Strategy Research Project

NETWORK CENTRIC WARFARE IN THE AGE OF CYBERSPACE OPERATIONS

BY

LIEUTENANT COLONEL RICHARD L. FOLKS II
United States Air Force

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
22-03-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

Network Centric Warfare in the Age of Cyberspace Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel Richard L. Folks II

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Colonel James C. Markley
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The emergence of cyberspace as a new warfighting domain and the DOD's establishment of Cyberspace Command make clear the United States' intent to gain superiority in this emerging area vital to overarching national interests. In the early 1990s a "theory of war" focused on information technology and networking rose to the forefront of military thinking with the emergence of Vice Admiral Arthur Cebrowski's Net-Centric Warfare. At the time it was hailed as a potential game changing revolution in military affairs. Specifically Net-Centric Warfare promised to deliver seamless networking of friendly force elements in order to increase combat power. Fast forward to December 2006, with the publication of the National Military Strategy for Cyberspace Operations, foundational DOD doctrine establishing cyberspace as a warfighting domain. With so much effort and national treasure being applied to cyberspace issues, it is crucial that past network centric warfare concept be applied in today's cyberspace environment. This paper examines the relevance of net centric warfare in the age of cyberspace operations and seeks to determine if combining the tenets of net centric warfare with emerging cyberspace operations doctrine could deliver improved operational capabilities.

15. SUBJECT TERMS

Cyberspace, Computer Network Operations, Net-Centric Warfare

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

NETWORK CENTRIC WARFARE IN THE AGE OF CYBERSPACE OPERATIONS

by

Lieutenant Colonel Richard L. Folks II
United States Air Force

Colonel James C. Markley
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

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

ABSTRACT

AUTHOR: Lieutenant Colonel Richard L. Folks II

TITLE: Network Centric Warfare in the Age of Cyberspace Operations

FORMAT: Strategy Research Project

DATE: 22 March 2011 WORD COUNT: 5,779 PAGES: 30

KEY TERMS: Cyberspace, Computer Network Operations, Net-Centric Warfare

CLASSIFICATION: Unclassified

The emergence of cyberspace as a new warfighting domain and the DOD's establishment of Cyberspace Command make clear the United States' intent to gain superiority in this emerging area vital to overarching national interests. In the early 1990s a "theory of war" focused on information technology and networking rose to the forefront of military thinking with the emergence of Vice Admiral Arthur Cebrowski's Net-Centric Warfare. At the time it was hailed as a potential game changing revolution in military affairs. Specifically Net-Centric Warfare promised to deliver seamless networking of friendly force elements in order to increase combat power. Fast forward to December 2006, with the publication of the National Military Strategy for Cyberspace Operations, foundational DOD doctrine establishing cyberspace as a warfighting domain. With so much effort and national treasure being applied to cyberspace issues, it is crucial that past network centric warfare concept be applied in today's cyberspace environment. This paper examines the relevance of net centric warfare in the age of cyberspace operations and seeks to determine if combining the tenets of net centric warfare with emerging cyberspace operations doctrine could deliver improved operational capabilities.

NETWORK CENTRIC WARFARE IN THE AGE OF CYBERSPACE OPERATIONS

> During the Industrial Age, power came from mass. Now power tends to come from information, access, and speed.
>
> —Vice Admiral (Ret.) Arthur K. Cebrowski

Throughout history militaries have used technological developments to improve their abilities to fight and win wars. The emergence of cyberspace as a new warfighting domain and the Department of Defense's (DOD's) establishment of Cyberspace Command make clear the United States (U.S.) military's intent to gain superiority in this emerging arena vital to overarching U.S. national interests. In 1998 a "theory of war" focused on information technology and networking rose to the forefront of military thinking with the emergence of Vice Admiral Arthur Cebrowski's Network Centric Warfare (NCW). At the time it was hailed by some as a potential game changing revolution in military affairs. Specifically NCW promised to deliver seamless networking of friendly force elements in order to increase combat power and situational awareness on the battlefield. Fast forward to December 2006, with the publication of the National Military Strategy for Cyberspace Operations, foundational DOD doctrine establishing cyberspace as a warfighting domain. With so much effort and national treasure being applied to cyberspace issues, it is crucial that past NCW concepts be applied in today's cyberspace environment.

This paper examines the relevance of net centric warfare in the age of cyberspace operations and seeks to determine if combining the tenets of net centric warfare with emerging cyberspace operations doctrine could deliver improved operational capabilities. As a part of the analysis, war theory and principles will be

considered in relation to NCW and cyberspace operations. This is done in order to establish the link between NCW, cyberspace operations, and warfighting principles. Furthermore, it helps to frame this analysis in terms of military application. In order to limit the scope of this analysis, net-centric and cyberspace effects outside the current scope of military operations will not be assessed. This focus is in no way intended to dismiss the tremendous strategic effects NCW and cyberspace operations have outside of the military domain. Indeed, it is entirely plausible that attacks against a nation state's economy, social interactions, communications, power infrastructures, commerce, or belief systems could win a war without so much as the firing of a single shot.

