REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-06-2007	Master's Thesis	31-07-2006 to 15-06-2007

4. TITLE AND SUBTITLE
Network Centric Warfare and the Principles of War

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Senenko, Christopher M.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton Blvd
Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION REPORT NUMBER
JFSC 25789

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 is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A central pillar of future warfighting concepts for the United States military is the idea of Network Centric Warfare (NCW). This new approach to military operations attempts to leverage Information Age innovations and apply them to the execution of warfare. Some advocates of this concept believe that it will change the character and nature of warfare, therefore, making the conventional concepts of warfare obsolete.

The principles of war are another way of referring to the conventional concepts and character of warfare. The United States military has adopted a standardized series of principles which have stood the test of time and can be traced back to many of the classical theorists of warfare such as the Prussian strategic theorist Carl Von Clausewitz and the ancient Chinese military thinker Sun Tzu. It is these principles that must be analyzed when determining whether or not NCW has radically altered the landscape of warfare. While NCW concepts are force enablers and will assist the military of the future in the execution of its mission, they do not radically alter the classical principles of warfare and for this reason they should not be considered the prime motivator for future resourcing and doctrinal decisions.

15. SUBJECT TERMS
Network Centric Warfare, Principles of War, NCW, netcentric.

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 Unlimited		**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified			757-443-6301

JOINT FORCES STAFF COLLEGE
JOINT ADVANCED WARFIGHTING SCHOOL

NETWORK CENTRIC WARFARE AND THE PRINCIPLES OF WAR

by

Christopher M. Senenko

LCDR, USN

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

Signature: _____

05 April 2007

Thesis Adviser: Dr. Paul Melshen, COL, USMCR (Ret)

ABSTRACT

A central pillar of future warfighting concepts for the United States military is the idea of Network Centric Warfare (NCW). This new approach to military operations attempts to leverage Information Age innovations and apply them to the execution of warfare. Some advocates of this concept believe that it will change the character and nature of warfare, therefore, making the conventional concepts of warfare obsolete.

The principles of war are another way of referring to the conventional concepts and character of warfare. The United States military has adopted a standardized series of principles which have stood the test of time and can be traced back to many of the classical theorists of warfare such as the Prussian strategic theorist Carl Von Clausewitz and the ancient Chinese military thinker Sun Tzu. It is these principles that must be analyzed when determining whether or not NCW has radically altered the landscape of warfare. While NCW concepts are force enablers and will assist the military of the future in the execution of its mission, they do not radically alter the classical principles of warfare and for this reason they should not be considered the prime motivator for future resourcing and doctrinal decisions.

CONTENTS

I. INTRODUCTION

A central pillar of future warfighting concepts for the United States military is the concept of Network Centric Warfare (NCW). This new approach to military operations attempts to leverage Information Age innovations and apply them to the execution of warfare. The United States Department of Defense (DoD) describes NCW as:

> … 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.[1]

The shift towards a network-centric capable force is classified by some of its advocates as a Revolution in Military Affairs (RMA) on par with the establishment of the *levee en masse* by France during the late 18th century.[2] The *Merriam-Webster's Collegiate Dictionary* defines a revolution as "a fundamental change in the way of thinking about or visualizing something: a change of paradigm"[3] With this definition in mind, it can be seen that what is being espoused when referring to NCW as an RMA is nothing short of a fundamental change in the way of thinking about military affairs. The implication of the establishment of a network-centric capable military force, therefore, will be to make the conventional concepts of warfare obsolete. Vice Admiral Arthur K. Cebrowski, a chief proponent of NCW theory, demonstrated this belief when he wrote

---

[1] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2d ed (Revised). (Washington, D.C.: CCRP, 2000), 2.

[2] Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Naval Institute Proceedings*, January 1998 [journal on-line]; available from http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm; Internet; accessed 12 February 2007. *Levee en masse* describes the system of mass conscription used by the French army during the wars of the French Revolution at the end of the 18th century. Prior to this period the armies of Europe were made up of professional soldiers.

[3] Frederick C. Mish, ed., *Merriam-Webster's Collegiate Dictionary Eleventh Edition* (Springfield, Massachusetts: Merriam-Webster, Incorporated, 2005), 1068.

the seminal work on NCW in the United States Naval Institute *Proceedings* in 1998. In this article he wrote:

> For Nearly 200 years, the tools and tactics of how we fight have evolved with military technologies. Now, fundamental changes are affecting the very character of war.[4]

The principles of war are another way of referring to the conventional concepts and character of warfare. The United States military has adopted a standardized series of these principles that "guide war fighting at the strategic, operational, and tactical levels and are the enduring bedrock of United States military doctrine."[5] These principals have stood the test of time and can be traced back to many of the classical theorists of warfare such as the Prussian strategic theorist Carl Von Clausewitz and the ancient Chinese military thinker Sun Tzu. It is these principles that must be analyzed when determining whether or not NCW has radically altered the landscape of warfare.

It is my belief that while NCW concepts are force enablers and will assist the military of the future in the execution of its mission, they do not radically alter the classical principles of warfare and for this reason should not be considered the prime motivator for future resourcing and doctrinal decisions. The Prussian military theorist Carl von Clausewitz recognized the immutability of the classical concepts of warfare in the face of advancing technologies when he wrote in his treatise *On War*:

> The need to fight quickly led man to invent appropriate devices to gain advantages in combat, and these brought about great changes in the forms of fighting. Still, no matter how it is constituted, the concept of fighting remains unchanged.[6]

---

[4] Cebrowski and Garstka.

[5] Department of Defense, *Joint Publication 1. Joint Warfare of the Armed Forces of the United State.* (Washington, D.C.: US Government Printing Office, 14 November 2000), B-1.

[6] Carl Von Clausewitz, *On War,* trans. by Michael Howard and Peter Paret (New York: Everyman's Library, 1993), 145.

There have been three major conflicts fought during what can be called the dawn of the "Net-Centric Age". Each of these conflicts was fought by a military force which had worked to achieve some degree of network-centric capabilities prior to the commencement of hostilities. In 2001, the United States engaged in military operations against Al Qaeda and Taliban forces in Afghanistan during Operation Enduring Freedom in response to the September 11th attacks against the World Trade Center and Pentagon. Subsequently, the United States undertook operations against Iraq in 2003 during Operation Iraqi Freedom to effect regime change and defend against the perceived threat of Weapons of Mass Destruction (WMD). Both of these operations have been touted as examples of the primacy of network-centric concepts. The third conflict fought during this period was conducted by the Israeli army against Hezbollah elements in southern Lebanon in 2006 in response to the shelling of Northern Israel and the kidnapping of two Israeli Defense Force (IDF) soldiers. These conflicts provide numerous examples which can be used in the analysis of the validity of the claims of NCW.

The danger in the assumption that NCW has altered the nature of warfare lies in the resultant actions taken by the Department of Defense and each of the military services towards their future force structure and planning. The fact that this future concept of war has been delineated in the 2004 National Military Strategy, the 2005 United States National Defense Strategy, and the 2006 Quadrennial Defense Review, demonstrates that NCW has become a key component of the strategic vision for the United States military. Additionally, major acquisition programs for all of the services rely heavily on NCW concepts. The Navy's development of the Littoral Combat Ship (LCS), the Army's development of its Future Combat System (FCS), and the Air Force development of the

Global Information Grid (GIG) and its enabling Transformational Satellite all are key components of the future “Networked” force.

II. WHAT IS NETWORK CENTRIC WARFARE?

The first use of the term Network Centric Warfare was by the Chief of Naval Operations (CNO) of the United States Navy, Admiral Jay Johnson, at the United States Naval Institute Annapolis Seminar and 123rd Annual Meeting in 1997. During the conference's principal address, Admiral Johnson referred to this new conceptual construct when he stated that the military was undergoing:

> …a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare.[7]

Platform-centric warfare refers to a form of fighting where the various military elements, whether they be ships, airplanes, tanks or soldiers behave as independent actors in the operational environment. As a result of their independence, these actors are notionally unable to efficiently collaborate, share information, or synchronize their efforts towards achieving the commander's goals. Admiral Johnson's contention was that the military and the technology employed by its forces had reached a point where it would now be possible to shift the focus from a platform-centric type of warfare to a network-centric type of warfare. With this new type of warfare, the various actors would be linked together using the latest in information technology so that they would be able to collaborate and share information. In effect, these forces would act as one towards achieving the commander's goal. Interestingly, Admiral Johnson's assertion implied that the networking of forces was a new concept. This has hardly been the case. From the days of sail with the use of signal flags, to the advent of wireless Morse code, to voice transmission via radio telephones and finally the use of tactical data links the military has

[7] Admiral Jay Johnson. Address at the U.S. Naval Institute Annapolis Seminar and 123d Annual Meeting, Annapolis, MD 23 April 1997.

continually evolved and taken advantage of the latest technological breakthroughs. These technologies have continually advanced the ability to achieve information sharing and shared awareness by all elements of the force. Admiral Johnson's statement may have been motivated by the Navy's development of a Cooperative Engagement Capability (CEC) for its surface combatants. The development of this new system, which commenced in May of 1995, promised to:

> … connect radar systems to enhance detection and engagement of air targets. Ships and planes equipped with their version of CEC hardware and software will share real-time data to create composite radar tracks—allowing the battle group to see the same radar picture.[8]

This new system would provide a significant capability increase over legacy tactical data-link systems such as Link 11 and Link 16 which could only provide near-real time information on targets such as position, altitude, course, and speed.

NCW was further developed by Vice Admiral Arthur K. Cebrowski who served as the Director for Space, Information Warfare, and Command and Control on the U.S. Navy staff. In his 1998 *Proceedings* article, Vice Admiral Cebrowski argued that the changes that were occurring in society and in the business sector as a result of increased information technology would impact the military. He stated:

> Here at the end of a millennium we are driven to a new era in warfare. Society has changed. The underlying economics and technologies have changed. American business has changed. We should be surprised and shocked if America's military did not.[9]

Vice Admiral Cebrowski's arguments for NCW revolved around a comparison of the impact of information technology advances of the 1990's on the business sector and

---

[8] U.S. Government Accountability Office. *Assessments of Selected Major Weapons Programs.* March 2005, [database on-line] available from http://www.gao.gov/new.items/d05301.pdf; Internet; accessed on 08 March 2007, 39.

[9] Cebrowski and Garstka.

the implied changes that these new technologies would have on the military. The structure of this new network centric system consisted of three components: sensor grids; transaction or engagement grids; and a high quality information backplane. These elements would then be supported by command and control processes and automaticity to increase the speed of decision.[10] The sensor grid would be responsible for the gathering of information about the operational environment. This information would then be shared with all elements of the network via the information backplane. The end result of this information sharing would be for the engagement grids to take actions against any adversaries quickly and efficiently.[11]

An additional key element of NCW is the human component.[12] While arguably the most important element of any military force, networked or not, this component has received the least amount of analysis in deference to the focus on the technological aspect of NCW. The study of how human behavior responds and acts in a networked environment and how information is processed are as critical to the success of military operations conducted using this construct as the network itself. The low regard for the human element in future warfighting is demonstrated in a 2001 Department of Defense report to Congress which stated:

---

[10] Ibid.

[11] Ibid.

[12] Department of Defense. Office of Force Transformation, *The Implementation of Network Centric Warfare*, 10 January 2005 [database on-line]; available from http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf; Internet; accessed on 07 September 2006, i.

