

## The Network-Centric Warfare Journey: Realizing the Power of Information

By Jeffrey L. Groh

*...the general unreliability of all information presents a special problem in war: All action takes place, so to speak, in a kind of twilight, which like fog or moonlight, often tends to make things seem grotesque and larger than they really are.*

*Whatever is hidden from full view in this feeble light has to be guessed at by talent, or simply left to chance. So once again for lack of objective knowledge one has to trust to talent or to luck.*

Clausewitz<sup>1</sup>

What is all this fuss about network-centric organizations? Is Network-Centric Warfare an “emerging theory of war” or just about technology? Is it possible to harness the power of information to gain a significant advantage in the operational environment? Scholars, politicians, appointed government officials and warfighters continue to line up to take sides on the utility of information sharing and reliance on networking of U.S. military forces.<sup>2</sup> Even the term “Network Centric Warfare” continues to spark emotion.<sup>3</sup> The business community continues to grapple with knowledge management, business process management, information technology (IT), and enterprise networking to gain a competitive advantage in the market place.<sup>4</sup> There is a plethora of literature documenting how IT is enabling innovation in business as well as the military.<sup>5</sup> It is time to continue the dialogue and raise the awareness of the benefits of network-centric operations as an enabler to gain a competitive advantage over current and potential adversaries in the 21<sup>st</sup> century. If we agree that Clausewitz is correct about the unreliability of battlefield information, could Network-Centric Warfare concepts and capabilities improve this situation? The Department of Defense continues to pursue an aggressive policy to develop network centric warfare (NCW) capabilities as a “source of warfighting advantage.”

This paper argues that the Department of Defense is on the right track to pursue advanced integrated information technology to enable warfighting in the future. This paper does not argue that information systems and technology are the panacea to solve all the complex issues associated with warfare in the 21<sup>st</sup> century. This essay begins with a brief discussion of the fundamental concept of network-centric warfare and the current Department of Defense policy for networking the force. Then, the paper will investigate the potential of information and knowledge sharing on the battlefield to provide a competitive advantage against potential adversaries. There are tactical, operational, and strategic implications<sup>6</sup> to sharing information and networking the force within the operational environment. This paper would not be complete without addressing a few of the most prevalent arguments by those who caution against relying on information technology and networking. The final section of the essay will outline a few recommendations to proceed with the implementation of network-centric warfare. This paper

chronicles the evolution of Network Centric Warfare and its implications for DOD and the future of warfare in the 21<sup>st</sup> century.

### **Network Centric Warfare (NCW): Developing a Concept**

It should not be a secret that the world is squarely in the age of information. One only needs to view the nightly news, scan the newspapers, or pick up the latest technology books and trade journals to understand the magnitude of corporate investments in information systems. “Worldwide, businesses spend nearly \$1 trillion a year on IT gear, software, and services—more than \$2 trillion if telecommunications services are included.”<sup>7</sup> The enormity of the spending by corporations around the world on new ways to capture, store, and share information inside and outside of organizations continues to increase since the turn of the century. The Department of Defense is well aware of the potential benefits of sharing information and knowledge to generate competitive advantage.

There is a significant body of literature that addresses the benefit of sharing information on the battlefield to develop a common operating picture. It is not possible to conduct an exhaustive review of the literature related to NCW in this short article. However, it is important to review some of the seminal works that establish the fundamental underpinnings of this dynamic concept. The former Office of Force Transformation, Office of Secretary of Defense was a leader to develop the concept of Network Centric Warfare. The Department of Defense Command and Control Research Program continues to be a conceptual leader developing the theory of Network-Centric Warfare. One of the last publications from the Office of Force Transformation, *Implementation of Network-Centric Warfare*, released in January 2005, established the current thinking on NCW, by providing “answers to some of the fundamental questions regarding NCW as emerging theory of war in the information age.”<sup>8</sup>

There is an important body of knowledge published by the Command and Control Research Program that provides the theoretical development of the concepts of Network-Centric Warfare for the Office of the Secretary of Defense.<sup>9</sup> One should begin the journey to examine the potential of NCW by closely reading the book authored by Dr. David Alberts, Mr. John Garstka, and Mr. Fred Stein titled, *Network Centric Warfare: Developing and Leveraging Information Superiority*.<sup>10</sup> A careful reading of the book will explain the purpose and concept of NCW, how NCW has the potential to leverage information age technologies, and a methodology to implement the concept over time.<sup>11</sup> The authors proposed this early concept of NCW as a point of departure:

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.<sup>12</sup>

The publications in 1998 set the stage for the intellectual debate on the potential of NCW as a new way to examine the conduct of war in the 21<sup>st</sup> century with networked forces and enhanced situational awareness.

NCW is about warfighting in the 21<sup>st</sup> century. It is about warfare in the information age. There are significant new information technologies that enable commanders to know more about the enemy, plan faster, make decisions faster, and synchronize sensors and shooters to create desired effects on the battlefield. David Alberts, in *Information Age Transformation*, conducts a thorough analysis of what warfare will entail in the 21<sup>st</sup> century; he postulates the challenges with warfare in the information domain. “As the global society enters the information age, military operations are inevitably impacted and transformed. Satellite communications, video teleconferencing, battlefield facsimile machines, digital communications systems, personal computers, the Global Positioning System, and dozens of other transforming tools are already commonplace.”<sup>13</sup> The question then becomes how to transform a military force with the appropriate capabilities to operate in this new environment.

The author proposes that the following NCW tenets should guide the adoption of information technologies and transformation:

- A robustly networked force improves information sharing.
- Information sharing and collaboration enhance the quality of information and shared awareness.
- Shared situational awareness enables self-synchronization.
- These, in turn, dramatically increase mission effectiveness.<sup>14</sup>

Alberts presents these tenets espousing the potential benefits of information sharing, networking, and enhanced situational awareness act as an organizing function to transform the force in the information age. These tenets provide a series of research questions to analyze case studies to investigate the potential benefits of a networked force.<sup>15</sup>

Alberts and Hayes continued to expand the idea of the inherent benefits of sharing information in a networked environment in their next book titled, *Power to the Edge: Command Control in the Information Age*. The book argues that current command and control relationships, organizations, and systems are just not up to the task of executing warfare in the information age.<sup>16</sup> It is critical to push essential decision-making information out to the “edges” of the organization. “*Power to the Edge* is about changing the way individuals, organizations, and systems relate to one another and work. ‘Power to the Edge’ involves the empowerment of individuals at the edge of an organization (where the organization interacts with its operating environment to have an impact or effect on that environment) or, in the case of systems, edge devices.”<sup>17</sup> The ubiquitous nature of IT makes the vision of achieving “Power to the Edge” possible. The transition from strictly hierarchical organizational structures is already underway. The Army’s restructuring to smaller more lethal Brigade Combat Teams and Stryker Brigades takes advantage of more powerful networks to push information and thus greater situational awareness out to the edges of organizations.