So why does this matter? The DOD is implementing cyberspace operations with a great sense of urgency. This is a necessary reaction to successful attacks and exploitation of the U.S. global information grid and specifically DOD networks. According to Defense Secretary Robert Gates the United States is "under cyberattack virtually all the time, every day" and the DOD plans to more than quadruple the number of cyberspace experts it employs to ward off such attacks.[1] There is growing evidence that the U.S. has to a large extent abandoned its pursuit of NCW. According to Dr. Sean Lawson an Associate Professor in the Department of Communications at the University of Utah,

> The NCW that sought to achieve the very rational and modest goal of adopting the same kinds of technologies and organizational structures that seemed to have revolutionized the rest of society, all for the purpose of promoting a military flexible and adaptable enough to meet the challenges of an uncertain world, have been abandoned in favor of an incoherent, internally inconsistent, and in some ways even more technophilic and overconfident vision of future warfare.[2]

On the other hand Dr. Jeffrey Groh Professor of Information and Technology at the U.S. Army War College says that "the term NCW is going to die a slow death but the concept isn't going away."[3]

Recent examination of the cyberspace environment suggests that "the more cyberspace is critical to a nation's economy and defense, the more attractive to enemies is the prospect of crippling either or both via attacks on or through it."[4] Recognizing the tremendous growth and potential opportunities offered by globally interconnected networks the founding fathers of NCW offered a comprehensive theory for conducting warfare with the assistance of modern networking technology.

NCW Background

The beginnings of NCW can be traced back to the publishing of Joint Vision 2010. This key document published in 1996 by the Chairman of the Joint Chiefs of Staff, General Shalikashvili, envisioned a future centered on the term "dominant battlefield awareness"[5] and brought to light the idea that information superiority would lead to revolutionary battlefield successes. This portion of Joint Vision 2010 was successfully championed by then Vice Chairman of the Joint Chiefs of Staff, Admiral Owens and the Joint Staff J6 Director of Command, Control, Communications and Computers, Rear Admiral Arthur Cebrowski.[6] The authors proposed a new and transformational way of fighting saying:

> NCW is about human and organizational behavior. NCW is based on adopting a new way of thinking—network-centric thinking—and applying it to military operations. NCW focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent.[7]

There are nine governing principles of NCW. Overall, the principles offered by NCW theory were not intended to obviate the existing principles of war, but instead they were meant to build upon the existing principles making each of them more effective, especially in terms of time and distance. The principles are as follows:

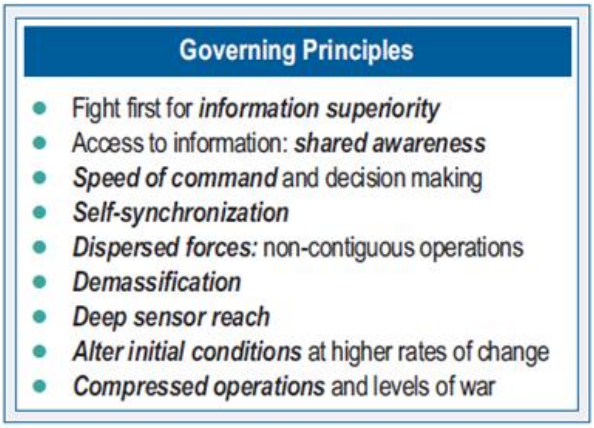

Figure 1. Governing Principles of a Net-Centric Force[8]

The first principle of NCW deals with gaining and sustaining information superiority. This can be done by increasing an adversary's need for information and simultaneously raising their uncertainty. The seminal military theorist Carl Von Clausewitz would see this as increasing an opponent's fog and friction thereby complicating their operations and overall situational awareness considerably.[9] Information superiority also requires open access to information and the availability of information resources across the global information grid. Finally to attain superiority, a force must decrease its own need for information especially in terms of volume, and focus on the sensors and data that are most applicable to the fight at hand.[10]

Next, a net-centric force must have access to information via shared awareness. This requires the building of collaborative networks to share information regardless of

location. Moreover the network must be secured in such a way that the system and information residing thereon can be defended against exploitation or attack.[11] The downside of collaborative information sharing is incorrect information can be propagated across the network and then acted upon leading to disastrous results. For this reason it is critical that information by verified and authenticated by multiple sources prior to acceptance. This validation process can lead to delays in information availability; however in a highly networked environment multiple source authentications should be relatively prompt compared to other non-networked alternatives.

