USAWC STRATEGY RESEARCH PROJECT

NETWORK CENTRIC WARFARE AND THE CHANGING ROLE OF THE SIGNAL CORPS

by

Colonel Mike Thorne
United States Army

Colonel James H. Thomas
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

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **03 MAY 2004**	2. REPORT TYPE	3. DATES COVERED **-**
4. TITLE AND SUBTITLE **Network Centric Warfare and the Changing Role of the Signal Corps**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Mike Thorne**		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT **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 **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**30**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

ABSTRACT

AUTHOR: Colonel Mike Thorne

TITLE: NETWORK CENTRIC WARFARE AND THE CHANGING ROLE OF THE SIGNAL CORPS

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 30 CLASSIFICATION: Unclassified

This research paper will explore the missions and construct for Army future force information and knowledge management organizations as part of a network centric information infrastructure. The Network Centric Information infrastructure will herald in a new paradigm for the Army Signal Corps—it no longer will be just a communications provider. Through the implementation of enhanced technologies and the adoption of a network centric approach, we can obviate the need for communications installers and maintainers on the future battlefield. This requires a vision predicated on dramatically changing the Signal Corps, as we know it. We must "begin with the end in mind" and recognize that technology and new doctrine will allow us to move to this new paradigm. We can field a future force with embedded communications capabilities thereby allowing the Signal Corps to move into the arena of joint information and knowledge management. This will require specialized training, but not a unique force to implement. We can mold Military Intelligence (MI), Information Operations (IO), and automation officers into a cohesive team of knowledge management professionals that will be the core of the new Signal Corps. Professional Army communicators must embrace new missions and define a new paradigm or find themselves in forced obsolescence. This paper will propose a feasible course of action that will facilitate the development of a network centric information infrastructure in support of the future force. Furthermore, the paper will present the benefits of transforming the core mission of the Signal Corps to one of knowledge management in keeping with the overall implementation of a network centric system in an era of joint interdependence.

TABLE OF CONTENTS

ABSTRACT ..... **III**

LIST OF ILLUSTRATIONS ..... **VII**

NETWORK CENTRIC WARFARE AND THE CHANGING ROLE OF THE SIGNAL CORPS **1**

- **NETWORK CENTRIC OVERVIEW** **2**
- **NETWORK CENTRIC WARFARE** **5**
- THE GLOBAL INFORMATION GRID (GIG) AND JOINT VISION 2020 7
- **ANALYSIS AND TECHNOLOGY REVIEW** **8**
- **RECOMMENDATIONS** **10**
- THE FIRST STEP – JOINT INTERDEPENDENCE 10
- STEP TWO – NEW SYSTEMS AT CORPS AND BELOW 12
- STEP THREE: IMPLEMENTING KNOWLEDGE MANAGEMENT (KM) 15
- **IMPLICATIONS** **16**
- **CONCLUSION** **17**

ENDNOTES **19**

BIBLIOGRAPHY **21**

LIST OF ILLUSTRATIONS

FIGURE 1. NETWORK CENTRIC INFORMATION GRID 2

FIGURE 2. INTERCONNECTED FUTURE FORCE 8

FIGURE 3. ARMY TRANSFORMATION 10

NETWORK CENTRIC WARFARE AND THE CHANGING ROLE OF THE SIGNAL CORPS

> Foresight is the ability to see the problems of the future and to solve those problems with solutions that are beneficial in both the short term and the long term.
>
> —Thucydides

The creation of the Signal Corps and its use in the Civil War contributed to a technological revolution in military affairs (RMA) in the latter part of the 19th century. While innovations such as the use of the railroad also contributed to this RMA, information technology proved to be a crucial enabler during the war. The essential contribution in the area of information technology was the introduction of the telegraph. This innovation framed to a large degree the approach to command and control that has remained to this day. During the Civil War, commanders in the field could communicate reliably and quickly with their strategic leaders. Indeed, Abraham Lincoln used the telegraph extensively to communicate with his generals in the field. His purpose was threefold. First, he could understand what was occurring on the battlefield; second, he could provide guidance to his commanders; third, the telegraph enabled him to set up what was arguably the first command and intelligence center to analyze the battlefield situation in light of other information available. Indeed, as one office manager describes Lincoln's approach to the telegraph, "He almost lived in the telegraph office when a battle was in progress."[1] This first Information Technology (IT) based command post had an immediate impact on Lincoln's ability to prosecute the war and changed how wars were fought. It is now time, through a network centric approach, to revise this 19th Century approach to command, control, and information dissemination.

Three important themes are guiding the current revolution in military affairs and are the basic guidelines for the recommendations in this paper. The three themes are transformation in general, the focus on jointness, and the desire to take advantage of network centricity as we proceed into the Information Age. This paper assumes that network centricity is a fundamental aspect of the current revolution in military affairs and will be implemented to some degree. The paper will not argue in detail the merits of network centricity or the benefits of its future implementation. The paper will recommend areas requiring action in the very near term to ensure network centricity is implemented efficiently and in keeping with the stated goals of the Department of Defense. This paper will mainly focus on specific actions the Army must take in transitioning to network centricity.

The major focus of this paper will be to highlight how the US Army Signal Corps, through near term changes in mission and organization coupled with a long term change in the

approach to future procurements, can ensure the successful implementation of a network centric information infrastructure as the Army and the Department of Defense (DoD) transforms. To set the stage, it will be necessary to review some basic tenets and concepts of network centricity, network centric warfare (NCW) and knowledge management (KM). It will also be necessary to review service plans for implementing NCW, key aspects of DoD transformation, the Global Information Grid (GIG), and Joint Vision 2020 (JV2020). It is not possible to explain each of these in detail but is important to introduce them to provide a context for the basis for the conclusions of the paper.