The power of the network has provided new and innovative approaches to command and control organizations. One needs only to review the legendary actions of small Special Forces Teams on horseback during Operation Enduring Freedom to see the power of interdependent edge organizations networked to accomplish desired effects on the battlefield.<sup>18</sup> Small Special Forces Teams operating with satellite communications equipment (data and voice) synchronized joint fires to attack targets. Special Forces Teams adroitly coordinated and laser designated targets for Joint Direct Attack Munitions from F-14, F-15E, B-1, and B-2 airframes during OPERATION ENDURING FREEDOM (OEF) with devastating results and accuracy.<sup>19</sup> The relationship between sensors (Special Operating Forces, Predator, and Global Hawk) and shooters (AC 130, B-1, armed Predators, numerous USAF fighter assets) linked through a network to command and control demonstrates the potential benefits of the concept. This is but one example of the future potential of a networked force that pushes critical information to those that need it when they need to accomplish tasks in the operational environment.

Let's fast forward to operations in Iraq and Afghanistan today. General David Petraeus, commander U.S. Central Command, stated,

I was a skeptic of network-centric warfare for years...But thanks to years of wartime funding the military now has the ability to transmit data, full-motion video, still photos, images, information. So you can more effectively determine who the enemy is, find them and kill or capture, and have a sense of what's going on in the area as you do it—where the friendlies are, and which platform you want to bring to bear.<sup>20</sup>

The U.S. military is in the early stages of understanding the full potential of network-centric warfare and sharing knowledge out to the edges of an organization i.e., *Power to the Edge* becoming a reality.

This brief NCW literature review would not be complete without mentioning the Network Centric Operations Conceptual Framework Version 2.0. There are numerous critics of NCW calling for academic rigor to be applied to this emerging concept. There is a need to develop a framework to produce metrics that can empirically measure the efficiency and effectiveness of NCW. It is important to validate where to spend finite defense dollars to achieve the greatest possible return on investment.

As a consequence, OFT [the Office of Force Transformation] and OASD-NII [Office of the Assistant Secretary of Defense, Networks & Information Integration] began collaborating on an effort to develop metrics to test hypotheses in the NCW value chain. The primary objective was to develop a rich and comprehensive set of NCW-related metrics that could be used in experimentation and other research endeavors to gather evidence. This evidence then could be used in experimentation and other research endeavors across the DOTML-PF [doctrine, organization, training, materiel, leadership and education, personnel and facilities] spectrum. This effort resulted in the

development of a Conceptual Framework for Network Centric Operations and a variety of other NCO-related research, outreach and publications.<sup>21</sup>

This document begins to address a more rigorous approach to measure the efficiency and effectiveness of NCW. This framework may provide measures of effectiveness and performance to truly measure the benefits of NCW in the future.

The Network Centric Operations Conceptual Framework (NCO-CF) proposes a series of concept definitions, attributes and metrics to measure numerous elements of NCW based on the NCO-CF:

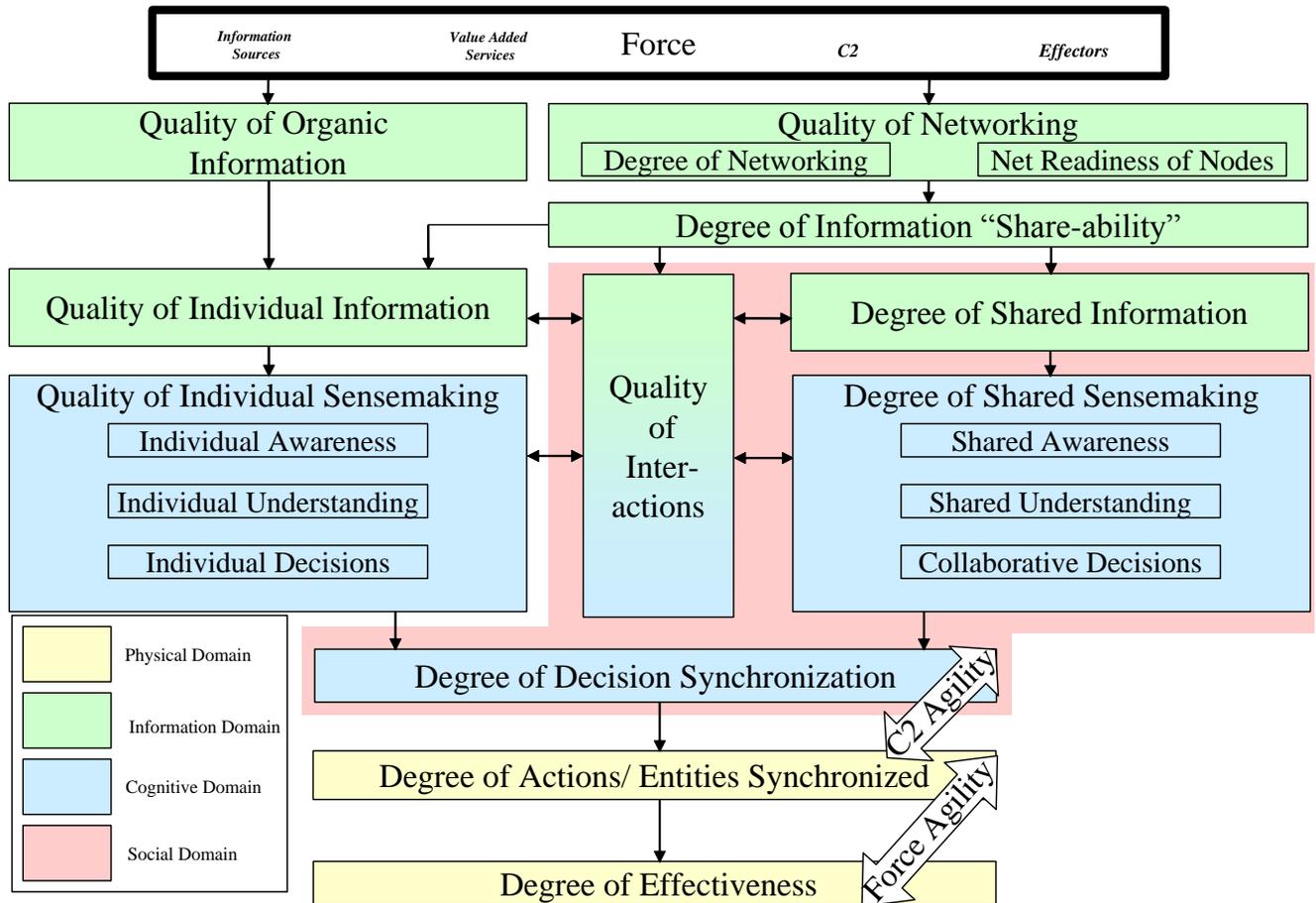


Figure 1: The Network Centric Operations Conceptual Framework<sup>22</sup>

The NCO-CF defines each concept and attribute and recommends a quantifiable metric for each. The draft schema presented in the NCO-CF is complex and untested. It is however, a step in the right direction. This framework goes well beyond the general assertions of efficiency and effectiveness outlined in the NCW Tenets. The NCO-CF “provides basis for quantitative exploration and/or assessment of NCW hypotheses; and investment strategies and other DOTML-PF related issues.”<sup>23</sup>