In addition to shared awareness, speed of command and decision making permits recognition of an information advantage and its subsequent conversion into a competitive battlefield enhancement. The principle of speed of command is familiar to all students of Colonel John Boyd, father of the Observe-Orient-Decide-Act (OODA) loop. Colonel Boyd posits that the combatant that can observe, orient, decide, and act the fastest wins the battle.[12] In order to achieve speed of command and decision making, innovation and adaptation must reduce decision timelines converting information advantage into decision superiority and decisive effects on the battlefield. Additionally, speed of command necessitates the ability to lock out an adversary's choices in order to achieve option dominance.[13]

Self-synchronization, a key tenet of NCW, enables low-level forces to gain shared awareness of the commander's intent and operate autonomously, even to the point of retasking themselves based on how the operational situation is unfolding.[14] This principal is made possible by facilitating subordinate force initiatives in response to the battlefield tempo, increasing force understanding of the commander's intent even as

it changes or evolves, and enabling subordinate unit adaptation and responses to battlespace developments as they occur in real time.[15]

The next principle, dispersed forces, seeks to move combat operations out of a linear context and focus them instead where they are needed at a decisive time and place. In order to disperse forces, net centricity couples operations, intelligence, communications, and logistics functions to achieve precise effects while at the same time gaining speed and increasing tempo as compared to the adversary.[16]

Going hand in glove with dispersed forces, "demassification" focuses on massing of the desired effect rather than massing of force at a geographical position on the map. Of all principals of war, the principal of mass is most jeopardized in a distributed, network-oriented environment. According to Joint Publication 3-0, "The purpose of mass is to concentrate the effects of combat power at the most advantageous place and time to produce decisive results."[17] Clausewitz declared "there is no higher and simpler law of strategy than that of keeping one's forces concentrated."[18] Demassification however specifically seeks to avoid the massing of friendly forces until absolutely necessary and upon conclusion of the massing event is often followed by another demassification of combat power. Demassification also recognizes that given technology associated with remotely piloted vehicles, global reach capabilities, and instantaneous air-to-ground engagements, force massing may be undesirable and indeed counterproductive. This principle has been used to great effect against the United States military in Iraq and Afghanistan, and by non-state actors launching attacks using small groups or even individuals to spectacular effect.[19]

The expansion of forward deployed networked sensors is referred to as deep sensor reach. This principle leverages the use of intelligence, surveillance, and reconnaissance assets, satellite systems, blue force tracker, and individual operators on the battlefield. To be employed most effectively the sensor data must be fused and acted upon quickly. This is clearly the perfect job for a networked intelligent system.[20]

Like the OODA loop, the principle of altering initial conditions at higher rates of change than the enemy seeks to befuddle an adversary by adjusting faster than they can respond. For the purposes of NCW, operating swiftly and adapting rapidly to unfolding operations can have a profound negative psychological impact on an adversary even to the point of confusion where they would be unable to react or if they chose to do so would almost surely choose incorrectly, further deteriorating their situation.[21]

The final principle, compressed operations and levels of war, is attained by eliminating bureaucratic procedures between Services and forces and pushing down operations to the lowest level at which they can be conducted to achieve decisive and rapid effects. The intent of this principle is to attain the fastest speed across the spectrum of operations, enhance cooperation between low-level units, and eliminate artificial boundaries allowing the lowest possible organizational levels to work together to accomplish the mission.[22]

Understanding the governing principles of NCW is important to the overarching concept that seeks to enhance or revolutionize military operations across all warfighting domains. At its highest level, NCW hypothesizes: robustly networked forces improve information sharing; information sharing enhances information quality and situational

awareness; shared situational awareness improves collaboration, self-synchronization and speed; and finally, that these taken together increase mission effectiveness.[23] At its core, NCW is about enabling the fight in a given battlespace—this is a theory focused on warfighting.

Cyberspace Operations Background

Whereas NCW is directly focused on war fighting effects and improving commander's ability to operate in the battlespace, cyberspace operations tends to focus more on the global network enterprise as a whole. The emergence of cyberspace as a new warfighting domain has created an entirely new set of challenges and opportunities for federal institutions and commercial entities alike. At the same time, U.S. adversaries entry into the cyberspace domain has provided them a new method of attacking and exploiting system vulnerabilities at relatively low costs with little to no attribution, in near real-time across vast distances.

The definition of cyberspace has evolved over time starting with its first appearance in 1982 when Science Fiction author William Gibson used the term in the story "Burning Chrome" and later in his 1984 novel *Neuromancer* although his use of the term was far different from the one we recognize today.[24] He defined it as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation. . . data abstracted from banks of every computer in the human system.[25] The currently accepted definition was published in the September 2010 release of Joint Publication 1-02 stating cyberspace is, "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[26] Another key term is Cyberspace

Operations, defined in Joint Publication 1-02 as, “The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.”[27] The conduct of cyberspace operations is divided into three key areas: computer network defense, computer network attack, and computer network exploitation.

The three central areas of cyberspace operations: computer network attack, computer network defense, and computer network exploitation offer a useful and simplified way of examining military operations in cyberspace. A distinction between cybercrime and cyberwar is vital to understanding what is within the realm of military activity and what is within the realm of law enforcement responsibility. This analysis makes the distinction based on the political objectives sought and the effect of the attack. Borrowing from Clausewitz, if the object is political in nature with the aims of causing a submission to the adversaries will by attacking its economic, military, or political power, it shall be considered within the realm of warfare.[28] An additional consideration would have to be the seriousness of the cyberspace attack. On the low end of the spectrum, probes and exploitation would rarely necessitate war but on the other end of the spectrum creating casualties, affecting military operations, or interfering with intercontinental ballistic missile delivery systems would undoubtedly require a firm response.[29] Having defined the boundaries and intent of this analysis of cyberspace operations, the first area of examination is computer network attack.