> In the future, the network will be the single most important contributor to combat power. [13]

The overarching vision of NCW as developed above was then further refined by the Department of Defense C4ISR (Command, Control, Communications, Intelligence, Surveillance, and Reconnasaince) Cooperative Research Program (CCRP) to create a vision for the implementation and the operationalization of NCW. This operationalization of the NCW vision hoped to make significant impact on the way the United States conducts warfare and, "… promises to bring operations to a successful conclusion more rapidly at a lower cost."[14]

In its development of an operational version of a NCW capable force, the CCRP developed the following four tenets of NCW:

- A robustly networked force improves information sharing.
- Information sharing enhances the quality of information and shared situational awareness.
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.
- These, in turn, dramatically increase mission effectiveness.[15]

If realized, the increased information flow described above could have significant impact on the way that forces interact and share information. Information will no longer be pushed to the users but will be pulled by the war fighters from DoD and other United States agencies as necessary in support of their mission.[16] Additionally, it has been

---

[13] Department of Defense, *Network Centric Warfare Report to Congress*, 2001 [database on-line]; available from http://www.dodccrp.org/research/ncw/ncw_report/report/ncw_main.pdf; Internet; accessed on 07 September 2006, 12-3.

[14] Alberts, Garstka, and Stein, 55.

[15] Department of Defense, *Network Centric Warfare Report to Congress*, 4-1.

[16] John P. Stenbit,, "Moving Power to the Edge." *Chips Magazine*, Summer 2003, 6.

argued that the use of this concept as the basis for a new warfighting system would potentially allow for more precise effects and would:

> …enable a shift from attrition-style warfare to a much faster and more effective warfighting style characterized by the new concepts of speed of command and self-synchronization.[17]

Similar to its development of the tenets of NCW, the CCRP developed the following nine governing principles of NCW: information superiority; shared awareness; speed of command; self-synchronization; dispersed forces; de-massification; deep sensor reach; alter initial conditions; and compressed operations.[18]

Information superiority is defined in Joint Pub 3-13 as:

> The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[19]

The value of information superiority is that it, "promises to bring operations to a successful conclusion more rapidly at a lower cost."[20] The concept of ending combat operations quickly with minimal cost reverberates throughout the development of NCW. The importance of minimizing cost and maximizing efficiency for NCW should come as no surprise since the concept has its origins as a business model. The goal of information superiority is to "generate an information advantage through better timeliness, accuracy, and relevance of information. This includes increasing an enemy's information needs, reducing his ability to access information, and raising his uncertainty while assuring our

---

[17] Arthur K. Cebrowski and John J. Garstka.

[18] Department of Defense. Office of Force Transformation, 8.

[19] Department of Defense, *Joint Publication 3-13. Information Operations* (Washington, DC: US Government Printing Office, 13 February 2006), GL-9.

[20] Alberts, Garstka, and Stein, 55.

own information access through a well networked and interoperable force and protection of our information systems, including sensor systems."[21]

The concept of shared awareness calls for "the routine translation of information and knowledge into the requisite level of common understanding and situational awareness across the spectrum of participants in joint and combined operations. This calls for the building of collaborative networks of networks, which are populated and refreshed with quality intelligence and non-intelligence data, both raw and processed, to enable forces to build a shared awareness relevant to their needs. Additionally, information users must also become information suppliers, responsible for posting information without delay and allow access to the data regardless of location. In order to achieve this high-quality shared awareness, secure and assured networks and information that can be defended are required."[22]

The concept of speed of command is "the recognition of an information advantage and converting it into a competitive advantage by creating processes and procedures otherwise impossible. This can be achieved through battlefield innovation and adaptation, which compresses decision timelines and turns information advantage into decision superiority and decisive effects."[23]

Self-synchronization is "the increase of opportunity for low-level forces to operate nearly autonomously and to re-task themselves through exploitation of shared awareness and the commander's intent. Self-synchronization will increase the value of subordinate initiative to produce a meaningful increase in operational tempo and

---

[21] Department of Defense. Office of Force Transformation, 8.

[22] Ibid, 8.

[23] Ibid, 9.

responsiveness and assist in the execution of the "commander's intent." Additionally, self-synchronization will assist in rapid adaptation when important developments occur in the battlespace and eliminate the step function character of traditional military operations."[24]

The use of dispersed forces "will potentially move combat power from the linear battlespace to non-contiguous operations. This concept emphasizes functional control vice physical occupation of the battlespace and generating effective combat power at the proper time and place. In other words a dispersed force will be non-linear in both time and space, but achieve the requisite density of power on demand. This will require an increased close coupling of intelligence, operations, and logistics to achieve precise effects and gain temporal advantage with dispersed forces."[25] NCW will theoretically have the ability to allow for dispersed forces by creating a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent.[26] The belief that dispersed forces will be as effective as non-NCW capable massed forces is due to the fact that NCW will potentially free forces from limitations imposed by the need to communicate, move, and project effects.[27] The enablers of this dispersion will be increased weapons and sensor ranges along with the ability to rapidly move information. This dispersion will thus diminish the required battle space footprint, which will thus diminish the risk to forces.

---

[24] Ibid.

[25] Ibid.

[26] Cebrowski and Garstka.

[27] Alberts, Garstka, and Stein, 90.

Another benefit would be the reduction of the need to move physical objects from place to place, and allow the sensor/shooter to engage many targets without maneuvering. [28]

Demassification is "the movement from an approach based on geographically contiguous massing of forces to one based upon achieving effects. Demassification will require the use of information to achieve desired effects, limiting the need to mass physical forces within a specific geographical location. Additionally, this will allow for increased tempo and speed of movement throughout the battlespace to complicate an opponent's targeting problem."[29]

Deep sensor reach calls for "the expansion in use of deployable, distributed, and networked sensors, both distant and proximate, that detect actionable information on items of interest at operationally relevant ranges to achieve decisive effects. This concept calls for the leveraging the increasingly persistent intelligence, surveillance, and reconnaissance (ISR) and will use sensors as a maneuver element to gain and maintain information superiority. Additionally, this concept calls for the exploitation of sensors as a deterrent when employed visibly as part of an overt display of intent and will enable every weapon platform to be a sensor, from the individual soldier to a satellite."[30]

Altering the initial conditions is "the exploitation of the principles of high-quality shared awareness, dynamic self synchronization, dispersed and de-massed forces, deep sensor reach, compressed operations and levels of war, and rapid speed of command to enable the joint force to swiftly identify, adapt to, and change an opponent's operating context to our advantage. Warfare is highly path-dependent; hence, the imperative to

---

[28] Ibid.

[29] Department of Defense. Office of Force Transformation, 9.

[30] Ibid, 10.

control the initial conditions. The close coupling in time of critical events has been shown historically to have profound impact both psychologically and in locking out potential responses."[31]

The concept of compressed operations calls for "the elimination of procedural boundaries between Services and within processes so that joint operations are conducted at the lowest organizational levels possible to achieve rapid and decisive effects. This will require the increased convergence in speed of deployment, speed of employment, and speed of sustainment. Additionally, this concept will require the elimination of the compartmentalization of processes (e.g., organize, deploy, employ, and sustain) and functional areas (e.g., operations, intelligence, and logistics) and the elimination of structural boundaries to merge capabilities at the lowest possible organizational levels, e.g., joint operations at the company/sub-squadron/task unit level."[32]

Since these principles of NCW are the basic concepts for the functioning of a NCW capable force, it is these items that need to be analyzed when addressing the validity of the classical principles of war.

[31] Ibid.

[32] Ibid.

III. PRINCIPLES OF WAR AND NETWORK CENTRIC WARFARE

The United States military has adopted the following traditional nine principles of war: objective; offensive; mass; economy of force; maneuver; unity of command; security; surprise; and simplicity.[33] These principles have been tested throughout the history of armed conflict and have their roots in the classical thinkers of military strategy.

In the Fiscal Year 2001 Defense Authorization Act (Public Law 106-398), the United States Congress mandated that the Secretary of Defense submit to the congressional defense committees a report on the development and implementation of network centric warfare concepts within the Department of Defense.[34] In this report, the Department of Defense recognized the nine principles of war and made the case that the ongoing, information-driven RMA promised to improve the ability to realize each of these enduring principles in practice.[35]

This chapter defines the traditional principles of war and describes how the Department of Defense sees the concept of NCW bringing about the realization of these principles. Additionally, this chapter looks at historical examples from recent conflicts to demonstrate the validity of this argument.

---

[33] Department of Defense, *Joint Publication 1. Joint Warfare of the Armed Forces of the United State*. (Washington, D.C.: US Government Printing Office, 14 November 2000), viii. Other nations define these Principles of War in a slightly different manner. The British have adopted the following principles of war: Selection and Maintenance of Aim; Offensive Action; Concentration of Force; Economy of Force; Flexibility; Cooperation; Security; Surprise; Maintenance of Morale. The People's Republic of China has adopted the following principles of war: Selection and Maintenance of Aim; Offensive Action; Concentration of Force; Initiative and Flexibility; Coordination; Security; Surprise; Morale; Mobility; Political Mobilization; Freedom of Action.

[34] Administrative Procedure Act. Statutes at Large 106, sec 555 (2001).

[35] Department of Defense, *Network Centric Warfare Report to Congress*, 3-17.

Objective

The principle of objective is the most fundamental of all of the Principles of War. Understanding the objective to be attained with the use of military force frames all other aspects of preparation and execution. This concept is critical to not only the tactical, but also to the operational and strategic levels of war. Clausewitz recognized this important aspect of warfare when he wrote:

> War plans cover every aspect of a war, and weave them all into a single operation that must have a single, ultimate objective in which all particular aims are reconciled. No one starts a war or rather, no one ought to do so without first being clear in his mind what he intends to achieve by that war and how he intends to conduct it.[36]

According to *Joint Publication 1, Joint Warfare of the Armed Forces,* objective is defined in the following manner:

> The purpose of the objective is to direct every military operation toward a clearly defined, decisive, and attainable objective. The objective of combat operations is the defeat of the enemy's armed forces' capabilities or the enemy's will to fight. The objective of an operation other than war might be more difficult to define; nonetheless, it too must be clear from the beginning. Objectives must directly, quickly, and economically contribute to the purpose of the operation. Each operation must contribute to strategic objectives. Avoid actions that do not contribute directly to achieving the objective.[37]

This definition agrees with Clausewitz in its understanding of the need for early recognition of the purpose for conducting military operations. Additionally, this modern definition of objective ties military operations to achieving strategic objectives and does not limit itself to tactical operations.

The DoD describes the impact that NCW will have in realizing the principle of objective by the following:

---

[36] Clausewitz, 700.

[37] Department of Defense, *Joint Publication 1,* B-1.

> The principle of the objective refers to focusing the entire effort in ways that ensure the assigned military mission (the objective) is achieved. Information Superiority, which includes creating and maintaining a continuous, high quality information flow throughout the force and creating shared situational awareness in the form of a Common Operating Picture (COP) for all commands, helps to ensure a clear and common understanding of the objective to be supported, the threats to mission accomplishment, and the commander's chosen course of action for achieving the objective. Given the rapid pace of change in this battle space and the decision cycle speed needed to dominate it, the ability to share information, maintain a current COP, and enable commanders to work in a collaborative environment whenever necessary are central to this principle. As our competitors get access to even more powerful Commercial Off-the-Shelf (COTS) capabilities, only our ability to leverage these capabilities to achieve dominant speed in decision making (speed of command) will enable us to maintain the advantage.[38]

This definition focuses the principle of objective on the achievement of assigned military missions, without any mention of the greater strategic aims. While this difference may appear innocuous, it belies a short sighted view of war where the military mission is the ultimate goal as opposed to the strategic and political objectives. The importance of the political objective was recognized by Clausewitz when he stated:

> The political object – the original motive for the war – will thus determine both the military objective to be reached and the amount of effort it requires.[39]

and

> The political object is the goal, war is the means of reaching it, and means can never be considered in isolation from their purpose.[40]

Alfred Kaufman, a study director at the Institute for Defense Analyses, summarizes this shortsighted focus of NCW when he stated:

---

[38] Department of Defense, *Network Centric Warfare Report to Congress*, 3-17.

[39] Clausewitz, 90.

[40] Ibid, 99.