It will take a substantial effort to validate the attributes and metrics proposed in the NCO-CF. The metrics for many of the attributes are based on a Likert scale i.e., a scale of 1-5. There is a degree of subjectivity involved with assigning a value to the attribute. How does one truly measure quality, consistency, currency, precision, completeness, accuracy, relevance and timeliness of information? These attributes begin to investigate, experiment, and test metrics. However, the next step must be to gather a committee of experts to further define the attributes and metrics based on more objective criteria. Another approach is to begin gathering data using the proposed attributes and metrics to determine the validity of the framework. This work started with the publication of the *Network-Centric Operations Case Study: the Stryker Brigade Combat Team*.<sup>24</sup> This report along with the NCW Operation Iraqi Freedom case, *A Network-Centric Operations Case Study: US/UK Coalition Combat Operations during Operation Iraqi Freedom*,<sup>25</sup> points out the difficulties of applying the attributes and metrics of the NCO-CF in an empirical study.

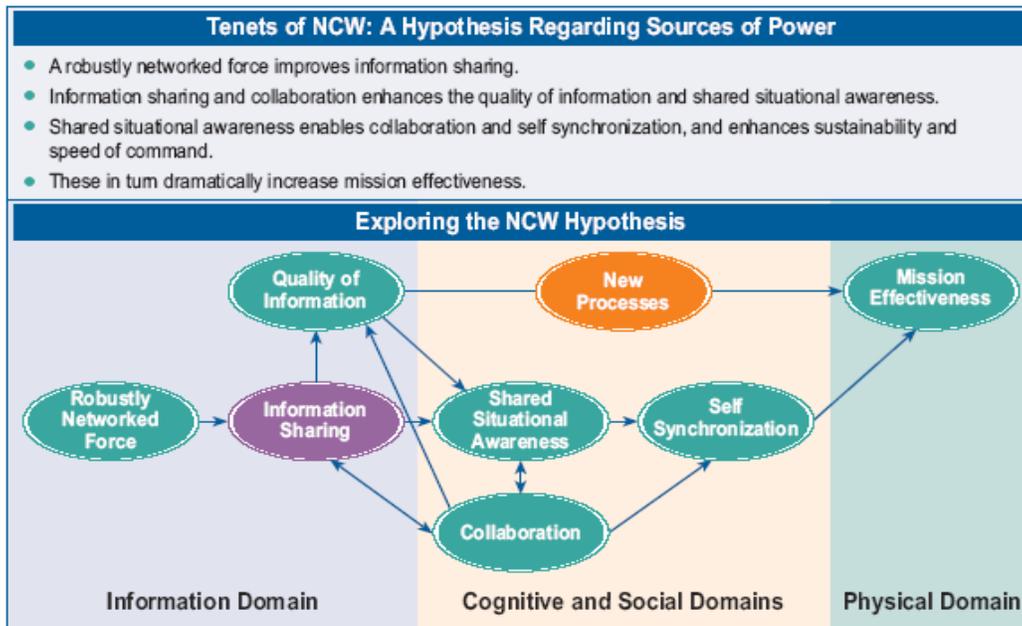
The publication that explains the potential of NCW and NCO as an emerging theory war is the Office of Force Transformation publication *The Implementation of Network-Centric Warfare*. This publication by the OFT touts NCW as an “emerging theory of warfare in the information age.”<sup>26</sup> The authors bring the numerous concepts associated with NCW, outlined in this compressed literature review, into a concise framework. The purpose of the framework is to begin to work the fundamental hypothesis of Network-Centric Warfare. “The working hypothesis of network-centric warfare (NCW) as an emerging theory of war, simply stated, is that the behavior of forces, i.e., their choices of organization relationships and processes, when in the networked condition, will outperform forces that are not.”<sup>27</sup> It is important to review this work in order to have a meaningful dialogue about the potential of Network-Centric Warfare as an emerging theory of warfare.

The hypothesis stated above focuses on several critical variables prior to discussing the issue of a “networked force.” Many critics of NCW have focused mainly on the technology aspect of NCW.<sup>28</sup> However, NCW is much more than the information technology. First, NCW entails examining organizational relationships and processes. Then, highly effective and efficient organizations are networked to leverage shared knowledge and information in the operational environment. A balanced and holistic assessment of NCW is called for to determine the potential of this concept on the modern battlefield.

The human behavior variable remains a crucial aspect of NCW. “The implementation of NCW is first and foremost about human behavior as opposed to information technology. While ‘network’ is a noun, ‘to network’ is a verb. Thus, when we examine the degree to which a particular military organization, or the Department as a whole, is exploiting the power of NCW, our focus should be on human behavior in the networked environment.”<sup>29</sup> This publication goes into considerable detail outlining the numerous benefits of networking humans to share information and knowledge. NCW is all about connecting individuals across the operational environment to leverage information age technologies to reduce the “fog and friction of war.” There is no attempt to imply that a networked force can eliminate fog and friction of war. “This will not be the case. Rather, the issue is how one creates and exploits an information advantage within the context of the fog and friction of war.”<sup>30</sup> However, there is a case to be examined that linking warfighters together on the battlefield may increase speed of command and synchronize dispersed forces to more efficiently and effectively accomplish objectives. Therefore, although

the reliance on technology is apparent when discussing the potential of NCW, it is important to examine the literature as it relates to the human dimension of the concept.

The OFT publication *Implementation of Network-Centric Warfare* goes further to outline the importance of human behavior in NCW by investigating the tenets of NCW. Figure 2 demonstrates the important relationship between the information domain, the cognitive and social domains, and the physical domains. The essence of the concept is in the understanding of these relationships. The information domain is where data, information, and knowledge are created, manipulated and shared among warfighters. The cognitive domain is where the data, information, and knowledge are manipulated in the mind of the warfighter. The all important social domain is where the interaction between humans occurs. “This is also the domain of culture, the set of values, aptitudes, and beliefs held and conveyed by leaders to the society, whether military or civil.”<sup>31</sup> An understanding of the relationship between the information, cognitive and social domains begins to address the core principles of NCW as they relate to the physical domain i.e., mission accomplishment.



**Figure 2: Tenets of NCW and the Value**

The human behavior aspect of this schema is central to understanding NCW as a “source of Warfighting advantage.” The networked force enables information sharing, shared awareness, and self synchronization within the information domain. The real warfighting and decision-making functions remain in the cognitive and social domains. Is there any evidence that units are actually operating within this framework?