Computer network attack, also referred to as cyberattack, is defined as the deliberate disruption or corruption by one state of a system of interest to another state.[30]

It's the only artificial manmade warfighting domain, is primarily run and operated by commercial business interests, is largely considered a non-kinetic environment, and is accessible worldwide at low cost and with effects that can be far reaching up to and including the strategic level.[31] Clausewitz held strongly that the defense was superior to the offense at the tactical and strategic levels of war.[32] In cyberspace, this hypothesis is completely upended. Counter to Clausewitz' assertion, the offensive in cyberspace is instantaneous, relatively easy to accomplish, and is often nearly impossible to attribute to any particular state or non-state actor. Cyberspace is constantly changing so that what was secure yesterday is suddenly completely unprotected simply because a new piece of improperly configured software or hardware was added or installed on a node or series of nodes comprising the network. Sun Tzu posits in his assessment of offensive strategy that "to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."[33] In cyberspace, perhaps more than any other warfighting domain winning without fighting can be accomplished with comparative ease. For instance a cyberspace operator can effectively attack an adversary's political aims directly by means of an offensive information campaign. This can be accomplished by creating websites and propaganda that undermine the enemy's stated political goals or by convincing the global audience that the enemy's political ends are unjust. A simpler method would be to modify the enemy's political message to eliminate popular support. The fight for public opinion could also be effective in disrupting enemy alliances and gaining momentum for one's own political aims on the world stage. Al Qaida's use of the Internet to inflame fundamentalist's passions and gain recruits immediately comes to mind. Clausewitz's

recognition that the attack has the advantage of initiative is especially relevant in cyberspace. In cyber war, an attack can be conducted with little to no risk and often times in a way that is all but untraceable. Furthermore, Clausewitz's recognition that surprise, popular support, and the exploitation of moral factors are crucial to strategic effectiveness all resonate perfectly in cyberspace.[34] Clearly the offensive or attack in cyberspace is superior to the defense. This is true if for no other reason than the ease by which attacks can be conducted in relation to the complexity of defending a globally interconnected information network. Recognition of the offensive's superior role in cyber warfare in no way diminishes the crucial role of cyberspace defense—indeed a perfect security posture would change these roles if technology or tactics presented such a solution.

Cyberspace defense or computer network defense is focused on the protection of computer based systems and information networks and is often referred to as information assurance. Defending computer networks is a cyberspace practitioner's most difficult task. In terms of warfare it is akin to building defensive barriers to prevent an adversary from penetrating vast expanses of sovereign territory. Perhaps a useful analogy would be France's Maginot Line of fortifications that were built following World War I to prevent or slow a German offensive. Much as these barriers were overrun in World War II; the defense of a network can be easily circumvented at its weakest point. Taking this example a step farther, imagine that France had global interests and extended the fortifications to cover the globe with thousands and perhaps millions of required entry points for the purposes of its own interests. While an overly simplified illustration, it provides some sense of the difficulty of defending such a massive frontier.

Network defenders tasked to provide information assurance view the global information grid as a series of linked defenses. The weakest link in the defense causes it to fail and an unfounded belief that the overarching system is secure provides a false sense of security that is easily exploited. By its very nature the development of redundancies or multiple entry points to ease network access simplifies the task of determined hackers. As the beneficiary of the Internet's great promise, the United States has invested heavily in economic, commercial, and governmental access to networked resources. The problem is that cyberspace like the maritime and space domains is an unconquered realm shared by the world and no one can claim or fully control it. The Internet was designed from its earliest conception to ease interaction, communications, and information sharing—in this it has exceeded all expectations. Perhaps if the Internet had been developed as a "fortress" from the outset the ease of defense would have been manageable. This, however, would have defeated its purpose and relegated it to relative obsolescence over time. So what might Clausewitz have contributed to cyberspace defense? The answer lies in economy of force at the decisive point. Clausewitz recognized that applying force where it matters most is critical to success. Therefore, it is incumbent on those that operate in cyberspace to focus effort at the decisive point. In cyberspace this requires understanding what must be protected and what is irrelevant to the strategic purpose writ large. To a large extent this goes to Sun Tzu's assertion "Know the enemy and know yourself; in a hundred battles you will never be in peril."[35] This axiom requires first a clear understanding of the enemy's capabilities in cyberspace; both what they wish to attack or exploit and what they need to protect or defend. Furthermore it dictates a solid understanding of our vital information, cyber

capabilities, strengths and weaknesses so that the information can be protected from cyber exploitation.