> NCW misses the point that war is still the end of political objectives, and that war is not an end to itself.[41]

The lack of focus on the long term political and strategic objectives was demonstrated in the execution and aftermath of Operation Iraqi Freedom (OIF) in 2003. During this conflict the United States military was given the task of implementing regime change in Iraq with the primary military objective of the invasion being the capture of Baghdad and the toppling of the regime of President Saddam Hussein. The Secretary of Defense, Donald Rumsfeld, was focused on achieving military victory with the minimal use of force and as quickly as possible. This desire for a quick and efficient victory fits well with the earlier stated objectives of a NCW capable force. The original planning effort called for an estimated 500,000 troops, while Rumsfeld wanted a total force around 125,000.[42] While the American military was able to achieve the capture of Baghdad in only three weeks, instability followed due to a lack of forces to secure the country. The military objective was achieved, but the inability to provide security due to insufficient combat forces on the ground allowed for the development of an insurgency which as of April 2007 was continuing.

The 2006 version of Joint Publication 3-0 describes the six phases of a joint campaign or operations as the following: shaping; deterring; seizing the initiative; dominating; stabilizing and reconstructing; and enabling civil authority.[43] Using this model, the overall political objective of regime change could not be accomplished until Iraq was stabilized and civil authority in place. In the development of the plan for

---

[41] Alfred Kaufman, "Caught in the Network," Armed Forces Journal (February 2005): 22.

[42] Michael R. Gordon and General Bernard E. Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Pantheon Books, 2006), 4.

[43] Department of Defense, *Joint Publication 3-0. Joint Operations*, Washington, DC: US Government Printing Office, 17 September 2006, IV-27.

Operation Iraqi Freedom, Secretary Rumsfeld focused on the dominate phase of operations. This lack of recognition of the true purpose of the war and the inability to see the way in which it should be fought were both shaped by the vision of NCW.

Frederick Kagan, a military historian and resident scholar of the American Enterprise Institute for Public Policy Research, recognized the short comings of the planning and execution of the Bush administration in the lead up to OIF :

> This vision focuses on destroying the enemy's armed forces and his ability to command them and control them. It does not focus on the problem of achieving political objectives. The advocates of a "new American way of war," Secretary of Defense Donald Rumsfeld and Bush chief among them, have attempted to simplify war into a targeting drill. They see the enemy as a target set and believe that when all or most of the targets have been hit, he will inevitably surrender and American goals will be achieved.[44]

The DoD itself demonstrated the view of the potential success of NCW in regards to the targeting of the enemy. In its 2001 report to Congress, the DoD stated the following:

> The NCW construct provides a valuable perspective for achieving success in a target-oriented warfare situation, where timely, relevant, accurate, and precise information is required to automatically engage targets expeditiously with the most effective weapons and forces available. [45]

In its report to Congress, the DoD identifies information superiority, which is one of the principles of NCW, as an enabler for achieving military objectives during conflict. The rationale behind this belief rests on the achievement of a clear understanding of the military objective and an understanding of the commander's intent. These elements are achieved with the creation of a common operating picture across the force that is enabled by the achievement of information superiority thus allowing all forces to gain shared awareness.

---

[44] Frederick. Kagan, "War and Aftermath," *Policy Review* 120 (August – September 2003): 4.

[45] Department of Defense, *Network Centric Warfare Report to Congress*, 4-2.

The classical military theorists have much to say concerning information and intelligence. Even with the advances in technology enjoyed by today's military forces these tenets remain true today. The belief in the need for accurate information concerning your own forces in addition to your enemies is a vital component in the achievement of information superiority. Sun Tzu recognized the importance of this knowledge when he stated:

> Know the enemy, know yourself; your victory will never be endangered. Know the ground, know the weather; your victory will then be total.[46]

Clausewitz recognized the need for information on the battlefield, but took a skeptical view on the ability to actually get accurate information. His lack of confidence in information was demonstrated in the following tenets:

> There is still another factor that can bring military action to a standstill: imperfect knowledge of the situation.[47]

> In short, most intelligence is false, and the effect of fear is to multiply lies and inaccuracies.[48]

Additionally, Clausewitz understood that the human element played an important role in understanding the information that was obtained. Even if the information gathered was accurate, there would still be difficulty in the comprehension of what that information means. He stated:

> The difficulty of accurate recognition constitutes one of the most serious sources of friction in war, by making things appear entirely different from what one had expected.[49]

---

[46] Sun Tzu, *The Art of War,* trans. Samuel B. Griffith. (London: Oxford University Press, 1963), 129.

[47] Clausewitz, 95.

[48] Ibid, 136.

[49] Ibid, 137.

This concept is important to recognize with regards to the concept of NCW. A networked force that has achieved information superiority and has created a common operating picture still might not be able to achieve shared awareness across all components of the force. The possession of the same information by disparate forces and commanders can be interpreted and recognized differently by each element, thereby becoming a source of friction.

During both OEF and OIF the United States military was able to achieve a level of shared awareness and information superiority never achieved before in combat. General Tommy Franks, Commander of the United States Central Command, for both conflicts stated the following during testimony to the United States Congress in 2003:

> Advanced technologies employed during OEF were also critical. The command and control of air, ground, naval, and SOF from 7,000 miles away was a unique experience in warfare as our forces achieved unprecedented real time situational awareness and C2 connectivity.[50]

While the ability to achieve this shared awareness was unprecedented, it did not eliminate the concerns that Clausewitz identified above. An example of the United States military's inability to gather sufficient accurate information during OIF was the capture of Objective Peach. Objective Peach was an important road bridge over the Euphrates which was decisive because it was large enough for armored vehicles to cross. Intelligence reported that this bridge was undefended, when in actuality it was heavily defended by forces concealed in simple camouflage.[51] This example demonstrates the

---

[50] Congress, Senate, Armed Services Committee, *Statement Of General Tommy R. Franks Former Commander US Central Command.* 108th Cong., 9 July 2003, 7.

[51] Greg Grant. "Network Centric Blind Spot: Intelligence Failed To Detect Massive Iraqi Counterattack," *Defense News,* 12 September 2005, 1.

ability of a determined adversary to use the simplest means to inject uncertainty and doubt into the vaunted COP.

Another example of gaps in the ability for a force to gain information superiority and achieve shared awareness was demonstrated by Israel in 2006 during its incursion into southern Lebanon. Prior to this operation the Israelis had been developing a network-centric capability that was designed to support military operations across the spectrum of conflict to include low intensity conflict against an adversary using asymmetric means. This network-centric command and control system was supposed to "increase the operational speed and agility of its ground forces. The system was designed to reduce sensor-to-shooter cycles by streaming real-time data to commanders, and provide links between all echelons of the chain of command from infantry squads up to the division level in a single network."[52] The Israelis ultimately were unsuccessful in achieving a clear cut victory due to its inability to gather the requisite information so that accurate and speedy decision making could occur. Israeli intelligence was unable to detect the presence of a C802 coastal missile defense site which was used to strike the INS Hanit, an Israeli corvette, or the thousands of rockets that were in the possession of Hezbollah.

These gaps in intelligence, both Israeli and U.S., demonstrate the ability of a determined adversary to circumvent the benefits that a NCW capability provides, by employing simple deception techniques to withhold vital information. Retired Army General Robert Scales recognized the inability of technology to gather all of the

---

[52] Kenyon, Henry S. "Israel Targets Network Centricity," *Signal Magazine*, May 2005 [journal on-line]; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=915&zoneid=148; Internet; accessed 13 February 2007.

information required to achieve the level of information superiority called for in the NCW concept. He demonstrated his disdain for NCW when he stated:

> The net-centric idea of lifting the fog of war by creating this giant strategic technological eye in the sky has been an abject failure, hundreds of billions of dollars wasted.[53]

Offensive

According to *Joint Publication 1, Joint Warfare of the Armed Forces,* offensive is defined by the following:

> The purpose of an offensive action is to seize, retain, and exploit the initiative. Offensive action is the most effective and decisive way to attain a clearly defined objective. Offensive operations are the means by which a military force seizes and holds the initiative while maintaining freedom of action and achieving decisive results. The importance of offensive action is fundamentally true across all levels of war. Commanders adopt the defensive only as a temporary expedient and must seek every opportunity to seize or regain the initiative. An offensive spirit must therefore be inherent in the conduct of all defensive operations.[54]

The DoD describes the impact that NCW will have in realizing the principle of offensive by the following:

> Seizing and maintaining the offensive, which enables the force to dictate the terms of combat, is directly dependent on the ability to work inside (or faster than) an opponent's decision cycle (the response time, sometimes referred to as the Observe, Orient, Decide, Act cycle (OODA) loop.) This is supported by Information Superiority both through effective offensive information operations (which disrupt and slow an adversary's decision making and force decisions under greater uncertainty) and by improving the integration and interoperability of C4ISR systems and processes across the board, from better monitoring of the battle space to faster fusion, improved decision quality and speed, to faster planning and implementation times.[55]

---

[53] Grant, 3.

[54] Department of Defense, *Joint Publication* . B-1.

[55] Department of Defense, *Network Centric Warfare Report to Congress*, 3-17.

The above DoD description describes NCW as affecting the ability of the military force to achieve and maintain the offensive as directly dependant on the ability to make sound decisions at a faster pace then the enemy (Speed of Command). The concept of the Observe, Orient, Decide, Act (OODA) cycle used in the DoD description of Offensive was developed by United States Air Force Colonel John Boyd in 1977.[56] The OODA cycle attempts to describe the steps that are required for decisions to be made and actions to be taken in any circumstance. The observe phase describes the process of gathering information. The orient phase describes the process of becoming acquainted with and understanding the information gathered during the observation phase. The decision phase is the act of settling on a course of action that is determined after understanding the information at hand. Finally, the action phase is simply executing the course of action decided upon.[57]

The elements of this loop that NCW directly affects are the observe and orient phases. As the above DoD definition states, information superiority, if achieved, will enhance our ability to quickly gather information and achieve understanding of what is being observed, which will in turn allow for rapid decision making and quicker action. Additionally, information superiority will impede an adversary's ability to do the same thereby allowing for the realization of Boyd's goal of getting through the OODA loop faster then the enemy.

The ability for the United States military to achieve faster decision-making during OIF was seen as a validation of this offensive characteristic of NCW by some observers.

---

[56] John Boyd, "Pattern of Conflict," December 1986 [database on-line]; available from http://www.d-n-i.net/boyd/pdf/poc.pdf; Internet; accessed 13 February 2007.

[57] Ibid.

In an issue paper from the Center for Strategic Leadership at the United States War College the ability to achieve faster decision making was recognized as a positive attribute which directly assisted in achieving mission success during OIF:

> Increased situational awareness had a significant positive impact on risk taking. Increased risk tolerance was reflected in boldness and audacity. One senior commander indicated he could assume a risk, discover he had made a mistake and correct it before the enemy realized he had taken the initial action."[58]

Additionally, this issue paper recognized that while there was still uncertainty in the decision making process, the information systems allowed commanders to make better decisions quicker, with more confidence because of the information that they had available to them.[59]

While OIF provides a good example of a conflict in which Information Superiority was achieved and allowed for rapid decision making, it does not provide a good demonstration of how a capable adversary will attempt to achieve faster decision making or impede the decision making process by United States forces. Once again the belief in the achievability of information superiority becomes a critical weakness in the ability to realize a Principle of War. Since the enemy is not a static actor in the operational environment they will attempt to undermine the ability to achieve this information superiority by deception or other means, thereby getting inside the OODA loop of the NCW capable force. One of Sun Tzu's tenets of warfare was that, "All

---

[58] Dennis Murphy, "Network Enabled Operations in Operation Iraqi Freedom: Initial Impressions," Center for Strategic Leadership, U.S. Army War College Issue Paper, March 2005 [database on-line]; available from http://carlisle-www.army.mil/usacsl/Publications/06-05.pdf; Internet; accessed 13 February 2007, 3.