The Office of Force Transformation had set out to document the fact that units are already operating in a network centric operational framework. OFT developed numerous NCO case studies that applied the NCO-CF, gather data, and analyze evidence. It is beyond the scope of this paper to review all of the case studies. However, the results of Ground Operations

(Stryker Bridge Combat Team) will illustrate the potential benefits of NCW. The case study explored the hypothesis that “the NCO capabilities of the Stryker Brigade Combat Team (SBCT) would enable information and decision superiority and increase force effectiveness.”<sup>32</sup> The conditions for the test were an operational environment (Small Scale Contingency) at the Joint Readiness and Training Center (JRTC) conducted in May 2003. The baseline for this study was to compare the SBCT against a non-digitized light infantry brigade. The study measured the quality of effectiveness of command and control based on the degree of situational awareness, speed of command, quality of decisions, and force self-synchronization.<sup>33</sup>

The results of the study are impressive. It is important to note that 75 percent of the SBCT had networked battle command systems. A few of the most interesting findings are the following:

- Friendly vs. enemy casualty ratio decreased from a normal JRTC rotation with a light infantry brigade from 10:1 to 1:1;
- Acceleration of speed of command from 24 to three hours in engagements;
- Increase in individual/shared information quality from 10% to 80%.<sup>34</sup>

The results only begin to scratch the surface of potential benefits of fully networked forces. One can argue the rigor, conditions, standards, and data gathering methods for this study. However, these results should stimulate additional rigorous experiments to validate the return on investment of maneuvering a networked force. The Army has yet to fully determine the actual benefits and effectiveness of the networked SBCTs serving in OPERATION IRAQI FREEDOM. It will be interesting to compare the results from this JRTC study, quantitative and qualitative, to the data collected in Iraq in ongoing counterinsurgency operations. It should then be possible to acquire a better understanding of the effectiveness of a networked force in an actual combat environment. Also, there is more analysis required to determine the potential benefits of networked forces at the operational and strategic levels of war.

### **Network-Centric Warfare: The Silver Bullet?**

Now that the literature review is complete, it is possible to investigate the potential of NCW. This author has not found any proponents of NCW touting that this concept is the “Silver Bullet” to solve all the problems of future warfare. Many of the same problems that have plagued warfighters in the past exist today and will exist in the future: fog and friction, competing advances in technologies, the unpredictable nature of human behavior on the battlefield, and asymmetric warfare to name only a few. The issue isn’t the existence of these challenges to modern warfare but how one exploits the advantages of information to mitigate risk and take advantage of strengths in the force to achieve objectives.<sup>35</sup> Are the potential benefits of NCW worth the opportunity costs associated with aggressively moving forward with the implementation of this new concept?

The concept of Network Centric Warfare has already moved beyond the “bumper sticker” stage. NCW is not a fad that will go quietly into the night. There is little doubt that DOD is spending significant finite resources to pursue NCW capabilities. DOD costs in the area of military electronics, aircraft avionics, vetronics, and missile guidance, communications, electro-

optics is approaching \$99.57 billion in the 2010.<sup>36</sup> There may be changes to terminology, shifts in policy, and alterations in implementation plans. However, the core concepts that relate to leveraging the power of information will remain.

The DOD and senior military leaders have been consistent yet cautious in their support of a networked force. Former Secretary of Defense Donald Rumsfeld concisely stated the importance a fully networked force in the *Transformation Planning Guidance*. “. . . We must achieve: fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the operational environment. Realizing these capabilities will require transforming our people, processes, and military forces.”<sup>37</sup> ADM Giambastiani, former Commander U.S. Joint Forces Command stated, “A fully collaborative and networked force is an imperative, not a luxury.”<sup>38</sup> The former Commandant of the U.S. Marine Corps, General Michael Haggee said, “The capability to connect disparate units spread over the battlefield will help to provide intelligence, surveillance and reconnaissance to commanders who can then call in fire support. . . Information Technology (IT) will also be critical to Sea Basing, a key component of the Navy’s Sea Power 21 Concept.”<sup>39</sup> Vice Chief of Staff, U.S. Army Gen. Peter Chiarelli recently stated, “Access to information can mean the difference between living and dying.”<sup>40</sup> General William Wallace, USA (ret) goes on to caution that “despite the enormous benefits of using a network, it would be folly to lose sight of the fact that it is still merely a tool to aid the commander in understanding and decision-making.”<sup>41</sup> Defense Secretary Robert M. Gates wrote in his recent *Foreign Affairs* article,

We should be modest about what military force can accomplish and what technology can accomplish. The advances in precision, sensor, information, and satellite technologies have led to extraordinary gains in what the U.S. military can do. The Taliban were dispatched within three months; Saddam's regime was toppled in three weeks. A button can be pushed in Nevada, and seconds later a pickup truck will explode in Mosul. A bomb dropped from the sky can destroy a targeted house while leaving the one next to it intact. But no one should ever neglect the psychological, cultural, political, and human dimensions of warfare.<sup>42</sup>

The question is not if DOD will proceed with NCW, but how.

### **NCW Way Ahead**

The DOD has a plan for the implementation of NCW. The plan calls for a holistic approach to the implementation of NCW that investigates the potential of NCO in joint, multinational, and interagency operations. As previously discussed in this paper, there has been a significant effort to establish the theoretical underpinnings of the concept. The publication, *Implementation of Network-Centric Warfare*, establishes the outline of the plan to move forward with NCW. The Services are working to integrate information systems, sensors, and decision-making processes and technology to leverage the capabilities of a fully networked joint force. The Air Force Command and Control Constellation network is an example of the integration of C2; ISR; tankers; space, ground, and sea-based systems; and strike platforms to achieve shared awareness in the operational environment to maximize effects.<sup>43</sup> Constellation works with FORCEnet (U.S. Navy), and LandWarNet (U.S. Army) to achieve synergy on the battlefield.

It is not in the scope of this paper to examine all of the specific sub-elements of the implementation plan for NCW. However, there are several key pieces that provide a flavor for the journey ahead. It is important to remember that NCW is in fact a journey and not a particular destination. This is a dynamic process. Theories will be tested, concepts will be modified, technology will continue to advance, and budgeting priorities will shift over time. The overall path leads to a convergence of disparate sensor and command and control systems to create synergy among the numerous joint information systems. Many of the critics of NCW focus solely on the technology aspect of the concept. This is a short sighted approach to a complex transformation in thinking about warfare to leverage technology to gain a competitive advantage over potential adversaries. "Progress in implementing network-centric warfare cannot be measured solely by focusing on one dimension, such as technology or doctrine. Rather, progress must be assessed in terms of the maturity of mission capabilities, that integrate key elements of DOTMLPF (Doctrine, Organization, Training, Materiel (technology), Leadership and Education, Personnel, and Facilities)."<sup>44</sup>

A program that highlights the potential advantages of NCW is the Force XXI Battle Command Brigade and Below (FBCB2/BFT) Blue Force Tracking systems. FBCB2/BFT was used extensively during Operation Iraqi Freedom to monitor the maneuver of U.S. Army, U.S. Marine, U.S. Special Forces, and British ground forces during the conflict. FBCB2/BFT uses the global positioning system and numerous sensors to pinpoint units on the battlefield. This capability provided unprecedented situational awareness to commanders at all levels on the battlefield. The qualitative data acquired from interviews with those on the ground validates the utility of acquiring better situational awareness. Leaders from General Tommy Franks, U.S.A. (Ret) down to battalion and company commanders marveled at the ability to track unit progress during major combat operations.<sup>45</sup> The data available through FBCB2/BFT allowed commanders to quickly adjust to changing operational conditions and manage complex logistical situations.<sup>46</sup> Of course warfighters continue to use these systems in current operations in Iraq and Afghanistan.