Cyber exploitation can be thought of simplistically along the lines of spying and eavesdropping. The purpose of cyber exploitation is to obtain information about your adversary's intents, strengths, and weaknesses. Clausewitz's famous concepts of fog and friction are relevant and compelling in cyberspace. He states "fog can prevent the enemy from being seen in time," and friction "is the force that makes the apparently easy so difficult."[36] In theory, cyber exploitation serves to lift the "fog" and reduce the "friction." Paradoxically, the vast information stores available via cyberspace and the perishability of data residing there may very well counteract the benefits gained by exploitation. Nonetheless, a determined and well trained intelligence agent with powerful search tools, multiple sources of verification, and patience will benefit greatly from the ease of access and anonymity afforded in cyberspace. Those that argue that the sheer volume and perishability of information offered across the network make it somehow useless do so at their own peril. Cyber exploitation used in conjunction with cyberspace attack and cyberspace defense compromise a basic yet workable understanding of cyberspace operations.

Similarities between NCW and Cyberspace Operations

When the National Military Strategy for Cyberspace Operations was developed, it was clearly done with a solid understanding of and respect for NCW. Of all the military doctrine developed concerning the conduct of cyberspace operations, it contains the most parallels with NCW theory. The four priorities of cyberspace operations[37] are:

- Gain and maintain initiative to operate within adversary decision cycles

- Integrate cyberspace capabilities across the range of military operations
- Build capacity for cyberspace operations
- Manage the risk for operations in cyberspace

With a little analysis, these priorities can be aligned indirectly with NCW principles. The first priority aligns with the two network centric principles of speed of command and decision making and altering initial conditions. The second cyberspace priority applies across all principles of NCW seeking to operate across the entire range of military operations. Interestingly, the third priority is not addressed so much as a principal of NCW but applies more to its overarching tenants that a fully networked environment enables robustly networked forces, improving information sharing and increasing mission effectiveness. The fourth priority, managing the risk, correlates to the first NCW principle of attaining information superiority. In addition to these parallels major similarities include a foundation based upon the principles of war, the operating environment itself, and the complexity of the environment.

The first similarity is the building of both concepts on the foundation of the principles of war. The designers of both ideas wisely chose to build upon well-defined principals of war and seminal war theory. This was an important consideration since these concepts are already understood and taught to all military personnel. The United States Air Force even went as far as to directly correlate all twelve principles of war (objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, simplicity, restraint, perseverance, and legitimacy) directly to cyberspace operations.[38] The same thing was done for NCW by United States Marine Corps

Lieutenant Colonel William Callahan, tying each and every principle to full spectrum operations.[39]

Another clear parallel is the operating environment. NCW and cyberspace operations are both conducted within the cyberspace domain. Both recognize the domain as that environment where information is created, manipulated, processed, stored, and shared across the network[40]. Despite the fact that both operate in and through cyberspace, they do so in very different ways. Cyberspace operations are applied across the entirety of the cyberspace domain while NCW is more narrowly focused on the battle at hand. Whereas cyberspace operations could support simultaneous warfighting operations across multiple theaters, NCW would exist as separate NCW focused efforts at the operational theater level. For illustration, cyberspace operations currently support operations in Iraq, Afghanistan, and at home in the U.S. against hackers. On the other hand, NCW is employed by the theater commander in Iraq and as a separate effort by the theater commander in Afghanistan as two distinct efforts. There are also significant differences in how the operating environment is viewed. NCW's framework extends beyond the information realm to include the cognitive, social, and physical domains[41] while the definition of cyberspace found in Joint Publication 1-02's focuses more on the global network as an operational environment.[42] Furthermore NCW tends to look at the operating environment in terms of how it directly correlates to warfighting within a prescribed battlespace whereas cyberspace includes the whole global information grid, including the Internet in its entirety. Arguments over scope aside, there is no dispute regarding the operating environment where both NCW and cyber operations reside.

The final major similarity between the two concepts is that they are both incredibly complex and have stringent training requirements. The complexity of the environment means that managing vast stores of information, maintaining network availability, and protecting the network from intrusions are difficult to assure. During warfighting operations there is little tolerance for mistakes or failures when lives are at risk, and in the cyber environment maintenance downtime, outages, and disruptions are inevitable. These disturbances can largely be managed by providing redundancies across the network however; this increases the complexity of network administration. In order to minimize outages and maximize the tenets of cyber operations and net centricity, network operators must be highly trained and experienced. The very skills that these cyber operators demonstrate make it very difficult to retain them since they are so highly valued in commercial industry as well. NCW can also complicate the actions of lower-level operators since they now have an additional requirement to provide information upon which decision makers must rely to make operational decisions. The complexity of the environment can also complicate already disjointed coalition operations. During Operation Enduring Freedom the U.S. was required to purchase communications equipment to bolster NATO interoperability, and with the newest NATO nation's technology training was also a tremendous hurdle.[43] Complexity and rigorous training requirements in the coalition environment serve to ratchet up interoperability complications to near intolerable levels.