NETWORK CENTRIC OVERVIEW

In nearly every document describing the future, optimum use of the communications and information network receives considerable mention. Implementation of a network that enables the future force usually leads to a discussion of network centricity and network centric warfare. This paper presumes that with network centric warfare will take primacy in terms of the military implementation of network centricity. Before discussing the area of network centric warfare, it is important to review the basics of network centricity itself. The essential aspects of network centricity relevant to this paper are the following:

- Sensors and Actors
- Knowledge Management (KM)
- Simultaneous development

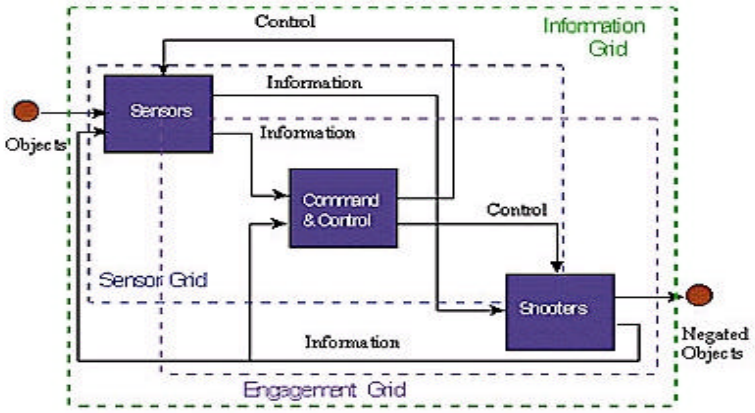

FIGURE 1. NETWORK CENTRIC INFORMATION GRID

The above diagram combines some of the important concepts of network centricity with that of network centric warfare. In the overall context of a network centric environment, three distinct grids are highlighted. The first is the Information Grid, typically referred to as the physical infrastructure (processing, storage, and flow of information) that enables NCW. The second grid, the Sensor Grid, is the collection of sensors that enables battlespace of situational awareness through the input of data. Finally, the Shooter Grid comprises the operational planning and execution community. [2] All processes within the overall information grid are enabled by the presence of and access to information. In the diagram, the actors are the shooters – they act on the information and as such are the target audience for information in the overall NCW environment. The concept of command and control (C2) is an integral part of both network centricity and NCW as the conduit between the communities of sensors and shooters. The C2 arena is where the access to knowledge will prove the most valuable.

The network centric construct is enhanced by the power of knowledge management (KM) and by the simultaneous or mutual development in the implementation of the system. To optimize this construct, all members and systems must be both interconnected and part of the information infrastructure by design. Central to successful network centricity and, by extension NCW, is the concept of networking knowledgeable participants. Simply having information "out there" on the information grid serves little purpose. Sharing knowledge enables collaboration and provides a superior information position over the enemy. FM 100-6 describes information as "Data collected from the environment and processed into usable form" and knowledge as "Information that has been tested and accepted as factual."[3] Differentiating knowledge from information is valuable in the network centric construct given the voluminous amounts of data and information residing in the overall information infrastructure.

An instructive practical NCW example might be the success a cement company achieved by using a network centric approach while empowering subordinates to use information as a way to gain advantage in the marketplace. The company, Cemex, was in the ready-mix cement business characterized by an environment of rigid time schedules and seemingly endless delays (due to road conditions, etc). This resulted in an on-time delivery rate of less than 35%. The leadership decided to implement an approach that combined extensive networking and the empowerment of subordinates. Cemex used a variety of networking means such as cell phones and GPS combined with a knowledge center (for ensuring data on customers was correct) to provide their drivers with information concerning delivery locations and routes that was relevant and timely. The drivers had the authority to act on this information at their discretion during the order and delivery process to determine which driver should fill a particular order. The result

was a system that was so efficient at delivering cement (98% on-time delivery rate) that the company offered a 20% discount if the cement was more than 10 minutes late.[4] The real key, decentralized decision making, was made possible through the implementation of a knowledge management and distribution system focused on the particulars of this industry given the environment they needed to operate within. Cemex did not set out to fix the roads or modify the process for making cement – they simply implemented a system to overcome obstacles using information, communications and knowledge. The use of this approach changed many aspects of the way the company did business and resulted in the company increasing its position in the market.

There must be an "actor" in the overall construct responsible for knowledge management. KM is "the systemic processes by which knowledge needed for an organization to succeed is created, captured, shared, and leveraged"[5]. Knowledge management is central to the implementation of network centricity and effective C2. Without knowledge processes and management, raw information could potentially float throughout the network in a haphazard manner. Trust in the information would be at a minimum since the sheer volume of unprocessed information would be vast on an undisciplined network. The link between knowledge management, information management, communications, and network centricity has yet to be fully explored or exploited. It is critical that the processes that result in the collection and dissemination of knowledge are defined in a network centric environment. It is also critical that a professional body of "knowledge managers" step forward and define the doctrine and processes necessary to ensure knowledge collection, storage, and dissemination. In short, "communicating knowledge is a process".[6] The ability to ensure information from the sensors (and everything is a sensor) is turned into knowledge capable of access as relevant, timely, and accurate information is critically important. KM is key to the success of a network centric environment and entails the secure storage and retrieval of information, the display of information, and in the aggregate the management and control of the requisite information infrastructure. Accomplishment of the KM mission will be key to the operational success of the future force.

Another key to implementing NCW is to construct an information infrastructure that optimizes information exchange. To evaluate the ability to facilitate information exchange between sensors and actors in the network, an approach is to look to Metcalf's Law which states that "as the number of nodes in a network increases linearly, the potential value of the network increases exponentially as the square of the number of nodes in the network".[7] It is critical that every part of the overall system be included in the information infrastructure to

achieve a network centric approach. This allows for a superior information capability which contributes immeasurably to achieving the goal of information superiority and information dominance. We create an information advantage through the construct of our information infrastructure and devise systems to exploit the information, which gives us the advantage required for information dominance.