The Global Information Grid-Bandwidth Expansion (GIG-BE) program provides the backbone to facilitate NCO now and into the future. It is difficult to discuss NCW without touching on the importance of the GIG-BE. GIG-BE is the technology that will facilitate numerous NCW initiatives in the years ahead. MG Marilyn Quaglotti, former Vice Director of the Defense Information Agency (DISA), described the vision for the GIG as a single secure Grid providing seamless end-to-end capabilities to all warfighting, national security and support users.<sup>47</sup> DISA achieved full operational capability of the GIG-BE in December 2005.<sup>48</sup>

It is essential to continue the development of the Global Information Grid (GIG)<sup>49</sup> to realize the potential benefits of NCW. The GIG provides the necessary technology to facilitate the interaction of sensors, linked to command and control, to effectively engage shooter platforms to achieve desired effects on the battlefield. The GIG will eventually provide necessary bandwidth to support requirements at all levels of warfare. The warfighters' ability to have access to necessary bandwidth with the appropriate integrated information systems across the Services, DOD, joint, and interagency communities has the potential to truly stimulate innovative approaches to solving complex tasks across the spectrum of conflict. DOD is far from achieving this lofty goal at this time. Also, there is no guarantee that as the pieces fall into place that the expectations of NCW will be achieved. However, the early indications of the potential

synergy afforded by networked forces continue to form a powerful augment to continue down this path.<sup>50</sup> “The U.S. military has deployed unmanned aircraft and other information collection devices at a pace that exceeds the capabilities of battlefield intelligence systems to archive, analyze and disseminate the video and imagery. Networks with limited bandwidth further compound the problem by slowing down data transmissions.”<sup>51</sup> There is obvious room for improvement as DOD and the Services invest large portions of their budgets to technology.

### **The Genie and NCW**

Let us postulate for a moment that this paper convinced you that the Genie representing the power of knowledge through collaboration enabled by a robust network (information system) characterized by the latest information technology is outside the bottle. The challenge is to ask for the correct wishes that would facilitate achieving the principles and tenets outlined in the NCO-CF. There are numerous potential disadvantages to NCW. One could easily ask the Genie for a worthless wish. There is a fairly substantial list of those who point out the shortcomings of NCW.<sup>52</sup> These authors provide a valuable service to highlight the potential deficiencies in the theoretical underpinnings of NCW as well as outlining the opportunity costs associated with pursuing this extremely expensive transformation of the defense information architecture. The naysayers stimulate dialogue and debate and assist proponents and decision makers to better allocate scarce resources in pursuit of NCW capabilities.

The disadvantages of NCW are well documented in the literature. Numerous scholars and warfighters have taken the time to thoughtfully outline the potential pitfalls in the pursuit of NCW capabilities. It would be impossible to enumerate all of the explicit and implicit disadvantages outlined by the critics. However, it is useful to highlight a few of the major concerns that deserve further attention and study in the years ahead:

- NCW places too much emphasis on tactics and the tactical nature of war.
- U.S. advances in information technology will outpace our allies and potential coalition partners ability to operate together on the battlefield.
- More information and superior information technologies do not translate into information dominance.
- Situational awareness is not going to eliminate the fog and friction of war.
- Too much speed of command can lead to unsound decisions.<sup>53</sup>
- NCW ignores the human dimension of warfare.
- Technology is dictating strategy. “[NCW] driven by its self-centered concern with technology for technology sake.”<sup>54</sup>
- NCW and its reliance on information technology fails to address the emergence of the current and future threat posed by insurgency, terrorists, Netwars, and 4<sup>th</sup> Generation Warfare.<sup>55</sup>

The articulated disadvantages help to focus research, funding, and execution of NCW in the years ahead. DOD will address many of these possible negative aspects of NCW with future investments based on years of lessons learned during a period of persistent conflict.

The proponents of NCW recognize these potential negative aspects of NCW. DOD is working to harness the power of industry, academia, and the military community at large to thoughtfully address each of these concerns with rigorous conceptual and empirical study. COL Douglas Macgregor, USA (Ret.), a well known critic of numerous aspects of Army transformation, understands the potential benefits of technology and acquiring information on the battlefield. "In the pursuit of knowledge, the U.S. Navy has broken new ground in context of network-centric warfare with its cooperative engagement capability (CEC). This system distributes raw sensor and weapons data among warfighting units, enabling them to combine and share composite data in a coordinated joint defense."<sup>56</sup> This is why it is critical to proceed with the study and focused conceptualization of how technology can enable and facilitate warfighting in the 21<sup>st</sup> century.

### **Moving Forward: Course of Action Missouri**

It should be apparent by now that this author is an advocate of NCW. This should not imply total agreement with the concept. This author supports the continued study of how the principles of NCW will leverage information and knowledge on the battlefield. It is understandable that the academic community and even warfighters want to see solid evidence supporting the need to make large investments of scarce funding to pursue NCW capabilities. Thus, there is a requirement to develop a strategy and course of action that clearly demonstrates the return on investment to stakeholders, i.e., *Course of Action (COA) Missouri*. The designation of COA Missouri was selected based on the state of Missouri's nickname of the "show me state." NCW will need to clearly demonstrate value added to the warfighter. Elements of this proposed course of action are already beginning to take shape in the Office of Force Transformation. The empirical evidence and future studies begin to outline the potential of aligning the appropriate technology to support joint warfighting in a collaborative information environment. So what are the key elements of COA Missouri?

### **The Human Dimension of Warfare**

As previously discussed, many of the critics state that NCW does not appropriately address human behavior in warfare. The NCW literature does address the importance of the interaction of the cognitive, social, and information domains as an essential element of NCW. To address this concern DOD should focus future research and publications on the human dimension and leadership issues associated with information age warfare. There is adequate coverage in the current literature to indicate that the warfighter on the battlefield is and will remain the key to success and not the technology. However, published case studies focus mainly on the enabling technology related to organizational effectiveness. Future studies should examine the effects of technology on human behavior in a combat environment at the tactical, operational, and strategic levels of warfare. Academic scholars in the fields of anthropology, sociology, and psychology should work with the developers of the NCO-CF to investigate the potential benefits as well as the negative aspects of NCW in the human behavior domain. Transformation chairs at all of the Senior Service Colleges and Service Academies could be the catalyst to reinvigorate an

examination of the human dimension in a network-centric environment. These scholars could sponsor studies investigating human behavior and leadership challenges to warfare in the information age. The results of this work should be published and disseminated for scholarly examination, critique, and additional study.