Differences between NCW and Cyberspace Operations

The key differences between cyberspace operations and NCW are their levels of support, the operators, the level of effects, and the adversaries' success in the environment. To a large extent the levels of support for each concept appears to have

greatly affected their overall relevance, longevity, and success. NCW was supported primarily by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff. There is no evidence that NCW rose to the level of Presidential influence and therefore with the exception of the U.S. Navy, the Services were not willing to invest in the associated technologies. Perhaps a more important indication of the level of support for NCW was the reaction of the business world to emerging NCW thinking. Because NCW was narrowly focused to the warfighting environment, businesses outside the military industrial base had little reason to invest in the development and success of NCW. Without the support of the business world it was a sure bet that NCW would be relegated to DOD circles alone.

Cyberspace, on the other hand, steadily gained momentum within DOD and industry circles as both experienced increasing instances of damaging cyberattacks and cyber exploitations. Seeing the need for a cohesive approach to protecting U.S. information, economic, and military interests, President George W. Bush released the National Security Strategy to Secure Cyberspace in February of 2003. This foundational document enabled all the other concepts and doctrine that followed to have significance across the federal government and industrial base. The President's strategy established a much needed national response system, a threat reduction program, a training program, and guidance on international cyberspace security cooperation.[44] The Chairman of the Joint Chiefs of Staff's National Military Strategy for Cyberspace Operations logically flowed from the President's strategy. The business world and federal government followed suite implementing their own systems to protect critical infrastructures and information stores from global threats. The level of

Presidential support and nature of the threat ensured that cyberspace would have an important place in America's priorities.

NCW and cyberspace operators share some similarities at the network administration level; however they differ greatly at the operational level. In the NCW battlespace every warfighter is a sensor. Correlated information obtained from sensors and disseminated in a near real-time environment drives faster decision cycles and enables decisions to be pushed down to lower-level operators for rapid reaction and response. In this information rich setting, NCW seeks to realize the promise of rapid decision making within the enemy's OODA loop. In contrast, cyberspace operations do not rely on fighters at the edge but instead focus on highly trained cyber operators at the core. The cyber community is comprised primarily of technicians to defend the network, intelligence personnel to exploit information, and a mix of intelligence personnel and operations personnel to conduct cyberattacks.

The operational levels of war that cyberspace and network centric operations are applied at are also quite different. Admiral Cebrowski intended NCW to apply "at all three levels of warfare—strategic, operational, and tactical—and across the full range of military operations from major combat operations to stability and peacekeeping operations" [45] Despite this intent, NCW has been criticized in government and military circles because its effects tend to apply primarily at the tactical and operational levels of war. This is not a flaw of NCW, but simply recognition that it tends to be narrowly focused within a specific theater of operations. In contrast, cyberspace operations have effects at all levels of war and the results of large scale cyberattacks have proven to have significant effects at the operational and strategic levels. A few recent examples

were the propagation of the “Stuxnet”[46] worm affecting Iranian nuclear reactors and “Titan Rain”[47] a data exploitation program that was wielded against the U.S. DOD very effectively.

The final difference between the concepts is closely tied to the ascent of cyberspace as a focus area—the effectiveness of system penetrations. Adversary successes against the U.S. in cyberspace have been destructive and effective at all levels of the business and government domains. The reason cyberspace operations matters so much is the enemy has been so successful at attacking and exploiting U.S. networks and information. NCW as employed in Iraq and Afghanistan has faced no comparable adversary or threat. The U.S. military’s technological dominance has made the possibility of the current opponent’s success attacking and exploiting U.S. networks somewhat immaterial. To coin a phrase “if it ain’t broke, don’t fix it” and with or without NCW, the U.S. military succeeds brilliantly at the tactical and operational levels of war enabling dominance across the full spectrum of military operations. As such NCW successes and failures are not nearly as significant or compelling as the potentially catastrophic failures in cyberspace.

Recommendations

As has been discussed while analyzing the backgrounds of NCW and cyberspace operations, there are many similarities and differences between the two concepts however the key to future success in cyberspace can best be achieved by blending the two concepts in the cyberspace operating environment. By uniting the two concepts combined effects are gained and amplified to better address the tactical, operational, and strategic levels of war. Where NCW is better applied at the tactical level, the two concepts converge at the operational level, and at the strategic level of

war, cyberspace operations more fully address desired effects than NCW which can yield strategic effects but is not designed to do so with any regularity. And where NCW is more gainfully employed by operators in the active theater of operations, cyberspace operations provide a global, secure, reliable, and trustworthy operating environment upon which NCW must necessarily rely. The advantage of combining NCW and cyberspace operations is that the strengths, weaknesses, similarities, and differences tend to overlap and complement each other filling gaps and seams in the concepts.