[59] Ibid, 2-3.

warfare is based on deception."[60] If this is true and effectively employed by an adversary, the orientation process of the OODA loop will become a stumbling block to achieving action. At a minimum, the correct decision might be delayed while the information is interpreted; at worst an incorrect decision could be made.

Mass

According to *Joint Publication 1, Joint Warfare of the Armed Forces,* mass is defined in the following manner:

> The purpose of mass is to concentrate the effects of combat power at the place and time to achieve decisive results. To achieve mass is to synchronize and integrate appropriate joint force capabilities where they will have decisive effect in a short period of time. Mass must often be sustained to have the desired effect. Massing the effects of combat power, rather than concentrating forces, can enable even numerically inferior forces to achieve decisive results and minimize human losses and waste of resources.[61]

The DoD describes the impact that NCW will have in realizing the principle of mass by the following:

> The principle of mass refers to concentrating military capabilities at the decisive time and place. This remains true even in non-linear battles, as when the Viet Minh brought major artillery and manpower to bear at Dien Bien Phu against the French. While this principle has referred to massing forces in the past, the RMA allows the United States to focus on massing effects through the use of enriched sensor capabilities and stand-off precision weapons. The ongoing shift from platform-centric to network-centric platforms and forces, enabled by Information Superiority, greatly improves our capacity to take advantage of all the information available, reduce the risk to U.S. forces, and still inflict maximum damage on an adversary.[62]

---

[60] Sun Tzu, 66.

[61] Department of Defense, *Joint Publication 1,* B-1.

[62] Department of Defense, *Network Centric Warfare Report to Congress,* 3-17.

Clausewitz recognized the need for the massing of forces in order to achieve military success. In *On War* he stated, "…..a main factor is the possession of strength at the really vital point."[63] The above DoD description shows that NCW addresses the concept of mass as a shift from the massing of forces to a focus on the massing of effects which is consistent with the concept of mass from Joint Pub 3-0. This shift in focus to effects and the networking of forces has led to the NCW principles of de-massification and dispersed forces. Both of these concepts advocate that possession of a given geographic area by a massed force is no longer required and can be replaced by dispersed networked forces which can leverage information superiority to achieve the requisite density of combat power based on effects when needed. An Office of Force Transformation (OFT) case study of the U.S Army V Corps operations during OIF recognized the success of dispersed forces:

> The extended connectivity allowed the force to fight more widely dispersed and over further distances than at any time in the past.[64]

While the use of dispersed forces was able to achieve success during the dominate phase of operations during OIF, it was unable to achieve security and stability during subsequent phases of operations as discussed previously. What the tenets of de-massification and dispersion fail to recognize is the important effect that a massed force has by itself.

The V Corps case study demonstrated the importance of manpower for stabilization operations. This case study stated:

---

[63] Clausewitz, 231.

[64] Dave Cammons et al, *Network Centric Warfare Case Study. U.S. V Corps and 3rd Infantry Division (mechanized) During Operation Iraqi Freedom Combat Operations (Mar-Apr 2003) Volume I: Operations*. U.S. Department of Defense, Office of Force Transformation.[database on-line];.Available from http://www.oft.osd.mil/initiatives/ncw/docs/Volume%20I%20-%20Operations.pdf; Internet; accessed on 13 February 2007, 66..

> … unless the nature of land warfare changes significantly, land forces will always become responsible for the land and its inhabitants once enemy forces are dominated in the area and the terrain is "rolled up." This requires sufficient ground forces for securing the lines of communications, tending to civil affairs and medical needs, securing and protecting enemy prisoners of war, and a multitude of other tasks. The enhanced information environment of a robustly networked force will increase the efficiency and synchronization of these tasks, but it will not eliminate them.[65]

This lesson directly contradicts the NCW Principle of Dispersed Force as described by the Office of Force Transformation. As previously stated by the OFT, a dispersed force "emphasizes functional control vice physical occupation of the battlespace and generating effective combat power at the proper time and place."[66]

Economy of Force

According to *Joint Publication 1, Joint Warfare of the Armed Forces*, economy of force is defined in the following manner:

> The purpose of economy of force is to allocate minimum essential combat power to secondary efforts. Economy of force is the judicious employment and distribution of forces. It is the measured allocation of available combat power to such tasks as limited attacks, defense, delays, deception, or even retrograde operations in order to achieve mass elsewhere at the decisive point and time.[67]

The DoD describes the impact that NCW will have in realizing the principle of economy of force by the following:

> Economy of Force refers to the need to use as little capacity as possible on aspects of the battle that are not central to the objective. Commanders think of accepting risk in some parts of the battle space in order to dominate in other parts considered more crucial. Given Information Superiority with the implied improvement in knowing adversary locations, status, and capabilities, as well as greater flexibility in using assets for

---

[65] Cammons et al, 3.

[66] Office of Force Transformation, 8.

[67] Department of Defense, *Joint Publication 1*, B-1.

> multiple purposes, this principle would be enhanced. With improved logistics; e.g., less material forward and greater use of timely delivery, economy of force in transport and maintenance would also benefit from Information Superiority.[68]

The DoD describes NCW as having an enhancing impact on economy of force via information superiority. As seen previously, real combat does not necessarily afford the ability to achieve the level of situational awareness required to fully meet the ideal state envisioned by NCW. The DoD description of the impact of NCW on Economy of Force states that the improvement in knowing the location of adversaries will result from achieving information superiority. The previously mentioned cases of Objective Peach and the Israeli incursion into Lebanon are both excellent examples of the inability of gaining this improvement even with superior technical means and robust networking of the fielded forces.

The network's bandwidth limitations become a quality of a force that must also have economy of force applied. Due to technical limitations:

> Bandwidth must be treated as a high-demand, low-density "class of supply" requiring command attention. Networked systems provide a greatly enhanced capability, but not without a price. Bandwidth is an issue for commanders. It is a commodity that must be acquired and requires prioritization and distribution.[69]

None of the tenets or principles of NCW discuss this important issue or how this real technical limitation might inhibit the achievement of information superiority across the force. The operational commander, when faced with bandwidth limitations might have to make economy of force decisions as to the allocation of bandwidth and by extension an allocation of who gets and who does not get the COP.

---

[68] Department of Defense, *Network Centric Warfare Report to Congress*, 3-17.

[69] Murphy, 2-3.

Maneuver

According to *Joint Publication 1, Joint Warfare of the Armed Forces,* maneuver is defined in the following manner:

> The purpose of maneuver is to place the enemy in a position of disadvantage through the flexible application of combat power. Maneuver is the movement of forces in relation to the enemy to secure or retain positional advantage, usually in order to deliver — or threaten delivery of — the direct and indirect fires of the maneuvering force. Effective maneuver keeps the enemy off balance and thus also protects the friendly force. It contributes materially in exploiting successes, preserving freedom of action, and reducing vulnerability by continually posing new problems for the enemy.[70]

The DoD describes the impact that NCW will have in realizing the principle of maneuver by the following:

> The principle of maneuver deals with placing the enemy at a disadvantage by wisely using the terrain and other aspects of the situation that constrain his courses of action and providing our forces with an advantage through flexibility and adaptation to the situation. Information Superiority provides high quality, current information about adversary force situation, terrain, weather (and their interaction such as mud and fog), and adversary capabilities as well as the knowledge necessary to exploit the mobility, stealth, and flexibility of our own forces.[71]

The DoD description above states that information superiority will help realize the principle of maneuver. If achieved, information superiority will allow military forces to exploit mobility against an adversary based upon superior knowledge of the situation and the location of enemy forces.

The OFT V Corps case study recognized the benefits achieved by the netting of forces and expanding the level of information sharing and awareness when it stated:

---

[70] Department of Defense, *Joint Publication 1,* B-1.

[71] Department of Defense, *Network Centric Warfare Report to Congress,* 3-17.

> … validated that, during OIF, new sensors, extended connectivity, and new information systems enhanced the combat effectiveness of the force. The information sharing increased the situational awareness, which improved the knowledge of the battle space and increased both the speed of maneuver and the responsiveness and precision of fires.[72]

Unity of Command

According to *Joint Publication 1, Joint Warfare of the Armed Forces*, unity of command is defined in the following manner:

> The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective. Unity of command means that all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose. Unity of effort, however, requires coordination and cooperation among all forces toward a commonly recognized objective, although they are not necessarily part of the same command structure. In multinational and interagency operations, unity of command may not be possible, but the requirement for unity of effort becomes paramount. Unity of effort — coordination through cooperation and common interests — is an essential complement to unity of command.[73]

The DoD describes the impact that NCW will have in realizing the principle of unity of command by the following:

> Unity of Command has long been understood as a prerequisite for effective military action. Even in coalition operations for "soft missions," such as peace operations, the lessons learned activities often point to problems arising from forces operating under different National commands and call for "unity of effort." Whatever the practical limits on unity for a particular operation, the ability to create and maintain a shared picture of the commander's intent, and the timely and assured dissemination of plans, orders, reports, and other key information all core elements of Information Superiority are vital.[74]

The DoD description of NCW's impact on achieving Unity of Command relies on the achievement of Information Superiority to ensure that shared awareness is achieved.

---

[72] Cammons et al, 3.

[73] Department of Defense, *Joint Publication 1,* B-1.

[74] Department of Defense, *Network Centric Warfare Report to Congress*, 3-17.

Ideally, NCW will allow for the rapid dissemination of plans, orders, and other key information which will facilitate the achievement of the military objective and the maintenance of rapid decision making for offensive operations. The shared awareness and synchronization of forces to the commander's intent will allow for the achievement of the NCW principle of self-synchronization.

A benefit discovered during OIF was the capability for the commander to maintain situational awareness and battle command regardless of location:

> Increased connectivity and the flow of information provided freedom to command regardless of location. The network allows the commander to move about the battle space and maintain command anywhere in the battle space. The commander is "untethered" and can conduct "battle command on the move.[75]

The Israelis experienced a different result of command and control during their incursion into Lebanon in 2006. They discovered that some commanders became too focused on the displays and information streaming into the command center and lost sight of actual events at the front.

> …after-action probes found egregious cases where commanders relied on situational awareness provided by the sensor-fused data streaming into command centers instead of moving forward to assess critical points in the evolving battle. This war underscored the limitations of plasma, especially when it is accorded disproportionate priority over training and discipline," said Matan Vilnai, a retired major general and former Israeli Defense Forces (IDF) deputy chief of staff, now a prominent member of Israel's Labor Party.[76]

Staff functioning and support for the commander's intent also improved during OIF through the use of netted information systems:

---

[75] Murphy, 2.

[76] Barbara Opall-Rome, *Does Technology Undercut War Leadership? Post-War Probes Target Israeli Command Failures,* Defense News, 20 November 2006 [journal on-line]. available from http://www.defensenews.com/story.php?F=2362496&C=mideast; Internet; accessed 13 February 2007.

> Information systems and the "richness" they provided changed the way upper echelon staffs functioned. Staffs spent less time gathering data. They had more time for analysis and synthesis and shifted to more execution based support for the commander's directed course of action rather than course of action development. This worked in a parallel "benevolent hierarchy" with senior and subordinate staff counterparts to meet the commander's intent.[77]

A negative side effect of achieving shared awareness up and down the chain of command via rapid communications was the ability for senior commanders to become more involved in the direction of subordinate actions as opposed to allowing them to self-synchronize to his intent. Professor Milan Vego of the Naval War College has observed this trend and stated:

> One of the principal tenets of U.S. command and control is centralized direction and decentralized execution. Decentralization of the decision-making process is a prerequisite for giving subordinates sufficient freedom of action. In contrast, a centralized execution leads to lack of initiative on the part of subordinates and forces the higher commander to take over part of their responsibilities in combat. This is not only bad for morale, but distracts the theater commander. The conflicts in Kosovo and Afghanistan reinforced the trend toward further centralization of command and control in U.S. military. Rather than reinforce decentralized command, advances in information technologies have led in the opposite direction.[78]

Security

According to *Joint Publication 1, Joint Warfare of the Armed Forces*, Security is defined in the following manner:

> The purpose of security is to never permit the enemy to acquire unexpected advantage. Security enhances freedom of action by reducing friendly vulnerability to hostile acts, influence, or surprise. Security results from the measures taken by commanders to protect their forces. Staff planning and an understanding of enemy strategy, tactics, and doctrine will enhance security. Risk is inherent in military operations. Application

---

[77] Murphy, 3.