### **NCO-CF Attributes and Metrics**

There is little doubt the developers of the NCO-CF are in the early stages of defining rigorous attributes and associated metrics to conduct empirical studies of the model. Two of the NCW published case studies have stated that attributes and metrics must be further defined.<sup>57</sup> The US/UK case study on NCO highlighted several insightful observations and recommendations about the NCO-CF:

- The language of the NCO-CF be changed so it is better understood by combat units and non-US forces.
- Quantifying metrics related to combat operations—as was done for this case study—can be very difficult. Beyond this report, it is recommended that a focused effort be made to incorporate into the NCO-CF recommendations for improvement and lessons learned from the application of NCO-CF within various case studies.
- Certain definitions and corresponding metrics difficult to translate into meaningful interview questions.
- Many attributes definitions and metrics are liable to variations in interpretation.
- Difficult to identify data sources.
- Weakness in consistency and completeness in descriptions, explanations, measures and metrics for each of the attributes.<sup>58</sup>
- The Stryker BCT NCW Case Study called for the development of additional metrics:
  - Develop metrics that reflect the degree to which the development, maintenance, and sharing of the Common Operational Picture critically depends on the interaction of technology, training and personnel experience.
  - Current metrics don't measure the synergy between net-centric current operations and improved planning in land warfare.
  - Metrics don't exist that reflect the degree to which the Military Decision Making Process (MDMP) has been properly reengineered to exploit the potential advantages of information networks.
  - Metrics are required to reflect the degree to which process design, technology, business rules, training, personnel experience and other factors combine to either enhance or impede effective and efficient collaboration.<sup>59</sup>

These observations highlight the requirement to conduct focused research to develop appropriate new attributes and metrics based on lessons learned in previous studies. This study could provide new insights and directions to develop the appropriate NCW capabilities. There has been a lack of focused scholarly study of the NCO-CF for several years. The NCO-CF is an adequate point of departure to investigate the real value added of NCW in the operational environment.

### **Convergence of Services' Information Systems**

A further defined NCO-CF with appropriate attributes and metrics will assist in selecting the correct enabling technologies. Information technology and systems will remain the cornerstone of the enabling technologies to create the competitive advantage against U.S. adversaries in the future. Currently, there is a proliferation of waveforms, software, and hardware dispersed throughout the current DOD information system. There should be little doubt that the "to be" DOD information system supporting NCW was based on the convergence and interoperability of the enterprise architecture. Voice, video, and data communications must be seamlessly shared between the services in an interoperable information system. This is the essence of transformational communications.<sup>60</sup>

The GIG became fully operational in December 2005 providing the backbone for a DOD information system to support Joint communications and enable NCW. The Services must continue to fund initiatives to integrate and upgrade their information systems. FORCEnet (U.S. Navy), Constellation C2 (U.S. Air Force), and LandWarNet (U.S. Army) have the potential to move toward an interoperable Joint communications network supported by the GIG. "Operationally, the foundation of transformational communications rests on four primary supports: the Transformational Satellite Communications System, or TSAT; the Global Information Grid Bandwidth Expansion, or GIG-BE; and the Warfighter Information Network Tactical system, or WIN-T; and the Joint Tactical Radio System, or JTRS."<sup>61</sup> The JTRS initiative provides the promise of a joint communications system that will support information sharing between the Services. The integration and convergence of Services' information systems and the abundance of disparate waveforms must remain a high priority. Many of these programs continue to morph or are in danger of extinction through the annual budget cycle (e.g., TSAT<sup>62</sup>).

Another critical link in the Services' information networks is Unmanned Aircraft Systems. There has been an explosion of Unmanned Aircraft Systems (UAS) to enhance situational awareness and conduct precision strike.

The Department of Defense's (DOD) use of unmanned aircraft systems (UAS) continues to increase. In 2000, DOD components had fewer than 50 unmanned aircraft in their inventory. By May 2008, they had more than 6,000. However, DOD faces challenges, such as UAS acquisition and the integration of UAS into joint combat operations.<sup>63</sup>

There should be little doubt that Unmanned Aircraft Systems add value to gaining situational awareness and executing precision strike missions.<sup>64</sup> This is another extremely visible example of NCW in 21<sup>st</sup> warfighting.

## **Network-Centric Warfare: Proceed with Caution**

This paper has demonstrated that NCW is much more than developing an integrated DOD information system on steroids. NCW is more than just technology. NCW is about harnessing the power of information in the operational environment. In order to argue the merits of NCW as more than just information technology it is essential to review the body of literature that supports the fundamental underpinnings of the concept. This paper has provided a brief literature review of the key documents to bring the dialogue on the merits of NCW up to date. NCW is still an emerging concept yet to be fully developed and validated. The term “Network Centric Warfare” doesn’t appear as prominent in the literature or in the news as in years past. The concept is still alive and well. The published NCW case studies only begin to illustrate the potential of leveraging information and knowledge on the battlefield. Clearly, scholars will need to examine the convergence of cyber warfare and NCW in the future. “Perhaps the best defining marker is that cyberspace is about networking, the two-way transfer of information, in contrast to broadcasting, in which information is transferred only one way. Networking appears to be the essence of cyberspace...”<sup>65</sup> There is still much work to be done to demonstrate benefits of NCW at the operational and strategic levels of war and the implications of cyber warfare.

DOD should continue to aggressively pursue case studies that investigate the relationships in the NCO-CF that deal with the human dimension of warfare. Gather data emerging from current operations in Iraq and Afghanistan to advance the investigation of the implications of a fully networked Joint force. The interaction between the information, cognitive, physical domains enabled by appropriate technologies should be a priority. There should be collaboration between scholars in the fields of psychology, sociology, and anthropology to examine the implications of NCO on human behavior and leadership. Next, this essay has provided ample evidence that it is time to reexamine the attributes and metrics associated with the NCO-CF. Finally, the Services and DOD must continue to work the “network” in terms of interoperability and convergence of unique applications, waveforms, and information technologies. A clearly articulated action plan for NCW that includes these recommendations will continue to move NCW in the right direction to harness the power of information on the battlefield to support the warfighter.

---

<sup>1</sup> Carl Von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton University Press, 1984), 140.

<sup>2</sup> David S. Alberts, John Garstka, J., and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C.: DoD Command and Control Research Program, 2002); Thomas P. M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *Proceedings: U.S. Naval Institute* 125 (1999); Arthur K. Cebrowski, "Transformation and the Changing Character of War", Office of the Secretary of Defense, Office of Force Transformation <http://www.afei.org/transformation/documents/TransformationTrends-17June2004Issue.pdf> (accessed September 7 2004); Milan Vego, "Net-Centric Is Not Decisive," *Naval Institute Proceedings* 129, no. 1 (2003).

