REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 04-05-2012	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)* Feb - May 2012

4. TITLE AND SUBTITLE

From Fog to Friction: The Impact of
Network-Enabled Command and Control
on Operational Leadership

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Guy M. Snodgrass, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

14. ABSTRACT

Leaders have historically grappled with the "fog of war," continually seeking ways to gain access to battlefield information deemed relevant for timely decision-making. This problem was exacerbated when leaders were forced to remove themselves from the battlefield, requiring advancements in technology to overcome operational factors of both time and space. Advances in information technology since World War I have largely conquered the problem of providing operational and strategic leaders access to the battlefield, though doing so has created additional vulnerabilities in command structure and command and control through increasing centralization and a reliance on communications systems.

15. SUBJECT TERMS

General/Flag Officers; Iraq; Afghanistan; Kosovo; Information Technology; Leadership; Network-enabled Command and Control (NEC2); Levels of War

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Department
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	24	**19b. TELEPONE NUMBER (*Include area code)*** 401-841-3414

NAVAL WAR COLLEGE
Newport, RI

From Fog to Friction: The Influence of Network-Enabled Command and Control on Operational Leadership

by

Guy M. Snodgrass

Lieutenant Commander, United States Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy

Signature: ____________________________

4 May 2012

Table of Contents

Abstract

Leaders have historically grappled with the “fog of war,” continually seeking ways to gain access to battlefield information deemed relevant for timely decision-making. This problem was exacerbated when leaders were forced to remove themselves from the battlefield, requiring advancements in technology to overcome operational factors of both time and space. Advances in information technology since World War I have largely conquered the problem of providing operational and strategic leaders access to the battlefield, though doing so has created additional vulnerabilities in command structure and command and control through increasing centralization and a reliance on communications systems. With the war in Iraq recently concluded and the one in Afghanistan expected to draw to a close soon, the military should reinvest time to evaluate how leaders interact with and rely on information technology systems, preparing future operational leaders for success.

"At the highest levels, the combination of networking and real-time information sources [has] fostered an odd mixture of disengagement and micromanagement."

-- Dr. Thomas Mahnken[1]

"An ability to embrace new ideas, routinely challenge old ones, and live with paradox will be the effective leaders premier trait."

- Tom Peters

As Commander of U.S. Central Command during Operation Enduring Freedom, General Tommy Franks oversaw the first widespread employment of unmanned aerial vehicles (UAVs) by the United States.[2] In his memoir *American Soldier*, Gen. Franks recalls how he spent hours in his Tampa headquarters watching data from a MQ-1 Predator in Afghanistan as it broadcast real-time video of insurgents in a sport-utility vehicle. Sensing an opportunity, General Franks personally coordinated for two orbiting F/A-18 Hornet aircraft to employ 500-pound bombs on the target.[3]

This strike demonstrates just how far the United States has advanced in its incorporation of network-enabled command and control systems (NEC2).[4] NEC2 has continued to evolve since Operation Enduring Freedom, resulting in newer networked weapons, enhanced tracking systems for friendly forces, and a multitude of UAV and unmanned combat aerial vehicle (UCAV) variants. These networked capabilities serve as vital communication links, affording American operational commanders unprecedented access to the battlefield.

The widespread adoption of NEC2 across all services has also created unintended consequences that affect military operations. NEC2 has facilitated the creation of a "Tactical

[1] Thomas G. Mahnken, *Technology and the American Way of War Since 1945*, (New York: Columbia University Press, 2008), 202.
[2] Ibid.
[3] Tommy Franks, *American Soldier* (New York: Harper Collins, 2004), 290-96.
[4] Ryan McCaskill, *Network-Enabled and Leader-Centeric Command and Control (C2): The Dangers of Digital Decision Making*, JMO Research Paper, Naval War College, 2011, 2.

General," enabling operational leaders to operate from command posts that have shifted rearward with each advance in technology, while simultaneously empowering their involvement in tactical execution.[5,6] The volume and speed of information provided via networked systems can adversely impact the decision-making of operational commanders, affecting their ability to manage the operational level of war. An increasing reliance on NEC2 has similarly created communication vulnerabilities that place the military at risk in future conflicts, especially against an adversary focused on command and control warfare (C2W). The increased dependence on NEC2 by the United States military has resulted in significant vulnerabilities to doctrinal command and control structures, endangering success in future wars.

