-Centric War Gains Pentagon Toehold," *Aviation Week & Space Technology* (27 Jan 2003). Database on-line. Available from ProQuest. Accessed 16 January 2004.

Scully, Megan. "Communications Snags Plagued U.S. Troops," *Defense News* 19 Jan 2004. Available from <http://ebird.afis.osd.mil/ebfiles/s20040120250175.html>. Internet, accessed 28 January 2004.

Stein, Fredrick P. "Observations on the Emergence of Network-Centric Warfare," Information Paper. Available from <http://www.dtic.mil/jcs/j6/eduction/warfare.html>. Internet. Accessed 16 November 2003.

Stenbit, John P., Department of Defense Chief Information Officer. "Internet Protocol Version 6 (IPv6) Interim Transition Guidance." Memorandum for Secretaries of the Military Departments. Washington, D.C., 29 September 2003.

"Success in Iraq May Affect Defense C4ISR Investment Plan, New Report Says" *C4ISR News* (24 June 2003). Database on-line. Available from ProQuest. Accessed 7 Nov 2003.

Tiron, Roxana. "Army's Blue-Force Tracking Technology was a Tough Sell," *National Defense* (December 2003). Database on-line. Available from ProQuest. Accessed 10 Jan 2004.

Toomey, Christopher J. "Army Digitization: Making it Ready for Prime Time", *Parameters*, Winter 2003-2004.

U.S. Department of Defense. *Network Centric Warfare - Creating a Decisive War fighting Advantage.* Washington, D.C.: DOD Office Force Transformation, Office of the Secretary of Defense, Winter 2003. Available from <http://www.oft.osd.mil/ library/ library_files/ document_318_NCW_GateFold-Pages.pdf>. Internet. Accessed 10 January 2004.

_____. *Network Centric Warfare, Report to Congress*. Washington, D.C.: U.S. Department of Defense, 21 July 2001. Available from <http://www.defenselink.mil/ nii/ ncw/ncw_main.pdf>. Internet. Accessed 8 November 2003.

_____. *Transformation Planning Guidance.* Washington, D.C.: U.S. Department of Defense, April 2003.

_____. *Transforming America's Military: Net-Centric Warfare* , White Paper Washington D.C.: Assistant Secretary of Defense Command, Control, Computers and Intelligence). Available from <http://www.don-ebusiness.navsup.navy.mil/pls/ portal30/docs/ folder/DoD_content/documents/asd_C3I_ncw_brochure.pdf>. Internet. Accessed 16 November 2003.

U.S. Department of the Army. *Army Knowledge Management Version 2.1, A Strategic Plan for an Agile Force.* White Paper. Washington D.C.: U.S. Department of the Army, 2001.

U.S. Department of the Army. *Army Transformation Roadmap*. Washington D.C.: U.S. Department of the Army, 2002. Available from <http://www.oft.osd.mil/library/library_files/ document_201_army_transformation.pdf>. Internet. Accessed 10 January 2004

_____. *Army Vision 2010*. Washington D.C.; U.S. Department of the Army. Available from <http://www.army.mil/2010/information_superiority.htm>. Internet. Accessed 10 November 2003.

_____. *The Way Ahead, Our Army at War…Relevant and Ready*, White Paper. Washington D.C.: U.S. Department of the Army, 2003.

U.S. Joint Chiefs of Staff. *An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution In the 21st Century* White Paper. Washington, DC, U.S. Joint Chiefs of Staff, 28 January 2003. Available from <http://www.dtic.mil/jointvision/jwcr_screen.pdf>. Internet. Accessed 10 November 2003.

_____. *Command and Control for Joint Air Operations*. Joint Pub 3-30. Washington D.C.: U.S. Joint Chiefs of Staff, 5 June 2003.

_____. *Enabling the Joint Vision* , White Paper, Washington D.C.: U.S. Joint Chiefs of Staff, May 2000. Available from <http://www.dtic.mil/jcs/j6/enablingjv.pdf>. Internet. Accessed 22 November 2003.

_____. *Joint Operations Concepts.* Washington, D.C.: U.S. Joint Chiefs of Staff, November 2003. Available from <http://www.defenselink.mil/nii/ncw/ncw_main.pdf>. Internet. Accessed 28 November 2003.

_____. *Joint Vision 2020*. Washington, D.C.: U.S. Joint Chiefs of Staff, June 2000. Available from <http://www.dtic.mil/jointvision/jvpub2.htm>. Internet. Accessed 10 November 2003.

_____. *Unified Action Armed Forces*. Joint Pub 0-2. Washington, D.C.: U.S. Joint Chiefs of Staff, 10 July 2001.

Wilson, Clyde T. “Training Transformation to Future Combat System (FCS),” *Armor* (Jan/Feb 2003). Database on-line. Available from ProQuest. Accessed 17 January 2004.