<sup>3</sup> Vice Admiral Robert S. Harward, deputy commander of US Joint Forces Command stated "the computerized C4ISR system should now be considered leader-centric instead of network-centric." See Gerry J. Gilmore, "Admiral Cites Need to Prepare for All Threats," *American forces press service* (2009). <http://www.defenselink.mil/news/newsarticle.aspx?id=5691> [accessed October 19]. General James Mattis, commander US Joint Forces Command stated, "A leader-centric, networked-enabled approach creates unity of effort if done right and creates harmony in the fog and friction of war." See Barry Rosenber, "Command and Control Advances to New Stage," *DefenseSytems*, September 2009.

<sup>4</sup> T Stewart, *The Wealth of Knowledge* (New York, NY: Currency, 2001).

<sup>5</sup> See Leslie C. Eliason and Emily O. Goldman, "Introduction: Theoretical and Comparative Perspectives on Innovation and Diffusion," in *The Diffusion of Military Technology and Ideas*, ed. Leslie C. Eliason and Emily O. Goldman (Stanford, CA: Stanford University Press, 2003).

<sup>6</sup> See Groh, Jeffrey L., and Dennis Murphy. "Landpower and Network-Centric Operations: How Information in Today's Battlespace Can Be Exploited." *Network Enabled Capabilities/Network-centric Warfare Journal* (2006), and Tisserand, Jay B. "U.S. V Corps and 3rd Infantry Division (Mechanized) During Operation Iraqi Freedom Combat Operations (Mar-Apr 2003) Volume III: Network Centric Warfare Insights." Carlisle Barracks, PA: Center for Strategic Leadership and Office of Force Transformation, Office of the Secretary of Defense, 2006.

<sup>7</sup> Nicholas G. Carr, *Does IT Matter?* (Boston, MA: Harvard Business School Press, 2004); Gartner Dataquest, "Update: It Spending" [http://www.dataquest.com/press\\_gartner/quickstats/ITSpending.html](http://www.dataquest.com/press_gartner/quickstats/ITSpending.html) (accessed 13 August 2003).

<sup>8</sup> Director Force Transformation Office of the Secretary of Defense, "The Implementation of Network-Centric Warfare," (2005). [http://www.oft.osd.mil/library/library\\_files/document\\_387\\_NCW\\_Book\\_LowRes.pdf](http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf) [accessed 5 January].

<sup>9</sup> Command and Control Research Program, "About the Program", Command and Control Research Program, Office of the Secretary of Defense [http://www.dodccrp.org/html2/about\\_program.html](http://www.dodccrp.org/html2/about_program.html) (accessed September 5 2005). "The Command and Control Research Program (CCRP) within the Office of the Assistant Secretary of Defense (NII) focuses upon 1) improving both the state of the art and the state of the practice of command and control and 2) enhancing DoD's understanding of the national security implications of the Information Age. It provides "Out of the Box" thinking and explores ways to help DoD take full advantage of the opportunities afforded by the Information Age. The CCRP forges links between the operational and technical communities, and enhances the body of knowledge and research infrastructure upon which future progress depends."

<sup>10</sup> Alberts, Garstka, and Stein.

<sup>11</sup> Ibid.

<sup>12</sup> Arthur K. Cebrowski and John Garstka, J., "Network Centric Warfare: Its Origins and Future " *Proceedings: U.S. Naval Institute* 124, no. 1 (1998). in Alberts, Garstka, and Stein.

<sup>13</sup> David S. Alberts, *Information Age Transformation: Getting to a 21st Century Military* (Washington, D.C.: Department of Defense Command and Control Research Program, 2002), 43.

<sup>14</sup> Ibid.

<sup>15</sup> Director Force Transformation Office of the Secretary of Defense, "Network Centric Operations Case Studies", Office of the Secretary of Defense, Office of Force Transformation <http://www.oft.osd.mil/initiatives/ncw/studies.cfm> (accessed September 6 2005).

<sup>16</sup> David S. Alberts and Richard E. Hayes, *Power to the Edge : Command, Control in the Information Age*, Information Age Transformation Series (Washington, DC: CCRP Publication Series, 2003).

<sup>17</sup> Ibid., 5.

<sup>18</sup> C-SPAN, "Military Restructuring Efforts [Videorecording]/National Defense University," in *C-SPAN Archives* (USA: 2002).

<sup>19</sup> John Garstka, J., "Defense Transformation and Network Centric Warfare", Office of the Secretary of Defense, Office of Force Transformation <http://navyleague.org/membership/NCW.pdf> (accessed September 2 2005).

<sup>20</sup> Noah Shachtman, "How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social-Not Electronic," *Wired Magazine*, no. 15.12 (2007). [http://www.wired.com/politics/security/magazine/15-12/ff\\_futurewar](http://www.wired.com/politics/security/magazine/15-12/ff_futurewar) [accessed November 27].

<sup>21</sup> John Garstka, J. and David S. Alberts, *Network Centric Operations Conceptual Framework Version 2.0* (Vienna, VA: Evidence Based Research, Inc, 2004), 2.

<sup>22</sup> Ibid., 20.

<sup>23</sup> Ibid., 59.

<sup>24</sup> Daniel Gonzales and others, *Network-Centric Operations Case Study: The Stryker Brigade Combat Team* (Santa Monica, CA: Rand, 2005).

<sup>25</sup> David Mawby, Ian McDougall, and Greg Boehmer, *A Network-Centric Operations Case Study: US/UK Coalition Combat Operations During Operation Iraqi Freedom* (Washington, D.C.: Evidence Based Research, Inc and PA Consulting (UK), , 2005), Case study.

<sup>26</sup> Director Force Transformation Office of the Secretary of Defense, "The Implementation of Network-Centric Warfare."

<sup>27</sup> Ibid.

<sup>28</sup> See for example, Edmund Blash, "Network-Centric Warfare Requires a Closer Look," *Signal Magazine*, May 2003; Robert H. Scales, "Human Intel Vs. Technology," *Washington Times* 2004; Vego. See also, Rosennberg. General Mattis stated, "The military force that is most reliant on technology and network systems is also the most vulnerable..."

<sup>29</sup> Director Force Transformation Office of the Secretary of Defense, "The Implementation of Network-Centric Warfare."

<sup>30</sup> Ibid.

<sup>31</sup> Ibid.

<sup>32</sup> Ibid.

<sup>33</sup> Ibid.

<sup>34</sup> Gonzales and others.

<sup>35</sup> Director Force Transformation Office of the Secretary of Defense, "The Implementation of Network-Centric Warfare."

<sup>36</sup> John Keller, "DOD Budget for 2010 Proposes \$23.67 Billion for Military Communications, Electronics, and Intelligence," *Military & Aerospace Electronics* (2009).  
[http://mae.pennnet.com/display\\_article/362816/32/ARTCL/none/EXECW/1/DOD-budget-for-2010-proposes-\\$2367-billion-for-military-communications,-electronics,-and-intelligence/](http://mae.pennnet.com/display_article/362816/32/ARTCL/none/EXECW/1/DOD-budget-for-2010-proposes-$2367-billion-for-military-communications,-electronics,-and-intelligence/) [accessed November 27 2009].