It is important to note that while everything is intended to lie within the information grid, this is simply not possible. The classic Clausewitzian "fog of war" will continue to some extent. There will be actors that should be part of the system that will not participate in the overall information grid. There will be actionable information not contained in the overall body of knowledge and this fact will have to be considered as analysis is done on the knowledge that does exist in the network. The goal remains to have everything possible exist as part of the information infrastructure and to minimize those actors or sensors that do not participate. Minimizing the non-participants must remain an objective. The focus then, is to ensure that we do not intentionally place non-participants within the realm of the information grid.

NETWORK CENTRIC WARFARE

Network-centric warfare was introduced to most of us in the 1998 article "Network Centric Warfare: It's Origins and Future," in *Proceedings of the Naval Institute*.[8] 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 is measured in terms of four principal competitive attributes: functionality, reliability, convenience, and cost.[9] In combat operations, this value can be measured in terms of key attributes of combat power, such as survivability, lethality, speed, timeliness, and responsiveness.[10]

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. [11] 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 represents a powerful set of warfighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner. NCW operations can be hierarchical or collaborative or a combination of decisional styles needed to meet the commander's intent.[12] NCW is defined as,

" a concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."[13]

It is important to note that some critics of NCW see it as an impossible plateau to reach and consistently use the terminology incorrectly to ridicule the overall concept. For example, according to Frederick Kagan, military historian and author, "NCW thus aims to use the "near-perfect" intelligence that American satellites, aircraft, unmanned aerial vehicles (UAVs), and other "sensors" are supposed to permit commanders to identify the right targets and destroy them with precision-guided munitions."[14] The implication is that the intelligence apparatus is what is responsible for the increased situational awareness and that all of this only serves the purpose of delivering precision guided munitions. From this precept, he goes on to say, "The dubiety of the concepts of perfect intelligence and "predictive battlespace awareness" are more troublesome."[15] He swiftly moves from "near-perfect" to "perfect" in terms of describing NCW required intelligence.

What Kagan fails to consider is that in a network centric environment, as depicted earlier, nearly everything is a sensor that contributes to the overall information available throughout the network. This "emergence of sensor-based warfare" as envisioned by VADM Arthur Cebrowski, Director of Force Transformation, places sensors in the position of primacy in the implementation of our network and moves the sensor to a position of critical importance as a part of the maneuver force.[16] The sensors in this environment exist as more than part of a target acquisition system or as part of a narrowly focused intelligence system. The intelligence apparatus as we know it today as a stove-piped community is not a network centric organization. Everything in the network centric paradigm contributes to the information and knowledge available on the network. Kagan has a point but only if we attempt to implement network centricity piecemeal or in a haphazard manner. The danger is that we will pursue network centricity, but we will implement parts of it without implementing the whole. In this case, Mr. Kagan's pessimism will prove out. A partially implemented network centric information infrastructure may be worse than remaining with the status quo. However, as stated earlier, this paper assumes we are pursuing a network centric information infrastructure and will propose near and far term means toward achieving that end.

THE GLOBAL INFORMATION GRID (GIG) AND JOINT VISION 2020

Joint Vision 2020 identified the GIG as an important enabler of information superiority. The GIG will play an essential 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 and timeliness of information sharing. The GIG Capstone Requirements Document (CRD) further defines the GIG as: A set of globally interconnected, end-to-end information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.[17] In the final analysis, the "GIG is all about enabling the flow of information."[18]

The Defense Information Systems Agency (DISA) has begun to reorganize to help the Defense Department achieve network-centric operations and better align activities with DOD agencies. DISA is restructuring in five areas: acquisition, engineering, operations, finance and governance. "We will now have an organizational structure that positions us to be [DOD's] provider of end-to-end, global net-centric solutions," said DISA's director, Air Force Lt. Gen. Harry Raduege, in a statement.[19] DISA must adjust to remain relevant, said Raduege in a memo to some agency employees. "We must continue to guarantee our forces global information dominance by providing interoperable, secure capabilities to our customers on a daily basis as we transform ourselves for future success." [20]

JV 2020 is firmly grounded in the view that the US military must be a joint force capable of full spectrum dominance and recognizes the centrality of information technology to the evolution of not only our own military, but also the capabilities of other actors around the globe. Information, information processing, and communications networks are at the core of every military activity. Throughout history, military leaders have regarded information superiority as an essential enabler of victory. The transformation of the joint force to reach full spectrum dominance rests upon information superiority as an essential enabler. Information superiority is defined as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[21]

The foundation of jointness is service competencies pulled together. The objective in implementing a joint vision is the optimal integration of joint forces and effects. The interdependence of the services requires mutual trust and reliance and a significantly improved level of interoperability – especially in the areas of command and control and sustainment. Interdependence will ultimately result in a whole greater than the sum of its parts. The synergy gained through interdependence makes clear that jointness is more than interoperability. [22]

ANALYSIS AND TECHNOLOGY REVIEW

Any discussion of communications capabilities eventually revolves around bandwidth. Nearly every after action report (AAR) from both peacekeeping and warfighting operations identifies bandwidth as a major issue during the operation. Operation Iraqi Freedom (OIF) interviews and AAR's mention the need for more satellite access and more bandwidth.[23] The standard solution is to increase the amount of satellite usage both intra-theater and inter-theater. The current Army CIO/G6 has continued to push for increased satellite access to the point that very high ranking officers on the Army staff have stated that terrestrial communications capabilities will no longer be funded.[24] While improved use of satellite assets can improve access to communications, this approach is not network centric and cannot be depended on to form much more than the minor backbone of a network centric infrastructure.