Background

NEC2 represents the culmination of decades of command and control (C2) system development, enabling leaders to more directly interact with and influence the battlefield.[7] A multitude of intelligence collection systems, data processing nodes, communication relays, and tactical operations centers operate nonstop to disseminate information rapidly throughout the entire chain of command. NEC2, as envisioned by the *Department of Defense C2 Implementation Plan (2009),* is intended to "leverage emerging network technologies to enhance a commander's ability to make faster and more well-informed decisions."[8,9] United States joint doctrine states that "joint C2 must enable commanders to decentralize command and

[5] P.W. Singer, "Tactical Generals: Leaders, Technology, and the Perils of Battlefield Micromanagement," *Air & Space Power Journal*, Vol 23, No 2, Summer 2009, 1.

[6] Ibid., 3.

[7] "NEC2" is a DoD concept designed to provide leaders greater networked access to information, in order to merge the "art of war (humans) with the science of war (technology)." NEC2 includes systems that provide a Common Operating Picture (COP.) U.S. Department of Defense, *Command and Control Implementation Plan, Version 1.0* (Washington, D.C.: Networks and Information Integrations, 2009), 5.

[8] McCaskill, 2.

[9] *Command and Control Version 1.0*, 5.

control, encourage initiative in lower echelons, and quickly respond to changes in the operational environment."[10]

Effective battlefield communication between a leader and his forces has been a prerequisite for victory since the earliest days of warfare. A leader may display the very essence of *coup d'oeil* and develop the perfect battle plan, but the inability to transmit that plan to his superiors (for alignment) and subordinates (for execution) risks failure. Joint Pub 6-0, "*Joint Communications System*," states that two key elements are required for communication. The first element is comprised of people, who "acquire information, make decisions, take action, communicate, and collaborate with one another to accomplish a common goal."[11] The second element is the physical construct: the equipment and procedures necessary to enable the process of communication.[12] Only by leveraging both elements can communication prove successful.

Historically, heads of state also served as their nation's military leaders, leading armies onto the field of battle to provide direction to tactical units for the achievement of strategic ends. Over time, rulers were forced to return home and attend to the domestic affairs of their kingdoms, relinquishing their role on the battlefield and effectively creating the earliest vestiges of an operational level of war, necessitating a means by which tactical actions could be linked to strategic ends.[13] The departure of strategic leaders from the field of battle created two requirements: an operational level of war (and corresponding leaders), and a way for strategic leaders to communicate with the battlefield. This requirement to

[10] U.S. Department of Defense, *Command and Control Joint Integrating Concept Final Version 1.0* (Washington DC: Pentagon, 2005), 12.

[11] Joint Publication 6-0, "Joint Communications Systems" (Washington, D.C.: Joint Chiefs of Staff, 2010), ix.

[12] Ibid., ix.

[13] Vego, Milan N. *Joint Operational Warfare.* (Newport, RI: Naval War College Press, 2007), I-16.

establish communication with the battlefield represents the first major driver for the development of communication systems to coordinate operations.

Communications technology has changed dramatically over the course of the past 230 years. Sending a message from Britain to America during the American Revolution took eight weeks and the situation in theater was likely to change by the time orders reached the battlefield and updates could be returned.[14] Transitioning to railways and steamships reduced transit time, but the speed of communication was still inhibited by the physical medium in which it traveled. Subsequent introduction of the telegraph and radio rapidly transformed the ability of operational commanders to exercise command and control from remote locations. Admiral Chester Nimitz, Commander in Chief of the Pacific Fleet during WWII, could radio messages to his group and tactical commanders at sea, providing near-instantaneous guidance.[15] Likewise, Nimitz could monitor incoming reports to build an accurate operational picture. Communication was now limited by the speed of light, not the distance to be traversed.

Whereas leaders and their decisions were previously restricted by the speed of communications, throughput now serves as the limiting factor when sending and receiving information.[16] Frequent improvements to communications technology have continued to increase the size of an operational commander's area of operations, while simultaneously decreasing the time required for making decisions. Operational commanders are no longer beholden to a communication technology that dictates the pace of operations, but rather their

[14] John A. Tokar, "Logistics and British Defeat in the Revolutionary War," *Army Logistician*, Vol. 31, Issue 5, Sep-Oct 1999.