<sup>37</sup> Director Force Transformation Office of the Secretary of Defense, "The Implementation of Network-Centric Warfare."

<sup>38</sup> Anonymous, "Giambastiani: Networked Force Is "Not a Luxury"", *Defense News*  
<http://www.defensenews.com/story.php?F=740965&C=america> (accessed April 5 2005).

<sup>39</sup> Geoff Fein, "Info Sharing We Be Vital in Future Combat Operations, Hagee Says," *Defense Daily*, March 31 2005.

<sup>40</sup> Barry Rosenberg, "Cookie-Cutter Security Hinders Warfighters," *DefenseSystems*, September 2009.

<sup>41</sup> William S. Wallace, "Network-Enabled Battle Command," *Military Review* LXXXV, no. 3 (2005).

<sup>42</sup> Robert M. Gates, "A Balance Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs* 88, no. 1 (2009).

<sup>43</sup> Director Force Transformation Office of the Secretary of Defense, "The Implementation of Network-Centric Warfare."

<sup>44</sup> Ibid.

<sup>45</sup> Tommy Franks, "Impact of the Network on Operation Iraqi Freedom," in *Network Centric Warfare 2004* (Washington, D.C.: IDG, 2004); Nick Justice, "Situational Awareness in OEF/OIF Via FBCB 2-Blue Force Tracker," in *Network Centric Warfare Conference* (Washington, D.C.: IDG, 2004).

<sup>46</sup> Jay B. Tisserand, *U.S. V Corps and 3rd Infantry Division (Mechanized) During Operation Iraqi Freedom Combat Operations (Mar-Apr 2003) Volume III: Network Centric Warfare Insights* (Carlisle Barracks, PA: Center for Strategic Leadership and Office of Force Transformation, Office of the Secretary of Defense, 2006).

<sup>47</sup> Marilyn Quagliotti, "Moving to a Net-Centric Environment," in *Network Centric Warfare 2005* (Washington, D.C.: IDG, 2005).

---

<sup>48</sup> Jason miller, "DOD's GIG-BE Reaches Full Operational Capability ", Government Computer Network [http://www.gcn.com/online/vol1\\_no1/37848-1.html](http://www.gcn.com/online/vol1_no1/37848-1.html) (accessed August 9 2007).

<sup>49</sup> Defense Information Systems Agency, "GIG Operations (GO)", DISA <http://www.disa.mil/news/pressresources/factsheets/go.html> (accessed November 2009).

<sup>50</sup> ADM Cebrowski, USN, Ret., stated in an interview, "We have a mountain of evidence now, ranging from simulations, to experimentation, to real world combat experiences, that verify the power of networking." See Anonymous, "The Power of Information Comes from the Ability to Share," *Defender*, April 29 2005. This study has already commented on the impressive results of the *Network-Centric Operations Case Study: The Stryker Brigade Combat Team* conducted by Rand. Also, there are seven case studies being published by the Office of Force Transformation that will further document the potential of NCO. The Center for Strategic Leadership, U.S. Army War College is completing a case study that examines network centric operations involving V Corps and 3 Infantry Division during Operation Iraqi Freedom. The initial findings indicate, "New information systems, sensors, and extended connectivity improved combat effectiveness. This extended connectivity allowed V Corps and 3 ID to both fight widely dispersed over extended distances and rapidly task organize and fully integrate newly arrived units into combat operations..." See Murphy, Dennis. 2005. *Network Enabled Operations in Operation Iraqi Freedom: Initial Impressions*. In, Center for Strategic Leadership, U.S. Army War College, <http://www.carlisle.army.mil/usacsl/Publications/06-05.pdf>. (accessed May 9, 2005).

<sup>51</sup> Grace V. Jean, "Battlefield Intelligence: Easy to Collect, Tough to Share," *National Defense*, November 2009.

<sup>52</sup> See for example: Barnett, Thomas P. M. "The Seven Deadly Sins of Network-Centric Warfare." *Proceedings: U.S. Naval Institute* 125 (1999): 36-39; Blash, Edmund. "Network-Centric Warfare Requires a Closer Look." *Signal Magazine*, May 2003, 56-57; Hammes, Thomas X. *The Sling and the Stone: On War in the 21<sup>st</sup> Century*. St. Paul, MN: Zenith Press, 2004; Kaufman, Alfred. "Caught in the Network: How the Doctrine of Network-Centric Warfare Allows Technology to Dictate Military Strategy." *Armed Forces Journal*, February 2005, 20-22; and Vego, Milan, "Net-Centric is Not Decisive." *Naval Institute Proceedings* 129, no. 1 (2003): 52-58, and Kagan, Frederick W. *Finding the Target: The Transformation of American Military Policy*. 1st ed. New York: Encounter Books, 2006.

<sup>53</sup> See Vego. The first five bullets paraphrase Dr. Vego's concerns about NCW.

<sup>54</sup> Alfred Kaufman, "Caught in the Network: How the Doctrine of Network-Centric Warfare Allows Technology to Dictate Military Strategy," *Armed Forces Journal*, February 2005.

<sup>55</sup> Thomas X. Hammes, *The Sling and the Stone : On War in the 21st Century* (St. Paul, MN: Zenith Press, 2004).

<sup>56</sup> Douglas A. Macgregor, *Transformation under Fire: Revolutionizing How America Fights* (Westport, Connecticut: Praeger, 2003), 257.

<sup>57</sup> Gonzales and others; Mawby, McDougall, and Boehmer.

<sup>58</sup> Mawby, McDougall, and Boehmer, Appendix G.

<sup>59</sup> Gonzales and others, 109-111.

<sup>60</sup> John Keller, "Transformational Communications," *Military & Aerospace Electronics*, May 2005.

<sup>61</sup> *Ibid.*, 28.

<sup>62</sup> "The latest developments revolve around the end of the program. Despite a positive recent report from the GAO, key components of TMOS/TSAT are being canceled outright as part of the program's planned termination..." see Defense Industry Daily, "Special Report: The USA's Transformational Communications Satellite System (TSAT)"

---

<http://www.defenseindustrydaily.com/special-report-the-usas-transformational-communications-satellite-system-tsatsat-0866/> (accessed November 28 2009).

<sup>63</sup> Government Accounting Office, *Unmanned Aircraft Systems: Additional Actions Needed to Improve Management and Integration of DOD Efforts to Support Warfighter Needs*, GAO-09-175 Cong., 2008.

<sup>64</sup> Nic Robertson, "How Robot Drones Revolutionized the Face of Warfare", CNN  
<http://www.cnn.com/2009/WORLD/americas/07/23/wus.warfare.remote.uav/> (accessed November 28 2009).

<sup>65</sup> Martin C. Libicki, "Military Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington D.C.: National Defense University Press, 2009)., 276.