A quick review of the various service NCW approaches reveals some common threads that are important in relation to this paper. The first theme that is evident is that each service individually recognizes the power and importance of NCW and by extension Network Centric Operations. The second theme is that each service desires to take advantage of the power of NCW to enhance service capabilities in support of service missions. Finally, each service recognizes that implementation of NCW is in accordance with JV 2020 and supports their transformational objectives. On the surface, this is the good news. Each service embraces NCW and recognizes the importance of NCW and JV 2020. For example, the Army is transforming itself to meet the challenge of reaching the goals of *Joint Vision 2020* and the Army Vision. The *Joint Vision* recognizes that to be faster, more lethal, more precise, and more effective than today, the U.S. must continue to invest in new military capabilities. The Army has focused its implementation of NCW on the capabilities of the Future Combat System (FCS).[25]

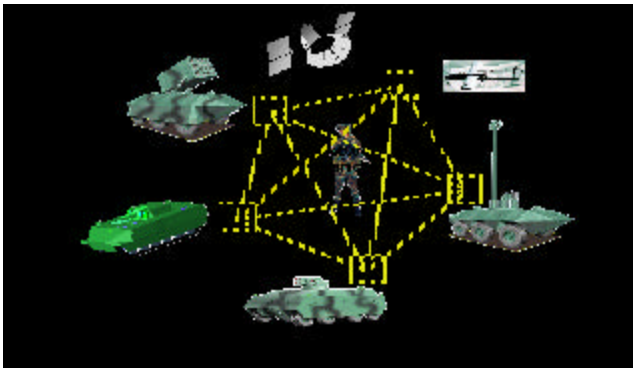

FIGURE 2. INTERCONNECTED FUTURE FORCE

The shortfalls in each of these service plans both in terms of transformation and NCW is that there is no mention of relying on true interdependence and true jointness in the pursuit of NCW or the objectives of JV 2020. No service identifies any areas where they should pursue consolidations of missions with a sister service in the pursuit of network centricity. No service looks to the creation of Joint organizations, to include the relinquishment of a service capability to a Joint Agency, as a possibility on the path toward network centricity. This is a serious shortfall and points out that truly embracing JV 2020 may in fact be something that the services may not be willing to do. Possibly, an even greater shortfall is the omission of the development of any future programs specifically to be network centric. These two shortfalls, lack of true jointness and lack of a focus on developing future network centric platforms, may ensure we never reach the capability to implement network centric warfare at all.

Realizing the full potential of the implementation of a network centric approach to warfare in terms of the communications information infrastructure will require adherence to two seemingly diametrically opposed philosophies. The first philosophy has to do with optimizing existing systems and organizations with a focus on optimizing opportunities for interdependence. The second philosophy is simply adhering to the basic premise of beginning with the end in mind. Stephen Covey describes this as "to start with a clear understanding of your destination."[26] That is, before beginning a task, first determine the end-state. In this case, network centricity is the end state. Therefore, before engaging in any new programs, we must ensure adherence to the basic premises of network centricity. The two philosophies must be implemented near simultaneously but at different echelons and with respect to different aspects of the network. Therefore, in one instance, we must optimize what currently exists while in the second instance we completely change how we develop our future system to ensure network centricity. In both instances, a significant mindset or paradigm shift will be required to implement the change. However, each shift in philosophy embraces the three drivers of the current RMA that have yet to be fully implemented.

It is important to note that the integration of these two philosophies fits well with the new construct and approach for Army transformation. The emerging guidance is to enable the current force while defining the future force – leveraging technology and information in each case. The figure below highlights this approach by depicting enhanced capabilities for the current force while depicting accelerated development across the range of DOTMLPF (Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities) in an enabled and interdependent network centric force.

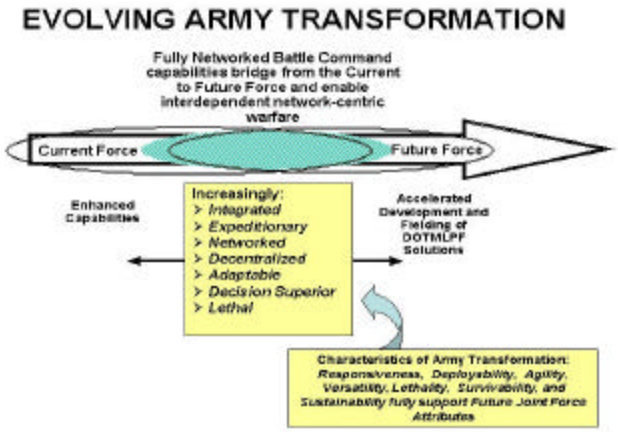

FIGURE 3. ARMY TRANSFORMATION

RECOMMENDATIONS

THE FIRST STEP – JOINT INTERDEPENDENCE

While it seems all of the doctrine and directives drive the services to network centricity and interdependence, the reality is that there is little real effort to arrive at the desired end state. The first paradigm that will have to change is the tradition of assigning joint information infrastructure missions to Army headquarters as part of the responsibilities of the Army Component Command. Traditionally, the Army Service Component Command (ASCC) as a subordinate command of a regional combatant commander or sub-unified commander is tasked with providing a theater level information infrastructure. This construct has resulted in commands and organizations focused on providing Army communications capabilities for a given theater. These capabilities include tactical forces and theater specific communications organizations that provide communications services as a routine mission. Service and other theater wide responsibilities may still prove applicable in the ASCC construct. However, the interdependent communications mission should move to a global, joint organization. Theater level is the optimum place to begin implementing a joint interdependent information infrastructure primarily because the resources are in place and the requirements for support are similar at this level across all services.

The major disconnect at the theater level with respect to network centricity is that each of the services has been given the authority and mission to provide their own communications network capabilities to support posts, camps, and stations separate and distinct from the GIG.

The requirement is to be interoperable with the GIG and to ensure the systems fielded can communicate within and across the GIG. True network centricity and compliance with Joint Vision 2020, however, would suggest an alternative approach to the establishment of the network at the theater level. An alternative is to replace the duplication of having the services each responsible for their networks with an approach that has the network at the theater level (whether in CONUS, forward based, or deployed) fully the responsibility of DISA. Implementing this approach in the near term would result in both a more streamlined network and one in compliance with Joint Vision 2020 and NCW. Clearly DISA, at least in terms of vision and organizational flexibility, is moving toward the realization that extending the GIG is their mission and they are posturing themselves to fully embrace all of the nuances of this capability.