[15] Elmer B. Potter. *Nimitz* (Annapolis: U.S. Naval Institute Press, 1976), 38.

[16] Throughput, as used here, is analogous to the term 'digital bandwidth capacity,' and is referring to the average rate of successful data delivery over a specified about of time. Electronic data travels at the speed of light, and is therefore limited not by speed, but by the amount of information that can processed and transmitted due to processing limitations.

own ability to interpret information and execute rapid decision-making through the use of an "OODA-loop" cycle.[17]

Counter-Argument

Operation Desert Storm in 1991 signaled a change in the way the military conducts operations. No longer constrained by limitations in communications technology, operational commanders started using information technology and greater battlefield awareness to increasingly affect direct control over tactical decisions.[18] The Gulf War demonstrated an incredible mismatch in the information superiority of U.S.-led coalition forces and those of Iraq, leading many to believe that a revolution in military affairs (RMA) was underway.[19] Systems like the Predator UAV, boasting a multitude of onboard sensors and a precision targeting capability, can provide persistent surveillance of a target area.[20] Coupled with precision strike capabilities, information superiority through networked information systems resulted in a nearly unprecedented capability for U.S. commanders to gather information, make decisions, and produce definitive results, ultimately reducing the targeting cycle.

Increased reliance on NEC2 can enable faster reporting of battlespace situational awareness up the chain of command, drastically improving the operational commander's decision-making cycle. NEC2 has been shown to substantially increase mission effectiveness and increase the operational commander's ability to achieve objectives during

[17] The process of observing, orienting, deciding, and acting championed by Colonel John Boyd, USAF. This combat operations process emphasizes speed in carrying out the four tenets, in order to out-pace your adversary. Doing so leads to an ability to seize the initiative and gain the advantage.

[18] *Merriam-Webster Dictionary,* s.v. "information technology." Information technology is defined as "the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data."

[19] Mahnken, 157.

[20] Mahnken, 182.

Operations Iraqi Freedom (OIF) and Enduring Freedom (OEF).[21] The fusing of data from multiple services into a common operating picture (COP) provides the operational commander the ability to coordinate and manage a truly joint force. During OIF, ground forces under attack had their position plotted real-time, providing geo-spatial awareness to commanders and allowing for the coordination of UAV or manned aircraft to interdict hostile forces. NEC2 allows for greater flexibility within the force, as well as for greater dispersal of military assets. In recognition of the operational-level successes of NEC2, this capability is rapidly becoming available at the tactical level, through new initiatives like the Force XXI Battle Command, Brigade and Below (FBCB2) system. The U.S. Army even created a program called "Every Soldier is a Sensor" (ES2) in 2004, leveraging NEC2 concepts to allow the real-time reporting of intelligence information from individual soldiers.[22]

Information technology, and more specifically NEC2, has the potential to enable greater control of forces through the real-time reporting of unit position and status. Leaders should be careful to draw the correct conclusions, however, as many recent evaluations of wartime NEC2 use were authored years into the conflicts. This "after the fact" look at NEC2 risks overstating capabilities, especially now that the military has operated in the same theater for nearly a decade. More importantly, the recent conflicts have been fought against technologically inferior adversaries that were unable to oppose U.S. information dominance, an advantage that might be lost in future conflicts. Despite NEC2's strengths, there are several shortcomings that should be addressed.

[21] Thomas McNaughter, "The Real Meaning of Military Transformation: Rethinking the Revolution," *Foreign Affairs*, January/February 2007.

[22] U.S. Department of the Army. "ES2: Every Soldier is a Sensor," *Association of the United States Army Discussion Paper*, No. 5, August 2004.

The Centralization of Operations

While NEC2 can provide a data-rich resource for leaders to exploit, the ability to link operational commanders directly with tactical units can result in increased control, negating the benefits of decentralized execution. Military doctrine in the United States continues to emphasize a C2 structure that reinforces the concept of centralized direction and decentralized execution.[23] Kolenda argues that "empowerment of professionals at the lowest possible levels is the most effective guarantor of excellence…creating a certain complex order that no central authority could conceive or direct."[24] In particular, centralization creates three concerns that warrant further examination.