[78] Milan Vego, "What Can We Learn from Enduring Freedom?" *U. S. Naval Institute Proceedings*, July 2002 [journal on-line]; available from http://www.usni.org/proceedings/Articles02/PROvego07.htm; Internet; accessed 13 February 2007.

> of this principle includes prudent risk management, not undue caution. Protecting the force increases friendly combat power and preserves freedom of action.[79]

The DoD describes the impact that NCW will have in realizing the principle of security by the following:

> The principle of security is also fundamental to military success. In today's military this translates into Information Assurance providing an uninterrupted flow of authentic communications and information. If the information processing or communications channels are compromised, or feared to be compromised, military success is imperiled.[80]

The DoD description of the implications of NCW on security recognizes the creation of a new requirement for the defense of forces. Ensuring that the communications networks are not compromised and the information located on the networks is valid has become a critical vulnerability to a networked force. As stated throughout these sections on the Principles of War, NCW relies on the achievement of information superiority to realize the Principles of War and ultimately achieve success on the battlefield. Since a NCW force is dependent on information superiority, a compromise of communication channels will not only imperil military success, but will doom it to failure. The concept of NCW will create a single point of failure that adversaries will no doubt attempt to exploit.

An important enabler of security that must be considered is that provided by the principle of mass. In addition to the benefits that a massed force provides in the stabilization of the operational environment described earlier, a massed force provides a significant advantage in providing force protection to not only ones own forces, but for

---

[79] Department of Defense, *Joint Publication 1,* B-1.

[80] Department of Defense, *Network Centric Warfare Report to Congress,* 3-17.

the cities located in the occupied territory and the securing of the country's borders.[81] This capacity for providing security will assist in the completion of Phase IV (Stabilization and Reconstruction) and Phase V (Enabling Civil Authority) enroute to the achievement of the desired political and military end states of the campaign. This requirement for a massed force to provide security contradicts the NCW principles of de-massification and dispersed force.

Surprise

According to *Joint Publication 1, Joint Warfare of the Armed Forces,* surprise is defined in the following manner:

> The purpose of surprise is to strike the enemy at a time or place or in a manner for which it is unprepared. Surprise can help the commander shift the balance of combat power and thus achieve success well out of proportion to the effort expended. Factors contributing to surprise include speed in decision making, information sharing, and force movement; effective intelligence; deception; application of unexpected combat power; operations security (OPSEC); and variations in tactics and methods of operation.[82]

The DoD describes the impact that NCW will have in realizing the principle of objective by the following:

> Surprise is the ability to strike the enemy at a time, place, or manner for which he is not prepared. It confers massive military advantage. Both intelligence preparation of the battle space and effective operational security (OPSEC) are essential to achieving surprise. Offensive information operations, both to know the enemy's state of readiness and to deceive him about our plans, can add to the likelihood of successful surprise. At the same time, the ability to know the battle space in detail is crucial to finding opportunities for surprise actions. The increased understanding of the situation that is achieved by sharing information and collaboration and the ability to respond more rapidly that comes from new

---

[81] Aldo Borgu, "The Challenges and Limitations of Network Centric Warfare - The Initial Views of an NCW skeptic" (presentation to the "Network Centric Warfare: Improving ADF capabilities through Network Enabled Operations" Conference, 17 September 2003).

[82] Department of Defense, *Joint Publication 1,* B-1.

> command concepts has the potential to make every engagement an ambush turning what was only an exceptional event into a standard operating procedure.[83]

Clausewitz identified two factors that produce surprise, these being secrecy and speed.[84] The need for secrecy is addressed by the concept of NCW in its recognition of the need for effective OPSEC to hide friendly plans and force dispositions from enemy forces. Speed is addressed in the NCW tenet of speed of decision making. Sun Tzu recognized the need for OPSEC in order to achieve a massing of forces against a divided enemy who attempts to defend at various points:

> The enemy must not know where I intend to give battle. For if he does not know where I intent to give battle he must prepare in a great many places. And when he prepares in a great many places, those I have to fight in any one place will be few.[85]

Clausewitz recognized that surprise was difficult to achieve at the strategic level due to the length of time required to prepare for war, which include the assembly of troops and the massing of supplies.[86] The NCW tenets of de-massification and compressed operations will potentially alleviate these concerns and make strategic surprise possible.

Simplicity

According to *Joint Publication 1, Joint Warfare of the Armed Forces*, simplicity is defined in the following manner:

> The purpose of simplicity is to prepare clear, uncomplicated plans and concise orders to ensure thorough understanding. Simplicity contributes to successful operations. Simple plans and clear, concise orders minimize

---

[83] Department of Defense, *Network Centric Warfare Report to Congress*, 3-17.

[84] Clausewitz, 233.

[85] Sun Tzu, 98.

[86] Clausewitz, 234.

> misunderstanding and confusion. When other factors are equal, the simplest plan is preferable. Simplicity in plans allows better understanding and execution planning at all echelons. Simplicity and clarity of expression greatly facilitate mission execution by reducing the stress, fatigue, and other complexities of modern combat and are especially critical to success in combined operations.[87]

The DoD describes the impact that NCW will have in realizing the principle of simplicity by the following:

> The principle of simplicity refers to the need to keep plans, guidance, and orders clear and uncomplicated. It has been established over history that the debilitating effects of human fatigue, excitement, and fear compounded by errors of miscommunication and ambiguity, have proven to be one of the greatest problems in war—the famous "fog and friction" of war. By reducing uncertainty (and thus simplifying the decisions to be made and the situational variations that need to be considered) and by streamlining the processes of situation assessment, planning, and execution, Information Superiority enables commanders to work at a simpler, more coherent level.[88]

The above description of NCW's impact on simplicity correctly recognizes Clausewitz's concept of the need for simplicity and the debilitating impact "fog and friction" have on warfare. What this description fails to recognize is that while a networked system theoretically presents a simpler more coherent picture, it creates new complexities of its own. The networking of a myriad of sensors, satellites, platforms, and human users creates a complex technical environment that is far from simple. Failing to recognize this new complexity and believing it to be simple has potential for clouding a commander's judgment and decision making. Clausewitz recognized the importance of simplicity when he stated in *On War*:

---

[87] Department of Defense, *Joint Publication 1,* B-1,2.

[88] Department of Defense, *Network Centric Warfare Report to Congress*, 3-17.

> Everything in war is simple, but the simplest thing is difficult. The difficulties accumulate and end by producing a kind of friction that is inconceivable unless one has experienced war.[89]

By recognizing the complexity inherent in a NCW capable force, commanders need to develop a trained staff and force in order to maximize the potential and minimize the friction that could be introduced into the decision making process. The Center for Strategic Leadership at the United States War College recognized this need in its analysis of OIF when it stated:

> Training and exercising with the information systems are vital for commanders, staffs, and operators. Similarly, information systems increase the requirement for planning, exercising, and rehearsals for the implementation of effective procedures. Networked systems do not, of and by themselves, solve problems. They simply enable the abilities of commanders, staffs and operators who are trained individually and collectively to exploit the enhanced situational awareness the network provides.[90]

During OIF, the ability to easily interface with the required information from mobile users presented a huge technical challenge. The unwieldy systems and speed of advance made it difficult to for the 3rd Infantry Division to synchronize with the current intelligence picture:

> The problem with command and control was everything was moving and so it was hard to track everything," Lt. Col. Shawn Weed, an intelligence officer with the 3rd Infantry Division now in Iraq, said in a recent interview. "To get an intel picture we had to stop to tap into the big database."[91]

---

[89] Clausewitz, 138.

[90] Murphy, 3.

[91] Grant, 2.

IV. U.S. MILITARY STRATEGIC VISION FOR NETWORK CENTRIC WARFARE

The United States military has embraced the concept of NCW and has made the concept a cornerstone of strategic thought and weapon systems development. At the highest level, this significance is demonstrated in the 2005 version of *The National Defense Strategy of the United States of America* (NDS). The NDS is a document that describes the strategy that the DoD will follow to meet the objectives set forth by the President in his National Security Strategy (NSS). In the NDS, eight Key Operational Capabilities are described which are the focus of defense transformation, one of which is "Conducting Network-Centric operations"[92] The "Conducting of Network-Centric Operations" operational capability has been chosen as a focus of transformation because of the belief that Information Superiority will be not only desired but required in future conflicts in order to achieve success. The NDS addresses this requirement when it states that the future force will rely on our capacity to harness and protect advantages in the realm of information in order to bring decisive capabilities to bear.[93] The use of the term "rely" indicates a vision of a future force that needs information and must protect it in order to execute its mission and will be impotent if unsuccessful. Without this restriction, a future force can be envisioned that is enabled by information and is robust enough to function, albeit non-optimally, with a dearth of information.

The NDS goes on to describe the importance of a network-centric force by stating that:

---

[92] Department of Defense, *The National Defense Strategy of The United States of America*, 01 March 2005 [database on-line]; available from http://www.defenselink.mil/news/Mar2005/d20050318nds1.pdf; Internet; accessed 13 February 2007, 14.

[93] Ibid.

> … a network-centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes by giving the users access to the latest, most relevant, most accurate information.[94]

This description relates back to the belief in the tenet of information superiority which assumes that all information residing on the network will be timely, relevant, and accurate, which will in turn translate to efficiency and effectiveness.

Another strategic document which addresses the DoD's shift of focus towards a network centric force is the 2006 Department of Defense Quadrennial Defense Review Report (QDR). This document sets out to describe the current state of the DoD and the direction that its leadership thinks it needs to go in order to fulfill its responsibilities to the people of the United States.[95] This new QDR continues to shift the focus towards the importance of developing a network capable force. It states that the new force will demonstrate a shift:

> From an emphasis on ships, guns, tanks and planes – to focus on information, knowledge and timely, actionable intelligence.[96]

This statement is interesting in that it explicitly states that information will become more important than the weapons of war in future conflicts.

In order to demonstrate the strides made in achieving the vaunted networked force the QDR identified accomplishments since the publishing of the last QDR in 2001, which included:

> Invested in new equipment, technology and platforms for the forces, including advanced combat capabilities: Stryker Brigades, Littoral Combat

---

[94] Ibid.

[95] Department of Defense, *Quadrennial Defense Review Report*, 06 February 2006 [database on-line]; available from http://www.defenselink.mil/qdr/report/Report20060203.pdf; Internet; accessed 13 February 2007, iii.

[96] Ibid, vii.

> Ships, converted cruise-missile firing submarines, unmanned vehicles and advanced tactical aircraft – all linked by Net-Centric Warfare systems.[97]

The United States Navy is planning on leveraging NCW concepts in the development of its new class of ship, the Littoral Combat Ship (LCS). The LCS is designed to counter anti-access threats in the coastal waters of both friendly and adversary nations. The anti-access threats include mines, diesel submarines, and small high speed surface craft. In order to accomplish these missions, the LCS is being designed with interchangeable mission modules that individually support separate missions, such as Anti-Submarine Warfare (ASW), Surface Warfare (SUW), and Mine Warfare (MIW).[98]

The ASW mission module will use remote vehicles, both Unmanned Undersea Vehicles (UUV) and Unmanned Surface Vehicles (USV) along with organic helicopter assets and underwater sensors to develop undersea battlespace awareness with a theoretical high level of detection and/or denial probability. The MIW mission module will also rely heavily on remote vehicles and the embarked helicopter to execute a MIW mission. For the ASW and MIW mission areas, the LCS will have limited or no capability for prosecution of the threats faced without networking amongst all elements of the mission modules (LCS, remote vehicle, off board sensors, helicopter, and deployed sensors). The LCS will maintain a SUW capability if the final configuration of the SUW

---

[97] Ibid, viii.