Currently the services maintain their own theater level communications commands. Additionally, Army Material Command (AMC) and the Army's MI Corps each have their own theater level communications units. AMC calls their communications units the Logistic Support Element. Army Intelligence community depends on its Trojan Spirit system to support the Joint Warfighter Intelligence Communications System (JWICS). There are even initiatives in the medical and other communities to field their own deployable and sustaining base communications capabilities. Finally, there are a variety of special purpose units that support special operations missions. Each of these units has as its basic purpose the requirement to provide connectivity back into the GIG and each does this in its own stovepipe fashion and does not routinely share its capabilities with any other customer. This is at odds with the fundamentals of Network Centric Warfare, the precepts of the GIG, and the purported goal of interdependence and jointness. Each service information provider procures its own equipment and trains its own personnel. They do share common technical standards and protocols and the need to access DISA controlled assets as part of the GIG. Additionally, each places its own burdens on the already overcrowded electromagnetic spectrum to include the requirement for use of sparse satellite assets.

An example of the inefficiency of the current system could be the deployment of Task Force (TF) Hawk and the Albanian humanitarian mission to Albania in the spring of 1999 during the war in Kosovo. During this deployment Army theater level and Corps assets were deployed in support of TF Hawk which primarily consisted of the V Corps headquarters, two Attack Helicopter Battalions, and the force protection and logistics assets required for support. Additionally, LSE, medical communications, and Trojan Spirit assets were deployed for TF Hawk. Across the runway in Albania, the AF deployed theater communications assets in support of a humanitarian support mission tasked to the Air Force. It was possible to

interconnect all of these systems based on common protocols and interfaces. However, the various customers did not allow for the systems to be interconnected or to share bandwidth out of theater into the GIG via DISA controlled access points called Strategic/Tactical Entry Points (STEP) sites or teleports. A minor amount of switching interconnectivity was authorized between the circuit switches of the Army and the AF. Even this proved problematic and was not reliable for a variety of procedural reasons mostly related to the separate interconnectivity into the GIG via the reachback to various DISA STEP sites. A single provider could have executed this mission much more efficiently and effectively.

Taking full advantage of the power of network centricity, interdependence, and transformation dictates a recognition that the provision of communications, especially at the theater level, must be joint and must be the responsibility of the organization tasked with implementing the GIG. For example, NETCOM (Network Enterprise Technology Command) has the mission of operating the Army's portion of the GIG and for providing theater level communications services for the Army. The theater level network is their primary focus both in terms of operations and in terms of protection of the network.[27] Theater level tactical Signal units that are an integral part of NETCOM should be consolidated with Air Force and other theater communications organizations as part of DISA. The remaining part of NETCOM that must be subsumed by DISA is the garrison support organization (regional Directors of Information Management (DOIM's) and Regional Chief Information Officers (RCIO's)). These pseudo-battalions and organizations should be completely civilianized and subsumed into DISA or outsourced altogether.

The start point for this implementation, and one that can be implemented in the near term, is the consolidation of service theater level communications units into one Joint Grid Extension Command that works for DISA. The prototype for this type of unit exists today in the form of the Joint Communications Support Element (JCSE) stationed at MacDill AFB, Florida. The JCSE is capable of providing communications for any theater level contingency regardless of service or agency customer.

STEP TWO – NEW SYSTEMS AT CORPS AND BELOW

Echelons Corps and Below (ECB) units are typically those units in the Army that conduct major combat operations and are generally viewed as the tactical level of war. This is the focus of the future force and most transformation initiatives. The efforts ongoing to transform the Army into the future force mirror past efforts. Primarily, the focus is on technology insertion to allow the current force to attain greater capabilities while at the same time stovepipe efforts are

ongoing within a variety of communities to define their role in the future force. The technology insertion for the current force is laudable and should continue. However, the flawed stovepipe approach to the development of the future force is anathema to ensuring the force can achieve the goals of a network centric force.

The very nature of network centricity is the simultaneous development and employment of the system to achieve a true system of systems. The network must include all possible actors and sensors to achieve network centric operations. These systems must be "born" network centric and not just grow to be network centric if we are to achieve true interdependence and synergy inherent in network centric operations. It is in the development of a network centric system where we need to alter the Future Combat System (FCS) approach. General Yakovac (Deputy Assistant Secretary for Army Acquisition Logistic and Technology) stated that "FCS is really an enabler of systems, a family of systems that really fit within a new organization, right now identified as a unit of action. It is a grouping of materiel solutions that really forms the backbone of this unit of action."[28] This approach implies that communities, like the Signal community, can develop their systems for inclusion into the overall system of systems. The relatively new acquisition process of appointing a Lead Systems Integrator (LSI) further reinforces this approach. The LSI is a contractor charged with developing the system of systems architecture and then integrating everything into an overall system. While this could be successful and result in a network centric overall system, a more pessimistic (or realistic) appraisal might be that this approach will result in a myriad of interface issues given the need for a ubiquitous network capability.

The communications systems in development for future force employ models used to develop the current family of communications systems used at ECB known as Mobile Subscriber Equipment (MSE). MSE is a point-to-point communications system relying on extensive installation and micro-management by literally hundreds of Signaleers. In many instances, Signaleers must operate these nodes absent any local subscribers. In instances where nodes are located with subscribers, the resultant Signal signature (in terms of people, equipment, and electronics) is sometimes larger than the subscribers the node supports. In both instances, the Signal infrastructure creates force protection and logistics problems not resident with a different architecture and approach. The other major characteristic of our current system is that a far greater number of actors or participants in the system have no network connections. These actors have no ability to communicate and therefore cannot participate in a network centric environment. Furthermore, some of the actors in our current system are not networked in the network centric sense but are only able to network within their own

communities of interest. This is entirely at odds with the network centric concept. Indeed, the fact that these two communities (no network connection and “stovepiped” communications connections) exist and continue in development is at odds with the concept of network centricity, Jointness, and transformation. Finally, the Army's tactical implementation of net centricity is likely to go into initial fielding without KM-enabled capabilities.