NCW and cyberspace operations were conceived to achieve different results. NCW was designed to enable the warfighter on the battlefield and empower forces from the lowest to the highest level in a theater of operations. NCW was designed to help warriors fight better, faster, and smarter at the same time understating the situation on the field in previously unimagined. Cyberspace operations were developed to service a different need altogether. Cyberspace operations never promised to improve the OODA loop, they never promised to improve situational awareness on the ground, and they never ever sought to change or empower human and organizational behaviors. Instead cyberspace operations focused on sustaining and protecting the U.S. operating environment, enabling attacks to shape and soften the enemy's core networked infrastructures, and prudently exploiting information that strengthens knowledge while weakening an opponent's understanding. To maximize the potential of NCW and cyberspace operations the two concepts should be fused into one all-encompassing model (figure 2).

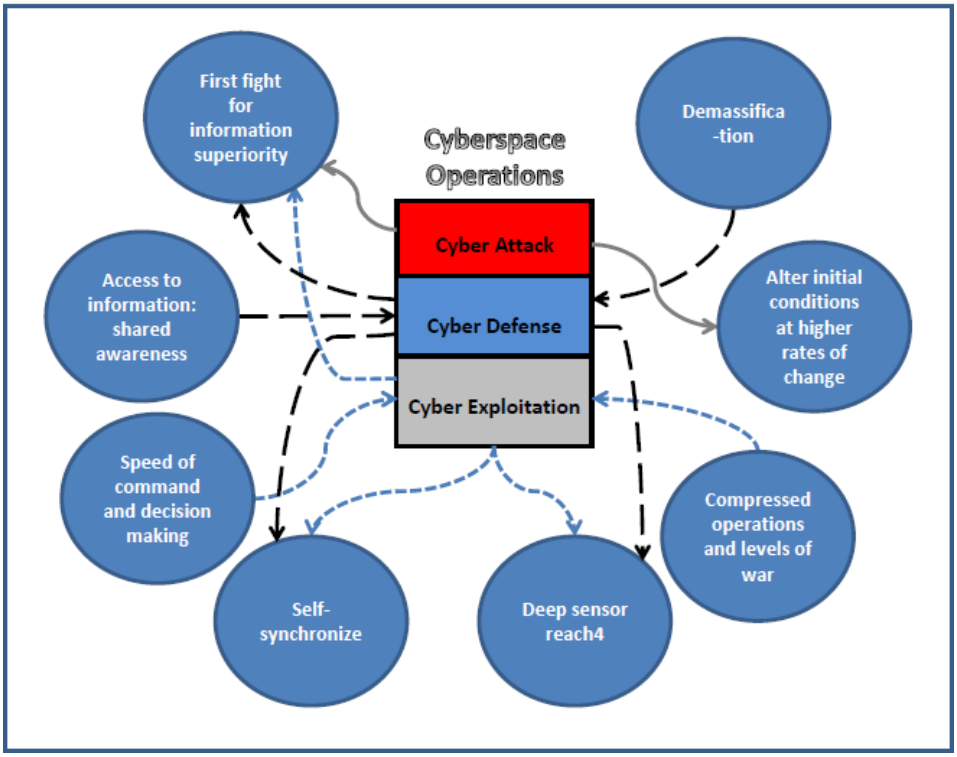

Figure 2. Synergistic Effects

Not surprisingly, since the concepts share a number of similarities integration should not require a tremendous expenditure of effort or cost. A notional diagram showing the relationships between NCW and cyberspace operations depicts the interaction of cyber-attack, defense, and exploitation with information superiority. In the focused NCW environment, cyber defense, attack, and exploitation are key contributors to the NCW fight for information superiority. On the other hand, the NCW concept of shared awareness needs to be developed across cyberspace operations. Currently cyber defense and anti-exploitation efforts suffer greatly from a lack of shared awareness across the global information grid. In the NCW environment every fighter is a sensor—the same approach is needed across the cyber enterprise. National and international government agencies, law enforcement organizations, and commercial

establishments need to act as sensors across the cyber realm so that defenses can be improved, attacks can be sensed and deterred, and exploitation efforts can be frustrated. This will require a multipronged approach that produces support at the highest levels of the federal government, delivers a comprehensive cyber strategy, amalgamates existing doctrine, and trains professional military operators at all levels from the core to the edge. Several other synergistic effects are logically laid out such as demassification of cyber forces to defend the network until such time as an attack is identified and can then be defended by a focused effort at the decisive point of attack.

Conclusion

NCW was an innovative and empowering concept that was arguably ahead of its time. Its principles and concepts improve and complement cyberspace operations by filling gaps, delivering immediate effects on the battlefield, and empowering battlespace awareness while at the same time benefitting from cyberspace operations ability to cripple the enemy's operations through cyberattacks, sustain our own cyber environment through cyber defense, and know what your adversary knows through cyber exploitation. The concepts of NCW and cyberspace operations concepts belong together and yes, NCW has earned its place in the age of cyberspace operations and the warfighter deserves the benefits afforded by fusing these concepts now.

Endnotes

[1] CBS Interactive Staff, "DoD Gates: We're always under cyberattack," April 22, 2009, http://www.zdnet.com/news/dod-gates-were-always-under-cyberattack/290770, (accessed January 12, 2011).