[98] Naval Warfare Development Command. *Littoral Combat Ship: Concept of Operations v3.1,* February 2003 [database on-line]; available from http://www.nwdc.navy.mil/CONOPS/Sea_Shield/LCSCONOPS.aspx; Internet; accessed 13 February 2007.

mission module includes short or medium range anti-ship missiles. If not, a 30 mm gun will provide a limited close-in capability to engage small high speed targets.[99]

The United States Army is developing the Future Combat System Brigade Combat Team (FCS (BCT)) as the central weapons system of the future army. The FCS (BCT) is not a specific vehicle, but a family of manned vehicles, Unmanned Air Vehicles (UAV), Line of Sight – Launch Systems (NLOS-LS), Intelligent Munitions Systems (IMS), Unmanned Ground Vehicles, the network and the soldier.[100]

The FCS (BCT) network is designed to consist of the following five layers that provide delivery of data: The standards; transport; services; applications; and sensors; and platforms layers.[101]

The standards layer is defined by the Army as:

> The foundation of the FCS (BCT) network. It provides the governance for which the other layers are shaped and formed. The FCS (BCT) network will conform to the standards documentation to ensure that the net-centric attributes (flexible, adaptable distributed computing environment) are in place to move into the net-centric environment as part of a service-oriented architecture in the GIG. Information needs, information timeliness, information assurance, and netready attributes provide overarching guidance to ensure the technical exchange of information and the end-to-end operational effectiveness.[102]

The transport layer is defined as:

> The FCS (BCT) Family-of-Systems (FoS) are connected to the command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) network by a multilayered transport layer with

---

[99] Ibid.

[100] Program Manager, FCS Brigade Combat Team. *Future Combat System (FCS) Brigade Combat Team (BCT) 18+1+1 System Overview*. 11 April 2006 [database on-line]; available from http://www.army.mil/fcs/whitepaper/FCSWhitepaper(11_Apr_06).pdf; Internet; accessed 13 February 2007.

[101] Ibid.

[102] Ibid.

> unprecedented range, capacity and dependability. The transport layer provides secure, reliable access to information sources over extended distances and complex terrain. The network will support advanced functionalities such as integrated network management, information assurance and information dissemination management to ensure dissemination of critical information among sensors, processors and warfighters both within, and external to the FCS (BCT)-equipped organization.[103]

The services layer is defined as:

> The Services Layer is the open architecture middleware of the FCS (BCT) Network; it provides a window to the Situational Awareness Data Base and enables the interactive functioning of the Applications Layer and the Network Manager. In addition, the Services Layer provides message translation services to achieve JIM interoperability.[104]

The applications layer is defined as:

> The Applications Layer is responsible for providing the integrated ability to assess, plan, and execute network-centric mission operations using a common interface and a set of non-overlapping functional services that provides the full range of FCS (BCT) Warfighter capabilities.[105]

The goal of the networked logistics system is to:

> …provide unprecedented depth and accuracy of logistics information and decision tools to the commanders and logisticians by enabling the distribution system to deliver the right stuff to the right place at the right time reducing O&S costs.[106]

The purpose of embedded training is to:

> The FCS (BCT) network facilitates the Soldier's ability to train anywhere, any time.[107]

The definition of the sensor and platforms layer is to:

---

[103] Ibid.

[104] Ibid.. JIM – Joint Interagency, Multi-national.

[105] Ibid.

[106] Ibid.

[107] Ibid.

> The Sensors and Platforms Layer is comprised of a distributed and networked array of multi-spectral sensors that provide the FCS (BCT) with the ability to "see first." Intelligence, Surveillance and Reconnaissance sensors will be integrated onto all manned ground vehicles, all unmanned ground vehicles and all four classes of unmanned aerial vehicles within the FCS (BCT). These sensors will be capable of accomplishing a variety of collection missions including Wide Area Surveillance (WAS), Reconnaissance, Surveillance and Target Acquisition (RSTA), Mobility and Survivability. In addition to collecting data locally within the FCS (BCT) area of operations, the ISR Layer architecture will facilitate the fusion of Joint, Current Force and national sensor data into the COP through the Distributed Common Ground System – Army (DCGS-A). The sensor data collect from FCS (BCT) internal, Current Force, Joint, and National sensors will provide timely and accurate situational awareness (SA), enhance survivability by avoiding enemy fires, enable precision networked fires, and maintain contact throughout an engagement.

The planned enabler of NCW for the DoD is the Global Information Grid (GIG). DoD defines the GIG as:

> The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority.[108]

A key component of the GIG is the Air Force Transformational Satellite (TSat) system. This new satellite system is designed to provide the necessary bandwidth for the establishment of the GIG on a global scale with all military forces able to connect to the network.

The QDR goes on to state the vision for achieving net-centricity using the recent examples of OIF and OEF as examples of the value of network centric operations:

---

[108] Department of Defense, *Global Information Grid (GIG) Overarching Policy, Directive 8100.1*, September 2002. [database online]; available from http://www.dtic.mil/whs/directives/corres/html/81001.htm; Internet; accessed on 13 February 2007.

> Harnessing the power of information connectivity defines net-centricity. By enabling critical relationships between organizations and people, the Department is able to accelerate the speed of business processes, operational decision-making and subsequent actions. Recent operational experiences in Afghanistan and Iraq have demonstrated the value of net-centric operations. Ground forces were able to reach back to remote UAV pilots in Nevada to direct UAVs in support of their operations, achieving a level of air-ground integration that was difficult to imagine just a decade ago. Such connectivity is helping joint forces gain greater situational awareness to attack the enemy.[109]

The final national strategic document that demonstrates the importance placed on NCW is the National Military Strategy of the United States of America (NMS) published in 2004. The purpose of the NMS is to relay the Chairman of the Joint Chiefs of Staff (CJCS) strategic direction to the Armed Forces of the United States in order to support the National Security and Defense Strategies.[110] This document, as can be expected, is in concurrence with both the NDS and the QDR. The NMS states that one of the desired attributes of the Joint Force is:

> A networked force capable of decision superiority can collect, analyze and rapidly disseminate intelligence and other relevant information from the national to tactical levels, then use that information to decide and act faster than opponents.[111]

In addition to praising the importance of NCW, the NMS goes on to recognize that there are inherent dangers to a networked force:

> Global proliferation of a wide range of technology and weaponry will affect the character of future conflict. Dual-use civilian technologies, especially information technologies, high-resolution imagery and global positioning systems are widely available. These relatively low-cost,

---

[109] Department of Defense, *Quadrennial Defense Review Report*, 58.

[110] Department of Defense, *The National Military Strategy of The United States of America*, 2004 [database on-line]; available from http://www.defenselink.mil/news/Mar2005/d20050318nms.pdf; Internet; accessed 13 February 2007, iv.

[111] Ibid, 16.

> commercially available technologies will improve the disruptive and destructive capabilities of a wide range of state and non-state actors[112]

and

> Software tools for network-attack, intrusion and disruption are globally available over the Internet, providing almost any interested adversary a basic computer network exploitation or attack capability.[113]

Additionally the NMS recognizes the importance of accurate information in order to achieve the effects desired of a network-centric force:

> Decision superiority requires precise information of enemy and friendly dispositions, capabilities and activities, as well as other data relevant to successful campaigns[114]

[112] Ibid, 6.

[113] Ibid.

[114] Ibid, 19.

V. DANGERS OF RELYING ON NETWORK CENTRIC WARFARE FOR FUTURE WEAPONS SYSTEMS AND OPERATIONAL CONCEPTS

As shown throughout this paper the vision of NCW relies on the establishment of an information technology based network that will allow for the sharing of real-time, accurate information across the expanse of the operational environment. This network will then become the key enabler to achieving information superiority, which in turn will help realize the nine classical principles of war based on the principles of NCW. This vision makes sense in the ideal, but leaves much to be desired when the "fog and friction" of actual combat are applied.

The first element that needs to be considered is the type of adversary that will be faced in future conflict along with the capabilities of its forces. As described throughout this paper, many advocates of NCW use the successes of OIF and OEF during the dominate phase of operations as validation of the tenets of NCW. Admiral Cebrowski commented on the success of OIF in 2003 when he stated:

> We are looking at a shift in sources of power. I think, when the lessons learned [from Operation Iraqi Freedom] come out one of the things we are probably going to see is a new air-land dynamic...we will have discovered a new 'sweet spot' in the relationship between land and air warfare, and a tighter integration between those. The things that compel that are good sensors, networked with good intelligence, disseminated through a robust network of systems which then increases speed.[115]

While OIF provides many good examples of the success enjoyed by the United States military, the lessons learned in many cases fail to address the limited "anti-network" capabilities of the Iraqi forces. The Iraqi's were unable to attack the methods and means of information sharing such as Unmanned Aerial Vehicle's (UAV), satellite

---

[115] Hunter Keeter. "Cebrowski: Iraq Shows Network Centric Warfare Implementation." *Defense Daily*. 23 April 2003 database on-line];.available from http://www.oft.osd.mil/library/library_files/article_56_DEFENSE%20DAILY.doc; Internet; accessed on 07 September 2006.

communications, and the radio frequency data links used to connect elements of the force. Not all adversaries will come to the fight with this limited capability. China, which could be a near peer competitor someday, has already demonstrated its ability to actively target information technology networks, and destroy low earth orbiting satellites.[116] Additionally many nations are applying the lessons learned of OEF and OIF in order to find the weaknesses and seams in the United States military force. Yu. E. Gorbachev, a retired Colonel in the USSR army, wrote in a defense journal of the need for developing the capabilities to disrupt the very form of warfare advocated by NCW when he stated:

> … it is necessary, right now, to adopt measures in order to improve the systems and assets of reconnaissance, electronic warfare, communications, command and control, and weapons, and to develop information weapons and directed energy weapons capable of disrupting the operation of automated databases and computer networks and disabling the main enemy command and control and reconnaissance components.[117]

Another component of the understanding of an enemy in regards to NCW is the assumption that the enemy will be compliant and will mass his forces against our distributed/networked force.[118] What is not considered or described in any detail is the effect that a dispersed enemy will have on our own dispersed force and our ability to mass effects. Vego summarized this concern when he stated:

> But the conflict in Afghanistan only proves that netting of diverse platforms technically works in a non-hostile or low-threat environment. It does not tell us whether U.S. systems are robust enough to operate

---

[116] Craig Covault, "Chinese Test Anti-Satellite Weapon." *Aviation Week and Space Technology,* 17 January 2007 [database on-line]; available from http://www.spaceref.com/news/viewnews.html?id=1188; Internet; accessed on 13 February 2007.

[117] Yu. E Gorbachev, "Network Centric War: Myth or Reality?" *Military thought 15* (Jan 2006): 153.

[118] Jeff Cares. "The Network-Centric Craze." Interview by Ted McKenna. *The Journal of Electronic Defense* (May 2006): 39.

> smoothly in the face of a determined physical and electronic attack by a resourceful and skillful enemy.[119]

An additional lesson learned from OIF and OEF is the realization that the enemy will be dynamic and will continually evolve to meet new capabilities. The ability to deceive high technology sensors using simple camouflage or immersing forces amongst civilian populations will make an opponent of the NCW force effective with minimal expenditures. This concept was recognized in the OFT V Corps case study when it stated:

> The enemies of the future will continue to adapt and continually move to more asymmetrical means of fighting U.S. forces. They will develop asymmetrical approaches to reduce the capabilities and efficiencies provided by the enhanced information environment. These asymmetrical approaches may include more urban fighting, network attacks, electronic warfare, guerilla/insurgent warfare, terrorism, and combinations of asymmetrical approaches.[120]

The robustness and vulnerabilities of the network need to be addressed in any discussion of the potential for the future military force. Not understanding the weaknesses and holes in the system and preparing backup plans with redundant capability will make forces that rely on NCW, as is the plan, not only less effective but potentially impotent and vulnerable to destruction in detail. This concern specifically needs to be addressed in the discussion of the utility of dispersed forces. If an adversary is successful in degrading or defeating the network used by dispersed forces for mutual support and shared awareness, that same dispersed force will potentially become cutoff and alone.