An alternative approach is to develop a system that is network centric from the beginning. The proposed approach emphasizes a large number of small information transfer mini-nodes incorporated into the fighting and support systems being fielded. This smart system would not require large terrestrial manned nodes that often impose constraints on the warfighter in terms of location and pace of maneuver. This new approach would mandate that every actor in the system serve as a communications node or relay and a sensor in addition to performing its primary mission. An example would be that every vehicle developed and fielded would have some level of network communications capability inherent in its design. This would enable every vehicle or weapons system to both serve as a communications platform and as a communications relay device as part of the overall network. This would be truly network centric and would facilitate network centric operations at every echelon. The result would be the enabling of a self-synchronizing structure inherent in all network centric implementations.

The basic concept is that everyone is a communicator much in the same way we have all become telephone operators and installers in our civilian lives. At one time, the telephone company provided the service of providing the telephone and all the wire required to support the telephone into our homes. Additionally, the telephone company provided operators that had to connect every call. At one point, the thought was that an operator was needed for everyone that had a telephone. Of course, technology solved this problem to some extent through the invention of manual and then automatic switching. Eventually, even the terminal instrument got smarter and standards improved such that anyone could install a telephone line in a house with very little training. We all became telephone installers and operators. The telephone company was then free to focus on long distance and data service. Eventually, they offered a variety of other services and information/knowledge via a global network.

In the tactical environment, three macro-level pieces of the overall system will make this paradigm work. The first piece is the wiring of all assemblages (analogous to the house) for network communications capability. The second aspect is that the ability to reach the global network when a major system is too far from a connection (like using the range extension unit) must be part of the system. Finally, network and knowledge management becomes even more critical. The role then for communications units will be limited to the need for additional range

extension between dispersed nodes. Implementing network centric concepts at the tactical level will require a paradigm shift in terms of how we develop communications systems. All tactical assemblages and systems should function as sensors, actors, and communications media. The current paradigm of a relatively small number of large communications nodes should give way to a new network centric paradigm of a large number of small dynamically interconnected nodes that act as both sensors and communications media. Every vehicle on the battlefield must have one of these sensor/communications devices. This will allow for a level of interconnectivity that both provides information and serves as a communications device for the overall network.

STEP THREE: IMPLEMENTING KNOWLEDGE MANAGEMENT (KM)

An important first step in this process is the implementation of Army Knowledge Online (AKO). While most in the Army consider this as simply a web page or e-mail service, AKO with its collaboration capability can become the initial KM capability for both the Army and the joint future force. AKO currently has over 1.6 million users who primarily use AKO and the classified version (AKO-S) to exchange electronic mail across all echelons strategic to tactical. Important applications in the areas of personnel and logistics are already moving to the AKO site allowing access to personnel records, etc. never possible in the past. Applying this approach and technology to operational and intelligence areas will reap similar benefits in terms of productivity and access to information. In operational arena's, as staffs become distributed and information therefore becomes more distributed, maintaining access to stored information will become even more critical. Maintaining repositories of distributed information will allow for changes in the way the future force conducts command and control and may allow for reductions in echelons of command. Each of the other services has implemented a similar web based collaboration and information system that has KM-style capabilities. The Chief Technology office (CTO) of Army CIO/G6 has worked with the other services as they implement their versions of AKO.

Further evolution of KM looks to ensure that a viable KM infrastructure is resident at the appropriate levels of the command structure. As we refine the organization of the headquarters of the future force, a knowledge management cell must be a viable and fully functional part of that staff. Current proposals from a variety of future-thinking headquarters are advocating a different staff structure from the traditional command and staff structure we have used for over a century. Typically, these staffs are more distributed and less stove-piped than traditional staffs and use as a premise nearly ubiquitous access to information. However, most staff designs fail

to include a robust KM organization as part of the overall structure. Knowledge management represents the future of the Signal Corps as we transition to a network centric information infrastructure.

In summary, we should combine strategic communications assets and assign this mission to DISA. We should insist that the FCS and future aircraft and tactical vehicles be developed with integrated communications and sensor capabilities. We can field a future force with embedded communications capabilities thereby allowing the Signal Corps to move into the arena of joint information and knowledge management. Finally, we should implement knowledge management at all levels of the force with the lead going to the new 21st century Signal Corps. This will require specialized training, but not a unique force to implement.

IMPLICATIONS

Implementing these recommendations will have various degrees of impacts on the Doctrine, Organization, Training, Mission, Leader development, Personnel, and Facilities (DOTMLPF) for the Army and the other services. The major changes will certainly take place at ECB although some significant changes will need to take place at theater level as well. The theater level changes inherent in assigning DISA the theater level communications mission in the short term will involve mission and organizational changes for DISA and the Army. A macro level overview of these changes is inherent in the recommendation presented. To implement the recommendations, to include KM, will require significant changes in some aspects of DOTMLPF and will involve a significant investment in terms of procurement dollars. Key changes will be required in all areas of DOTMLPF but specifically in the areas of areas of training, organization, and leader development.

Network Centric and knowledge based organizations are characterized by the need for decision making at the lowest level. Decision making and leadership at the individual, section/squad, and platoon level is enhanced through implementation of network centricity and knowledge management. To gain full advantage, however, training for junior leaders – both officer and enlisted, will have to change. This emphasis on junior leadership and decision making is often touted by Army senior leadership and is something most units in the Army strive for. However, it becomes even more essential in the network centric environment as is evidenced by the CEMEX example presented earlier. Leaders must understand the uses of the information at their disposal and have the flexibility to act on the knowledge resident in the system to gain advantage over the enemy either directly or indirectly. Direct advantages will be in terms of using information to support maneuver, fires, or other effects. Indirect advantage

can come in the increased efficiency and effectiveness of the leader's unit that will come from a better understanding of the leader's surroundings.