First, the time an operational commander spends executing events at the tactical level is time no longer available for the management of a campaign or major operation. The hours spent by General Franks in executing tactical control of a Predator UAV and F/A-18 Hornet aircraft illustrates centralized execution and demonstrates this problem. Often referred to as the "5,000-mile long screwdriver," centralized execution can create confusion in subordinate units.[25] In one example, a battalion commander in Iraq had a four-star and two three-star generals telling him where to place his units during a battle. In another, a captain operating with special operations forces had a brigadier general call to direct the placement of individual soldiers after watching video feed of an insurgent escape during a raid.[26] These incursions by senior leaders can result in friction and confusion at lower levels of command, effectively flattening the strategic, operational, and tactical levels of war.[27]

[23] Vego, VIII-8.
[24] Kolenda, 109.
[25] Barry Rosenberg, "Technology and Leadership," *Armed Forces Journal*, http://www.armedforcesjournal.com/2007/07/2786772/. Retrieved April 27, 2012.
[26] Singer, 3.
[27] Douglas MacGregor, "Future Battle: The Merging Levels of War," *Parameters* (Carlisle: U.S. Army War College, Winter 1992-93), 33.

The operational level of warfare is, by design, broad in scope and represents the level most closely attributed with the attainment of theater objectives.[28] Leaders at the operational level should ensure that appropriate theater and major operational objectives are set and achieved through the evaluation of rational courses of action, something that becomes increasingly difficult when dedicating substantial amount of time to the tactical picture.[29] Conversely, the tactical level of warfare is primarily concerned with the accomplishment of unit-level tasks, the cumulative effect of which should ultimately lead to the attainment of operational-level objectives.[30] The time required to make decisions at the tactical level precludes the exhaustive examination of alternatives and requires an intuitive recognition of the local situation, something that the operational commander rarely enjoys.[31,32] Sustained operations in Afghanistan and Iraq have proven to have a relatively low operational tempo. This, coupled with a steady-state war in a fixed area of operations, a well-established knowledge of the battlefield, and in a politically sensitive region makes tactical control by operational commanders tempting. In short, operational commanders should leverage their expertise and experience in the carefully evaluated operational employment of air, ground, and naval combat forces based on an understanding of doctrine, force structure, and policy.[33]

Second, increasingly centralized execution by operational commanders creates frustration, reinforces risk-aversion, and creates a climate in which tactical leaders continually seek operational commander approval for actions. Lieutenant General Michael Short, Joint Force Air Component Commander (JFACC) during Operation Allied Force,

[28] Carl von Clausewitz, *On War* (New Jersey: Princeton University Press - Kindle Edition, 1989), 128.
[29] Robert Bolia, Michael Vidulich, W. Todd Nelson, “Unintended Consequences of the Network-Centric Decision Making Model: Considering the Human Operator,” Air Force Research Laboratory, Feb 2006, 5.
[30] Vego, II-18.
[31] Bolia, Vidulich, Nelson, 5.
[32] Clausewitz, 101.
[33] Robert A. Fitton, “A Perspective on Doctrine: Dispelling the Mystery,” *Military Review*, 65 (February 1985), 68.

experienced this while working for the Supreme Allied Commander Europe (SACEUR), General Wesley Clark. General Clark, as SACEUR, bypassed both his Joint Task Force (JTF) Commander, Admiral Ellis, and Lieutenant General Short when he began making air apportionment decisions, even going so far as to pair weapons to assigned targets.[34] General Clark himself admits that his hands-on approach was largely driven by his belief that he "would be held responsible for the military success or failure in the NATO operation."[35] This resulted in his "working further down into the details than I would have preferred, in an effort to generate the attack effectiveness…I knew we needed."[36] This friction between General Clark and Lieutenant General Short resulted in extreme frustration for both parties, and an increasingly transparent passive-aggressive rebellion by General Short.[37]