[2] Dr. Sean Lawson, "Is Network-Centric Warfare (Finally) Dead? Only Partly," http://www.seanlawson.net/?p=772, (accessed September 20, 2010).

[3] Dr. Jeffrey L. Groh, "Network Centric Warfare (NCW) never went away," April 5, 2010, http://www.carlisle.army.mil/dime/blog/archivedArticle.cfm?blog=dime&id=97, (accessed 15 October, 2010).

[4] Martin C. Libicki, *Conquest in Cyberspace, National Security and Information Warfare*, (Cambridge University Press, 2007), 1.

[5] James Blaker, "Arthur K. Cebrowski: a retrospective," Spring 2006, http://findarticles.com/p/articles/mi_m0JIW/is_2_59/ai_n16689841/pg_5/?tag=content;col1, (accessed December 1, 2010).

[6] Ibid.

[7] Arthur K. Cebrowski and John Garstka, Jr., "Network Centric Warfare: Its Origins and Future," Proceedings: U.S. Naval Institute 124, No. 1, 1998, in Alberts, Garstka, and Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 88.

[8] Director, Force Transformation, Office of the Secretary of Defense, "The implementation of Network-Centic Warfare," January 5, 2005, http://www.au.af.mil/au/awc/awcgate/transformation/oft_implementation_ncw.pdf, (accessed 19 November, 2010), 8.

[9] Carl von Clausewitz, On War, ed. and trans. Michael Howard and Peter Peret (Princeton, NJ: Princeton University Press, 1976), 120-121.

[10] Director, Force Transformation, Office of the Secretary of Defense, "The Implementation of Network-Centic Warfare" 8.

[11] Ibid.

[12] Boyd, J. *PATTERNS OF CONFLICT*, December 1986. (Unpublished study), 5.

[13] Director, Force Transformation, Office of the Secretary of Defense, "The Implementation of Network-Centic Warfare" 9.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Joint Publication 3-0, A-1.

[18] Carl Von Clausewitz, *On War* (Princeton: Princeton University Press, 1984), 204.

[19] Director, Force Transformation, Office of the Secretary of Defense, "The Implementation of Network-Centic Warfare" 9.

[20] Ibid., 9.

[21] Ibid., 10.

[22] Ibid.

[23] Ibid., 7.

[24] Wikipedia, s.v. “Cyberspace,” http://en.wikipedia.org/wiki/Cyberspace (accessed 22 February 2011).

[25] Ibid.

[26] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 7 May 2002, 29.

[27] Ibid.

[28] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Peret (Princeton, NJ: Princeton University Press, 1976),

[29] Martin C. Libiki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 181.

[30] Ibid, 23.

[31] Lt Col David M. Hollis and Katherine Hollis, The cyberspace policies we need (Armed Forces Journal, Jun 2010), 20.

[32] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Peret (Princeton, NJ: Princeton University Press, 1976), 358.

[33] Sun Tzu, *The Art of War*, trans. Samuel B Griffith (Oxford: Oxford University Press, 1963), 77.

[34] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Peret (Princeton, NJ: Princeton University Press, 1976), 363.

[35] Ibid, 84.

[36] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Peret (Princeton, NJ: Princeton University Press, 1976), 120-121.

[37] "The National Military Strategy for Cyberspace Operations", Chairman of the Joint Chiefs of Staff, DoD, December 2006.

[38] Air Force Doctrine Document 3-12 on Cyberspace Operations, United States Air Force, July 2010, 16-17.

[39] Lieutenant Colonel William E. Callahan, *The Effects of Network-Centric Enabled Operations Forces on the Principles of War*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, 15 March 2008) 1-19.

[40] Center for Strategic Leadership, Network Centric Warfare Case Study, Dave Cammons, John B Tisserand III, Duane E. Williams, Alan Seise & Doug Lindsay (US Army War College, Mar – Apr 2003) 16.

[41] Ibid.

[42] National Military Strategy for Cyberspace Operations, December 2006.

[43] "Technologies Empower Coalition Information Sharing; but Not All Interoperability Challenges Are Equipment Based.," Digital Signal Magazine August 2006 (2006), http://www.afcea.org/signal/articles/anmviewer.asp?a=1175&print=yes. Page 1"

[44] The National Strategy to Secure Cyberspace, February 2003.

[45] Director, Force Transformation, Office of the Secretary of Defense, "The implementation of Network-Centic Warfare," January 5, 2005, http://www.au.af.mil/au/awc/awcgate/transformation/oft_implementation_ncw.pdf, (accessed 19 November, 2010), 4.

[46] William J. Broad, John Markoff and David E. Sanger," Israeli Test on Worm Called Crucial in Iran Nuclear Delay," 15 January, 2011 http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2, accessed 27 February, 2011).

[47] Nathan Thornburgh, "Inside the Chinese Hack Attack," 25 August, 2005, http://www.time.com/time/nation/article/0,8599,1098371,00.html, (accessed 26 February, 2011).