The cost of implementing the recommendations herein will be extensive at ECB and negligible at theater level. Theater level costs will likely come in the form of the reorganization and restationing of various units to ensure the capabilities required are provided both efficiently and effectively. The cost of including a sensor/communications device in every assemblage will at first seem prohibitive. However, the concept of opportunity cost must be included in the calculation. Opportunity cost is the cost of the loss of capability that results in not doing one thing in favor of doing another. In this case, the price of not implementing a fully robust network centric environment on the battlefield and the resultant loss of the promise of achieving information dominance must be assessed and compared to the cost of implementing the recommendation. Absent a cohesive architecture based on the paradigm presented for network centricity at ECB, it is not possible to estimate the cost of implementing the recommendation.

One essential area for investigation will be the spectrum impacts. Clearly employing a family of new emitters across the breadth of the battlefield will require a judicious and efficient use of the frequency spectrum. This impact is another justification for designing in this capability up front and not relying on the current FCS approach of integrating developing systems into an overall system of systems. The proposed ubiquitous system of sensors and communications capabilities at ECB will require significant research up-front to determine the right portion of the spectrum for the variety of devices encompassing the system. Affects on radar systems and other communications systems will have to be factored into the development of the system. Indeed the overall network centric philosophy will affect other emitters, as they will need to be leveraged into the system as sources of information and carriers of communications. The impacts on DOTMLPF and on the frequency spectrum are but two of the major areas that must be resolved on the path to network centricity. Relying on arriving at a network centric end state serendipitously is both dangerous and foolhardy.

CONCLUSION

The obvious result of implementing the approaches just described would be a massive restructure of the Signal Corps. However, the recommendations comply with the core aspects of all three guiding principles of the current RMA – network centricity, Jointness, and transformation. Additionally, implementing the recommendations would offer an opportunity for the Signal Corps to take the lead in the area of network centricity. This would facilitate transition to a mission of knowledge and information management that would not necessarily require a

separate corps to implement. Of course, some tactical communications providers would be required both in terms of providing GIG extension within a theater of operations and in terms of providing range extension on the battlefield. However, in keeping with the Joint nature of the future force and with network centric precepts, communicators need not be single purpose Army communications providers.

Just as the old adage has it that information is power, the new paradigm will be that the communities holding the reins of knowledge will posses the power. It is key to an understanding of this future role that the power lies only in the efficient and effective communication of knowledge – not in the ownership of the knowledge. Breaking the "information is power" paradigm will be difficult enough but will be impossible without a community of professionals dedicated to ensuring there is a network centric information infrastructure optimized for communicating knowledge. There will be significant resistance to allowing the Signal Corps to subsume the role of knowledge managers for the future force. While the Signal Corps will have little role in the generation of either information or knowledge, the Signal Corps has expertise to leverage the network to ensure optimization of the intricacies of sustaining and distributing knowledge occurs. The role of the new Signal Regiment will move from communications provider to knowledge facilitator. Ideally, this role will expand from knowledge support to the Army to Joint knowledge manager with the implementation of JV2020. The combination of recommendations enables us to ensure we have the foresight Thucydides espouses by correcting the problem in a manner acceptable for both the near and far terms.

WORD COUNT= 7299

ENDNOTES

[1] Kenneth Kemp and Charles Hudlin, "Civil Supremacy over the Military: its Nature and limits," Armed Forces and Society 19:1 (Fall 1992), 7-26; quoted in Eliot Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime* (New York, NY: Simon and Schuster Free Press, 2002), 26.

[2] Fred P. Stein, "Observations of the Emergence of Network Centric Warfare." available from <http://www.dodccrp.org/steinncw.htm>; Internet; accessed 30 November 2003.

[3] Kevin J. Bergner, *Information, Knowledge and Wisdom: Leader Development Implications for the Army After Next*, Monograph (Carlisle Barracks: U.S. Army War College, 1994); quoted in *Future Leadership, Old Issues, New Methods* ed. Douglas V. Johnson ("n.p.", 2000), 9.

[4] Arthur J. Corbett, "Proliferating Decisionmakers: Root Cause of the Next Revolution in Military Affairs," quoted in *Future Leadership, Old Issues, New Methods* ed. Douglas V. Johnson ("n.p.", 2000), 37.

[5] Melisse Clemmons Rumizen, *The Complete Idiot's Guide to Knowledge Management* (Madison, WI: CWL Publishing Enterprises, 2002), 9.

[6] Maija-Leena Huotari and Mirja Iivonen, *Trust in Knowledge Management and Systems in Organizations* (Hershey, PA: Idea Group Publishing, 2004), 4-5.

[7] David S. Alberts, John J. Garstka, and Fred P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, (Washington D.C.: CCRP Publications Series, 2000), 32.

[8] Arthur K. Cebrowski and John J. Garstka. "Network Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124:1 January 1998 [journal on-line]; 28-35; available from <http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm>; Internet; accessed 8 November 2003.

[9] Christensen, et el., "After the Gold Rush: Patterns of Success and Failure on the Internet," www.innosight.com, p. 22-24, quoted in Arthur L. Money, *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)* (Washington, D.C.: Office of the Assistant Secretary of Defense (C3I) , March 2001), 9.

[10] Arthur L. Money, *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)* (Washington, D.C.: Office of the Assistant Secretary of Defense (C3I) , March 2001), 6.

[11] Office of the Assistant Secretary of Defense (C3I), *Information Superiority: Making the Joint Vision Happen*, (Washington, D.C.: The Pentagon, November, 2000), 2.

[12] David S. Alberts, John J. Gartska, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C.: CCRP Publications , 1999), 64.

[13] Ibid., 49.

[14] Frederick Kagan, “War and Aftermath,” Policy Review Online August 2003 [journal on-line]; available from <http://www.policyreview.org/aug03/kagan.html>; Internet; accessed 8 November 2003.

[15] Ibid.

[16] Nathan Hodge, “Transformation Boss Sees Sensor-Based Warfare Era,” Defense Week Daily Update, 5 February 2002.