Officers in Afghanistan describe how NEC2 permitted Predator feeds to play in bases around the world, resulting in unwanted direction and attention. The problem is that this interference tended to originate from senior leaders, who were perceived as having the capability to "make or break careers."[38] Because of their seniority, direction also came in tagged as a priority, sowing confusion as to which order to follow. This intrusion from upper-echelons creates hesitancy at the tactical level, resulting in a "mother may I?" mentality. One officer states that he chose to disregard higher direction only because he was a veteran of the 1991 Gulf War and was willing to accept the career risks.[39] Author Bing

[34] Benjamin Lambeth, *NATO's Air War For Kosovo: A Strategic and Operational Assessment* (Arlington: RAND, 2001), 193.
[35] Wesley Clark, *Waging Modern War* (New York: Public Affairs, 2001), 244.
[36] Clark, 245.
[37] Lambeth, 190.
[38] Singer, 5.
[39] Singer, 6.

West, after multiple trips to Afghanistan, notes that "risk aversion leads to intervention, and information technology enables it."[40]

Lastly, the use of NEC2 creates second order effects, such as the informal training of leaders through personal experience that can have a drastic and lasting effect within the military.[41] Similarly, if NEC2 now affords operational commanders the opportunity to directly affect the tactical level of war, how do the leaders caught in the middle echelons gain decision-making experience? According to one former Predator squadron commander:

> You may have some general officer sitting behind four Toshiba big screens with greater knowledge of the battlefield from the distance. And maybe it works the first time when they intervene and save the day. But my worry is what happens with the next generation. What happens when that lieutenant, who learns thinking the guys in the back are smarter, becomes a colonel or a general. He'll be making the decisions, but not have any experience.[42]

The gradual removal of strategic leaders from the battlefield throughout history does not absolve their requirement to ensure success. Effective operational commanders ensure that the successful coordination of tactical actions is completed in order to create military conditions necessary for strategic victory. Effective, accurate, and timely communication between leadership throughout the levels of war is a requirement for unity of effort and ultimate success.

Decision Making Pitfalls

NEC2 relays a tremendous amount of information to operational commanders via networks that stream real-time data, creating vulnerabilities in the decision-making process. Systems with limited information capacity, such as Link-4, have been replaced in recent

[40] Interview with author Bing West, Newport, RI, April 27, 2012.

[41] The term "second order effect" is an extension of cause and effect logic. If a causal action results in an effect, is stands to reason that the effect can then become a subsequent cause in its own right. Michael G. Miller, "Thinking About Second & Third Order Effects: A Sample (And Simple) Methodology," *IO Sphere*, Summer 2006, 37.

[42] Singer, 6.

years by Link-16, enabling an unprecedented data fusion process capable of displaying hundreds of units within a defined field of regard. The Global Command and Control System (GCCS) is a web-enabled NEC2 system designed as a follow-on to the Worldwide Military Command and Control System, offering theater-level situational awareness to operational commanders. The data provided by Link-16, GCCS, and other NEC2 systems is typically aggregated and forwarded, to be made available at all levels of command. While this information has the potential to provide specific battlespace awareness, it also creates decision-making problems that can ensnare operational commanders. Common issues are information saturation, hesitation, and general misperceptions about the information being provided.

Information saturation is one of the most commonly cited concerns surrounding NEC2 systems, and research demonstrates that saturation can be one of the greatest impediments to effective leadership. In the wake of the BP oil spill disaster, Admiral Thad Allen estimates that he received 300-400 pieces of electronic information every day, which he cites as a causal factor for errors.[43] Angelika Dimoka, Director of the Center for Neural Decision Making at Temple University, has demonstrated that the more information that leaders try to absorb, the greater the number of mistakes made in judgment.[44] Her research also shows that decisions required of operational commanders, which require creativity and broad vision, are impeded by information saturation. Additional research shows that information saturation can also lead to paralysis, a debilitating inability to make a decision despite plenty of acceptable options available.[45]

[43] Sharon Begley, “I Can’t Think,” *Newsweek*, Feb 27, 2011.
[44] Ibid.
[45] Botti, S. & Iyengar, S.S., “The Psychological Pleasure and Pain of Choosing: When People Prefer Choosing at the Cost of Subsequent Satisfaction,” *Journal of Personality and Social Psychology*

While information saturation can cause paralysis and an inability to decide, some leaders require substantially more information than is truly required to make an appropriate decision, referred to as hesitation. Studies reveal that even when decision-makers have all the information required to make a decision, they hesitate until they receive enough subsequent information to raise their confidence level.[46] Closely related to this phenomenon is the fact that the brain is wired to acknowledge information that changes rather than information that is constant, regardless of the perceived quality.[47] The brain has a limited amount of "working memory," forcing operational commanders to prioritize information. Information received recently is typically regarded as being more valuable and relevant than information that hasn't changed, which can lead to poor decision-making, a problem compounded by frequently updating NEC2 systems.