At the technical level, it needs to be recognized that the networking of disparate forces requires the use of radio frequency (RF) technologies. These RF bandwidths are

---

[119] Milan Vego.

[120] Cammons et al, 67.

susceptible to intentional and unintentional jamming using cheap and crude methods. During OIF the expansion in the use of data links and communication nets had a dramatic impact on the range of tactical data links due to mutual interference.[121] The increase in the use of the RF spectrum is not limited to just United States forces. Allies, adversaries, and civilians alike are all expanding their usage of this limited resource. This combined with the threat of relatively low tech and cheap jamming technology could have severe impacts in the ability to use systems that will be relied on to conduct operations.

A more extreme type of interference that is raising concerns is the use by an adversary of an exoatmospheric nuclear detonation to cause an Electromagnetic Pulse (EMP). As the proliferation of missile and nuclear technologies spreads the likelihood of this occurrence grows. If an enemy is able to field and use such a system, an EMP will be able to damage unshielded electronic systems. This damage will occur throughout many systems used by the military due to the increasing use of Commercial Off the Shelf Technology (COTS). COTS materials are especially susceptible to EMP damage because they are designed with minimal shielding as had been required of previous generations of military specific technologies. The Israelis have begun to reevaluate their reliance on NCW capabilities in light of Iranian nuclear developments and weapons proliferation to Hezbollah, "Planners are concerned that computer and communications network attack, sophisticated jamming or other electronic attack, as well as Electromagnetic Pulses (EMP) produced by a nuclear blast above the atmosphere, could damage systems that link air and missile defenses, intelligence gathering and command and control."[122]

---

[121] David A. Fulgham, "Cracks in the Net," *Aviation Week and Space Technology*, 30 Jun 2003, 52.

[122] David A. Fulgham, "Holes in the Net," *Aviation Week and Space Technology*, 24 Jul 2006, 30.

Another source of weakness for a NCW capable force is the inherent vulnerability to the information infrastructure itself. Today it is becoming easier and cheaper for anyone with access to the internet to find the tools and execute a network attack virtually anonymously. The cost imbalance between creating a networked force and the ability to defeat it are becoming increasingly large. Additionally, the task of protecting all of the components of a networked force will become increasingly challenging as the network grows and our adversaries become more technologically astute. The Government Accounting Office (GAO) recognized this potential weakness in a report when it stated:

> DOD faces risks inherent with the nature and scope of the effort it is undertaking, for example, risks related to protecting data within the thousands of systems that will be integrated into the network.[123]

An analysis into the effects of a disruption in the network should be made. The range of disruptions that must be considered should be everything ranging from enemy direct action to inadvertent technical glitches. With a loss of the network, dispersed forces can become cut off without support. So with the loss of the network the force will go from one with massed effects to one with isolated and unsupporting elements. While this scenario does not mean that the force will be defeated it does mean that the doctrine of NCW will no longer be valid. Additionally, a platform or unit that relies on off board sensors, such as UAV's or satellites, to accomplish its mission will no longer be able to execute them due to a lack of information. Dale Burton, Vice President of technology for Northrop Grumman recognized the need for this assessment when he stated:

> The playbook effect of a community doing a [network supported] mission isn't always going to be possible, so networks have to be adaptable to the

---

[123] U.S. Government Accountability Office. *The Global Information Grid and Challenges Facing Its Implementation*. July 2004, [database on-line]; available from http://www.gao.gov/new.items/d04858.pdf; Internet; accessed on 04 March 2007, p3.

> situation. You must be prepared if parts of the network won't work. That means advanced planning for any possible losses and the construction of visual displays in operational centers that show what's connected in any given network and what might be in danger of failing.[124]

The impact of human perception and capability has a potentially significant impact on the execution of a NCW war. NCW calls for an integration of all information that is known about the operational environment so that users can access this information as they need. In order to gather all of this information the sensor grid of the networked force must be able to accurately acquire and store this vast amount of information. As Jeff Cares, the CEO of Alidade Inc. stated,

> Information exists in the world around us. We show up and sample the information, and we try to make sense of it to figure out what's going on. If you try to capture all that information into a central database, you have the problem of scale.[125]

NCW assumes that shared awareness will create shared understanding. This is not necessarily the case. The ability for humans to process information is shaped by experience, and education. Different people can see the same information and come to different conclusions about what the information means which directly impacts the decisions made. Kaufman recognized this when he stated:

> Shared information does not automatically, if ever, lead to shared understanding. Moreover, by thus ignoring the human dimension of the human process, NCW tends to overestimate man's capacity to deal with contradictory information.[126]

Robert S. Bolia of the Air Force Research Laboratory addressed whether or not a shared mental model would lead to a shared interpretation of the COP and whether or not a

---

[124] Fulgham., "Holes in the Net," 30.

[125] Cares, 39.

[126] Kaufman, 21.

shared interpretation of the COP would lead to a shared interpretation of what is the correct course of action. He found that:

> Regrettably, military history is replete with situations in which one or both of these conjectures proved false. What is difficult to prove in these cases is whether the failure was due to fallacious reasoning, or to the lack of a shared mental model. Regardless, this may present a major human factors challenge for the implementation of the network-centric CONOPS, which will only be exacerbated by adversary-induced uncertainty and information overload. [127]

Interestingly, the original DoD report to Congress recognized these shortfalls of the human capacity to interpret information in its description of the cognitive domain:

> The cognitive domain is in the minds of the participants. This is the place where perceptions, awareness, understanding, beliefs, and values reside and where, as a result of sense making, decisions are made. This is the domain where many battles and wars are actually won and lost. This is the domain of intangibles: leadership, morale, unit cohesion, level of training and experience, situational awareness, and public opinion. … By training and shared experience we try to make the cognitive activities of military decision makers similar, but they nevertheless remain unique to each individual, with differences being more significant among individuals from different Services, generations, and countries than they are among individuals from the same unit or Service.[128]

NCW states that one of its principals is the self-synchronization of subordinates to a commander's intent. This intent will support the completion of the mission objective which then must support strategic objective. What NCW fails to capture is the need for sound strategy and guidance for this to happen. Aldo Borgu, the Program Director for Operations and Capability at the Australian Strategic Policy Institute (ASPI) recognized this when he stated:

---

[127] Robert S Bolia, Michael A. Vidulich, and W. Todd Nelson. *Unintended Consequences of the Network-Centric Decision Making Model: Considering the Human Operator*. (Air Force Research Laboratory, Human Effectiveness Directorate Warfighter Interface Division, 2006). AFRL-HE-WP-TP-2006-0044.

[128] Department of Defense, *Network Centric Warfare Report to Congress*, 3-10.

> Information superiority is also no substitute or compensator for bad decision making or having a poor strategy to begin with.[129]

The potential for micro-management can increase with increased ability to achieve shared awareness. While this increased level of shared awareness is viewed by some as a success story of NCW as happened during OEF:

> …networking the unmanned aerial vehicle (UAV) systems and the AC-130 gunships with ground forces. This real-time capability moved from the conceptual stage to operational status during efforts to target Taliban and al Qaida fighters on the move. UAVs were used to a greater degree than ever before, Gen. Kellogg continues. The ability to pass information gathered by Predator and Global Hawk back to the combatant commanders enabled near-real- and real-time battlefield situational awareness.[130]

To others, the new level of shared awareness allowed commanders well removed from the scene of action to direct at the operational and tactical level:

> Another consequence of our expanded global connectivity was that "reach-back," a desirable capability when used with discrimination, metamorphosed into "reach-forward" as rear headquarters sought information from U.S. Central Command's forward-deployed Combined Air Operations Center (CAOC) and then used that information to try to influence events from the rear.[131]

Additionally, this capability for shared awareness at all levels of the chain of command allowed leadership at the highest levels to become involved in the targeting process during OIF. Lambeth described this process:

> Greatly expanded global communications connectivity provided unprecedented real-time situational awareness at all levels. That new capability allowed sensor-to-shooter links to be shortened, in some cases,

---

[129] Borgu.

[130] Robert K. Ackerman, "Defense transformation will accelerate the influence of information technology." *Signal Magazine*, April 2002 [journal on-line]; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=408&zoneid=80; Internet; accessed 13 February 2007.

[131] Benjamin S Lambeth, "The Downside of Network-Centric Warfare," *Aviation Week and Space Technology*, 02 January 2006, 86.

> from hours to minutes. It also, however, resulted in an oversubscribed target-approval process that lengthened rather than compressed the kill chain. As a result, the human factor became the main constraint impeding more effective time-critical targeting.[132]

An additional quality of the NCW concept is its promise of a smaller force structure with a reduced requirement for forces to execute a mission. This idea can have dire consequences in not only major combat operations but also in Operations Other than War (OOTW). Borgu identified this concern:

> However the major problem we face in NCW's applicability to OOTW - and practical implementation - is that the ultimate seduction of the NCW concept to politicians and policymakers alike is that it offers the possibility of a smaller force structure and less numbers of troops overall. That has attractions for reasons of both savings costs and potential casualties.[133]

The emphasis on NCW capabilities and the focus on the power of information tend to direct the limited resources of the DoD towards high cost technologically advanced systems. This focus takes away the emphasis on the human element of warfare. As observed in the reconstruction and stabilization phase of operations during OIF in Iraq, the value of a large force to conduct security and stabilization cannot be discounted. This unbalanced resource focus was described aptly in the Joint Force Quarterly:

> … overemphasis on airpower, precision engagement, and information superiority at the expense of an ability to seize and hold ground will pose grave risks for decision makers if allowed to crowd out, rather than complement, other critical capabilities.[134]

---

[132] Ibid.

[133] Borgu.

[134] Richard D. Hooker, Jr., H. R. McMaster, and Dave Grey. "Getting Transformation Right." *Joint Forces Quarterly 38* (Jul 2005): 23.

VI. CONCLUSION

Network Centric Warfare has become a key component for future war fighting concepts in the United States military. The importance that this concept holds is demonstrated by its inclusion in the three most recent strategic documents to come out of the Department of Defense. Additionally, the United States Navy, Army, and Air Force are all developing their next generation weapons systems based upon this concept. The Navy's Littoral Combat Ship, the Army's Future Combat System and the Air Force Global Information Grid all require a networked force to be useful components in the operational environment.

As demonstrated throughout this paper, NCW concepts, if achieved and maintained, can be force enablers on the battlefield. The importance of the human decision maker and the weapons of war employed by them must not be forgotten when the benefits of NCW are discussed.

The principles of war which have been adopted by the United States are well founded in historical examples and have been eloquently described by classical military theorists such as Carl von Clausewitz and Sun Tzu. In general, NCW attempts to realize these principles through the achievement of Information Superiority. This information dominance, if achieved, will allow for the development of shared awareness which will in turn allow for a faster and more effective decision making process. This reliance on the ability to achieve and maintain information superiority throughout a conflict becomes the weak link in the argument for the validity of the concepts of NCW. Information superiority becomes a self imposed single point of failure, which may not be able to be overcome if there is an over reliance on NCW concepts. As demonstrated throughout

this paper, future adversaries of the United States recognize this inherent weakness in the reliance on Information Superiority and are working towards novel, creative, and cheap asymmetric means to defeat our advanced technology.