[17] Department of Defense, *DoD Chief Information Officer (CIO) GIG CRD (Originally cited from* DoD CIO memorandum dated 22 September 1999, and revised on 12 January 2001 by agreement by the DoD CIO, USD (AT&L) and Joint Staff/J6), (Washington, D.C.: Department of Defense, 2001).

[18] Department of Defense Report to Congress, “Network Centric Warfare,” available from <http://www.defenselink.mil/nii/NCW/>; Internet; accessed 8 November 2003, 9-1.

[19] Mathew French, “DISA Reshuffles The Deck: Reorganization Seeks to Boost DOD's Net-Centric Operations,” *Federal Computer Week* , October 20, 2003, 1.

[20] Ibid.

[21] Joint Chiefs of Staff, Joint Vision 2020 (Washington, D.C.: U.S. Joint Chiefs of Staff, 14 November, 2002), 12.

[22] Ibid., 42.

[23] Matthew French, “2003 Bandwidth In Iraq A Subject Of Debate,” *Federal Computer Week* , October 20, 2003.

[24] A senior Army leader during a lecture given at the Army War College made the comments.

[25] Department of Defense Report to Congress, “Network Centric Warfare,” available from <http://www.defenselink.mil/nii/NCW/>; Internet; accessed 8 November 2003, A1-A2.

[26] Steven R. Covey, *7 Habits of Highly Effective People*, (New York, NY: Simon and Schuster, 1989), 98.

[27] “Interview with Major General James C. Hylton,” *Military Information Technology*, Oct 13, 2003, available from <http://www.mit-kmi.com/archive_article.cfm?DocID=230>; Internet; accessed 8 November 2003.

[28] Joseph L. Yakovac Jr., “Striving for Battlefield Omniscience*,” Military Training Technology*, (Volume 8, Issue 3 2003), 17-19.

BIBLIOGRAPHY

Alberts, David S., John J. Garstka, and Fred P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington D.C., CCRP Publications Series, 2000.

Bergner, Kevin J. *Information, Knowledge and Wisdom: Leader Development Implications for the Army After Next*. Monograph. Carlisle Barracks: U.S. Army War College, 1994. Quoted in Future Leadership, Old Issues, New Methods ed. Douglas V. Johnson. "n.p.", 2000.

Blaker, Jim. "The Owens Legacy: The Former Vice Chairman of the Joint Chiefs Laid the Groundwork for a Revolution." *Armed Forces Journal International* (July 1966): 20.

Cebrowski, Arthur K. and John J. Garstka. "Network Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124:1 January 1998. Journal on-line. Available from <http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm>. Internet. Accessed 8 November 2003.

Christensen, et el., "After the Gold Rush: Patterns of Success and Failure on the Internet," www.innosight.com, p. 22-24, quoted in Arthur L. Money, *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)* Washington, D.C.: Office of the Assistant Secretary of Defense (C3I): 2001.

Corbett, Arthur J. "Proliferating Decisionmakers: Root Cause of the Next Revolution in Military Affairs." Quoted in *Future Leadership, Old Issues, New Methods*, ed. Douglas V. Johnson "n.p.", 2000.

Covey, Steven R. *7 Habits of Highly Effective People*. New York, NY: Simon and Schuster, 1989.

French, Matthew "2003 Bandwidth In Iraq A Subject Of Debate." *Federal Computer Week* , October 20, 2003.

Hodge, Nathan. "Transformation Boss Sees Sensor-Based Warfare Era." Defense Week Daily Update, 5 February 2002.

Huotari, Maija-Leena and Mirja Iivonen, *Trust in Knowledge Management and Systems in Organizations*. Hershey, PA: Idea Group Publishing, 2004.

"Interview with Major General James C. Hylton." *Military Information Technology*, Oct 13, 2003. Available from <http://www.mit-kmi.com/archive_article.cfm?DocID=230>. Internet. Accessed 8 November 2003.

Kagan, Frederick. "War and Aftermath." Policy Review Online August 2003. Journal on-line. Available from <http://www.policyreview.org/aug03/kagan.html>. Internet. Accessed 8 November 2003.

Kemp, Kenneth and Charles Hudlin, "Civil Supremacy over the Military: its Nature and limits," Armed Forces and Society 19:1 (Fall 1992), 7-26. Quoted in Eliot Cohen*, Supreme*

Command: Soldiers, Statesmen, and Leadership in Wartime, 26. New York, NY: Simon and Schuster Free Press, 2002.

Money, Arthur L. *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)* (Washington, D.C.: Office of the Assistant Secretary of Defense (C3I) , March 2001), 6.

Rumizen, Melisse Clemmons. *The Complete Idiot's Guide to Knowledge Management*. Madison, WI: CWL Publishing Enterprises, 2002.

Stein, Fred P. "Observations of the Emergence of Network Centric Warfare." available from <http://www.dodccrp.org/steinncw.htm>; Internet; Accessed 30 November 2003.

U. S. Department of Defense. *DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001 Department of Defense and Intelligence Community GIG Overarching Policy*. Washington, D.C.: Department of Defense, 2000.

U. S. Department of Defense. *DoD Chief Information Officer (CIO) GIG CRD (Originally cited from* DoD CIO memorandum dated 22 September 1999, and revised on 12 January 2001 by agreement by the DoD CIO, USD (AT&L) and Joint Staff/J6). Washington, D.C.: Department of Defense, 2001.

U. S. Joint Chiefs of Staff. *Joint Vision 2020*. Washington, D.C.: U.S. Joint Chiefs of Staff. 2002.

U. S. Office of the Assistant Secretary of Defense (C3I*), Information Superiority: Making the Joint Vision Happen*. Washington, D.C.: The Pentagon, November, 2000.

Yakovac, Joseph L. "Striving for Battlefield Omniscience.*" Military Training Technology*, (Volume 8, Issue 3 2003): 17-19.