Additionally, discussions of how OIF and OEF have proven the validity of NCW need to be tempered with the realization that in both cases the adversaries during the major combat phase of operations were unable to match the overwhelming superiority of force applied by the United States. As Vego described:

> Many experts have asserted that the success in Afghanistan proved the value of the "revolution in military affairs." While many new technologies successfully passed the test, it must be remembered that U.S. forces possessed overwhelming power and faced a weak opponent. The enemy never had a chance to challenge air power. The victory in Afghanistan was easy and cheap because Afghanistan had few economic centers and poor infrastructure. The Taliban air defenses were virtually nonexistent and that accounts for the fact that the United States obtained air superiority within hours. The Taliban had few, if any, antiaircraft weapons with the reliability, range, and guidance systems to pose a credible threat against high-flying aircraft equipped with the most advanced sensors. The UAVs were used against almost nonexistent opposition, and Special Forces were allowed to roam freely in the countryside. At sea, the U.S. and coalition forces faced no opposition at all. Nor did the Taliban possess any capability to interfere with or attack U.S. computer networks[135]

While the use of NCW concepts in the development of our force structure and doctrine should not be abandoned, it should be done so with the understanding of the potential weakness that is being introduced into the force. With this in mind, the necessary redundancy and backup systems required to ensure uninterrupted war fighting capability for all forces regardless of the status of the network should be a critical design element for future weapons systems. The Center for Strategic Leadership at the United States Army War College paper on OIF provided a good summation of the value of NCW as seen through the lens of OIF when it stated:

---

[135] Vego.

> …[NCW] certainly enabled operations but did not change the human nature of warfare, and the "fog and friction" of war was not eliminated by networked platforms and increased situational awareness. Therefore NCW is not a panacea or substitute for the principles of war or the art of command…but it certainly enhanced the ability of commanders to conduct combat operations."[136]

[136] Murphy, 2.

BIBLIOGRAPHY

Ackerman, Robert K. "Defense transformation will accelerate the influence of information technology." *Signal Magazine,* April 2002. Journal on-line. Available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=408&zoneid=80. Internet. Accessed 13 February 2007.

Administrative Procedure Act. Statutes at Large 106 (2001).

Admiral Jay Johnson. Address at the U.S. Naval Institute Annapolis Seminar and 123d Annual Meeting, Annapolis, MD 23 April 1997.

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2d ed (Revised). Washington, D.C.: CCRP, 2000.

Bolia, Robert S., Michael A. Vidulich, and W. Todd Nelson. *Unintended Consequences of the Network-Centric Decision Making Model: Considering the Human Operator.* Air Force Research Laboratory, Human Effectiveness Directorate Warfighter Interface Division, 2006. AFRL-HE-WP-TP-2006-0044.

Boyd, John, "Pattern of Conflict," December 1986. Database on-line. Available from http://www.d-n-i.net/boyd/pdf/poc.pdf. Internet. Accessed 13 February 2007.

Cammons, Dave, John B. Tisserand III, Duane E. Williams, Alan Seise, and Doug Lindsay. *Network Centric Warfare Case Study. U.S. V Corps and 3rd Infantry Division (mechanized) During Operation Iraqi Freedom Combat Operations (Mar-Apr 2003) Volume I: Operations.* U.S. Department of Defense, Office of Force Transformation. Database on-line. Available from http://www.oft.osd.mil/initiatives/ncw/docs/Volume%20I%20-%20Operations.pdf. Internet. Accessed on 13 February 2007.

Cares, Jeff. "The Network-Centric Craze." Interview by Ted McKenna. *The Journal of Electronic Defense* (May 2006): 38-40.

Cebrowski, Arthur K, and John J. Garstka. "Network-Centric Warfare: Its Origin and Future," *Naval Institute Proceedings,* January 1998. Journal on-line. Available from http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm. Internet. Accessed 12 February 2007.

Clausewitz, Carl Von. *On War.* Translated by Michael Howard and Peter Paret. New York: Everyman's Library, 1993.

Fulgham, David A. "Cracks in the Net," *Aviation Week and Space Technology,* 30 Jun 2003, 52.

---------- "Holes in the Net," *Aviation Week and Space Technology*, 24 Jul 2006: 30.

Gorbachev, Yu. E. "Network Centric War: Myth or Reality?" *Military thought 15* (Jan 2006): 143-154.

Gordon, Michael R., and General Bernard E. Trainor. *Cobra II: The Inside Story of the Invasion and Occupation of Iraq.* New York: Pantheon Books, 2006.

Grant, Greg. *Network Centric Blind Spot Intelligence Failed To Detect Massive Iraqi Counterattack.* Defense News, May 2005. Database on-line. Available from http://www.oft.osd.mil/library/library_files/article_468_Defense%20News.doc. Internet. Accessed on 13 February 2007.

Hooker, Richard D., Jr., H. R. McMaster, and Dave Grey. "Getting Transformation Right." *Joint Forces Quarterly 38* (Jul 2005): 20-27.

Kagan, Frederick. "War and Aftermath." *Policy Review* 120 (August – September 2003): 3-27.

Kaufman, Alfred. "Caught in the Network." Armed Forces Journal (February 2005): 20-22.

Keeter, Hunter. "Cebrowski: Iraq Shows Network Centric Warfare Implementation." *Defense Daily*. 23 April 2003. Database on-line. Available from http://www.oft.osd.mil/library/library_files/article_56_DEFENSE%20DAILY.doc. Internet. Accessed on 07 September 2006.

Kenyon, Henry S. "Israel Targets Network Centricity." *Signal Magazine*, May 2005. Journal on-line. Available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=915&zoneid=148. Internet. Accessed 13 February 2007.

Lambeth, Benjamin S. "The Downside of Network-Centric Warfare," *Aviation Week and Space Technology*, 02 January 2006, 86.

Mish, Frederick C, ed., *Merriam-Webster's Collegiate Dictionary Eleventh Edition.* Springfield, Massachusetts: Merriam-Webster, Incorporated, 2005.

Murphy, Dennis, "Network Enabled Operations in Operation Iraqi Freedom: Initial Impressions." Center for Strategic Leadership, U.S. Army War College Issue Paper, March 2005. Database on-line. Available from http://carlisle-www.army.mil/usacsl/Publications/06-05.pdf. Internet. Accessed 13 February 2007.

Naval Warfare Development Command. *Littoral Combat Ship: Concept of Operations v3.1,* February 2003. Database on-line. Available from http://www.nwdc.navy.mil/CONOPS/Sea_Shield/LCSCONOPS.aspx. Internet. Accessed 13 February 2007.

Opall-Rome, Barbara. *Does Technology Undercut War Leadership? Post-War Probes Target Israeli Command Failures.* Defense News, 20 November 2006. Journal on-line. Available from http://www.defensenews.com/story.php?F=2362496&C=mideast. Internet. Accessed 13 February 2007.

Program Manager, FCS Brigade Combat Team. *Future Combat System (FCS) Brigade Combat Team (BCT) 18+1+1 System Overview*. 11 April 2006. Database on-line. Available from http://www.army.mil/fcs/whitepaper/FCSWhitepaper(11_Apr_06).pdf. Internet. Accessed 13 February 2007.

Stenbit, John P. "Moving Power to the Edge." *Chips Magazine,* Summer 2003, 6.

Thompson, Loren. "The Hidden Dangers of Networked Warfare." *The Lexington Institute Issue Brief.* 17 June 2003. Database on-line. Available from http://www.lexingtoninstitute.org/defense.asp?aid=76. Internet. Accessed 09 August 2006.

Tzu, Sun. *The Art of War.* Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

U. S. Congress. Senate. Armed Services Committee. *Statement Of General Tommy R. Franks Former Commander Us Central Command.* 108th Cong., 9 July 2003.

U.S. Department of Defense, *Global Information Grid (GIG) Overarching Policy, Directive 8100.1*, September 2002. Database on-line. Available from http://www.dtic.mil/whs/directives/corres/html/81001.htm. Internet. Accessed on 13 February 2007.

U. S. Department of Defense. *Joint Publication 1. Joint Warfare of the Armed Forces of the United States.* Washington, DC: US Government Printing Office, 14 November 2000.

U. S. Department of Defense. *Joint Publication 3-0. Joint Operations.* Washington, DC: US Government Printing Office, 17 September 2006.

U. S. Department of Defense. *Joint Publication 3-13. Information Operations.* Washington, DC: US Government Printing Office, 13 February 2006.

U. S. Department of Defense. *The National Defense Strategy of The United States of America*. 01 March 2005. Database on-line. Available from

http://www.defenselink.mil/news/Mar2005/d20050318nds1.pdf. Internet. Accessed 13 February 2007.

U.S. Department of Defense. *The National Military Strategy of The United States of America*. 2004. Database on-line. Available from http://www.defenselink.mil/news/Mar2005/d20050318nms.pdf. Internet. Accessed 13 February 2007.

U.S. Department of Defense. *Network Centric Warfare Report to Congress*. 2001. Database on-line. Available from http://www.dodccrp.org/research/ncw/ncw_report/report/ncw_main.pdf. Internet. Accessed on 07 September 2006.

U. S. Department of Defense. *Quadrennial Defense Review Report*. 06 February 2006. Database on-line. Available from http://www.defenselink.mil/qdr/report/Report20060203.pdf. Internet. Accessed 13 February 2007.

U.S. Department of Defense. Office of Force Transformation. *The Implementation of Network Centric Warfare.* 10 January 2005. Database on-line. Available from http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf. Internet. Accessed on 07 September 2006.

U.S. Government Accountability Office. *The Global Information Grid and Challenges Facing Its Implementation*. July 2004. Database on-line. Available from http://www.gao.gov/new.items/d04858.pdf. Internet. Accessed on 04 March 2007.

U.S. Government Accountability Office. *Assessments of Selected Major Weapons Programs.* March 2005. Database on-line. Available from http://www.gao.gov/new.items/d05301.pdf. Internet. Accessed on 08 March 2007.

Vego, Milan, "What Can We Learn from Enduring Freedom?" *U. S. Naval Institute Proceedings*, July 2002. Journal on-line. Available from http://www.usni.org/proceedings/Articles02/PROvego07.htm. Internet. Accessed 13 February 2007.

AUTHOR BIOGRAPHY

LCDR Senenko, a native of West Nyack, New York, graduated from the United States Naval Academy in 1994 with a Bachelor of Science in Physics (with Merit). Upon graduation, LCDR Senenko reported for duty at the Surface Warfare Officer School Division Officer Course in Newport, Rhode Island. Upon completion of training, LCDR Senenko reported as CF division officer in USS VICKSBURG (CG 69) stationed in Mayport, FL. LCDR Senenko was designated a Surface Warfare Officer in 1996. While attached to VICKSBURG, LCDR Senenko completed two deployments to the Mediterranean Sea and Persian Gulf. During his time in VICKSBURG, LCDR Senenko also served as Strike Officer, Fire Control Officer, and Ordnance Officer.

LCDR Senenko reported to the Naval Postgraduate School in June 1998 and graduated in December 2000, earning a Masters of Science in Astronautical Engineering (with Distinction).

Upon completion of Department Head training, LCDR Senenko reported as Operations Officer in USS PORTER (DDG 78) stationed in Norfolk, VA. During this tour, PORTER executed a surge deployment in support of OPERATION IRAQI FREEDOM, conducting TLAM Strike missions, Theater Ballistic Missile Defense (TBMD) of Israel and participated in OPERATION ACTIVE ENDEAVOUR while assigned to Standing Naval Forces Mediterranean (SNFM).

LCDR Senenko was awarded the Surface Navy Association Arleigh Burke Award for Operational Excellence for 2003.

LCDR Senenko assumed command of USS TEMPEST (PC 2) in February 2004, and subsequently assumed command of PC Crew Charlie upon its commissioning. PC Crew Charlie executed a surge deployment in support of Operation Iraqi Freedom from June through December 2004, and deployed again in December 2005. During these deployments, PC Crew Charlie conducted Maritime Security Operations in Iraqi territorial waters, defending key oil infrastructure locations.

LCDR Senenko’s awards include the Meritorious Service Medal, the Navy Commendation Medal (Four Awards), the Navy Achievement Medal (Three Awards), various campaign, unit, and service awards.