Several additional psychological issues are at play when considering the impact of NEC2 systems. NEC2 systems, presenting tactical-level information, can lead operational commanders to believe that they have "dominant battlespace knowledge, that they know everything necessary to make rapid and sound decisions."[48] Actions in Afghanistan demonstrate that operational commanders wound up focusing on what they could see via linked networks and Predator feeds, and ignoring information that wasn't available online.[49] More specifically, operational commanders had a tendency to ignore the "primacy of

87 (3, 2004), 312-326.

[46] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Langely: Central Intelligence Agency, 1999), 51.

[47] Begley.

[48] Kolenda, 109.

[49] Thomas Ricks, "Live Video of Afghan Fighting Had Questionable Effect," *Washington Post*, March 26, 2002, A01.

locality," discounting the experience and knowledge of local tactical commanders when viewing NEC2 information.[50]

Physical Vulnerabilities

The increased utilization of NEC2 has effectively amplified the dependence on NEC2 hardware and systems, creating C2W vulnerabilities that adversaries are likely to exploit during the next armed conflict. Some of these internal vulnerabilities, such as logistical considerations for radios and a shortage of parts and energy sources, become part of the friction of war. NEC2 has created a vicious cycle where operational commanders request as much sensor information as possible, resulting in greater dispersion of radios, communications relays, data-link systems, and command centers. This, in turn, places a greater demand on logistics to supply the equipment necessary to expand coverage, creating shortages in critical items like fuel and batteries. During Operation Iraqi Freedom, a shortage of parts for aircraft-installed Link-16 systems resulted in the sidelining of the aircraft as "partially mission capable." This reliance on technology can quickly become an asymmetric disadvantage for the United States, especially when facing nations that only require basic weapons and food in order to fight.

External vulnerabilities have also been created because of the increasing reliance on NEC2. China watched with great interest as the United States swept to a swift victory during the 1991 Gulf War, subsequently producing reports detailing the use of electronic information systems (C4ISR) as deployed by the United States and multinational troops in

[50] "Primacy of locality" is a term used by the author to describe the tendency for decision makers to provide increased weighting to their own knowledge and information, even when better and more germane information is available further down the chain of command at tactical level.

the Gulf area.[51] China has consequently embarked on an ambitious and rapid program to advance their indigenous C2 capabilities while acquiring technology that enables them to attack the C4ISR systems of the United States that are viewed as brittle and susceptible to C2W.[52] The National Defense Strategy and 2010 Quadrennial Defense Review explicitly recognize this threat, an overt acknowledgement of a recognized vulnerability.[53] NEC2 might also be disrupted by an agnostic external factor – the environment. Equipment designed for climate controlled environments suffered regular breakdowns in Iraq because of dust and extreme heat, reducing the amount and types of information available via NEC2.

The danger posed by C2W is two-fold. First, forces have become accustomed to the steady centralization of execution that has occurred due to pervasive access to NEC2 coupled with the sustained low operational intensity conflicts in Afghanistan and Iraq. Tactical units, as well as operational commanders (and the layers in between), utilize NEC2 systems to pass along information, provide guidance and direction, file reports, make logistics arrangements, and a host of other tasks. If an adversary were to jam communications using electronic warfare techniques or attack critical communications nodes, there is a high likelihood that access to NEC2 would be lost, at least temporarily. Even more worrisome would be a cyber-attack that disrupts the entire network or corrupts the information being passed, sowing seeds of doubt that could immediately slow the pace of operations. Second, NEC2 and information technology heavily pervades military and operational doctrine as well as service culture. Forces routinely train and operate in an information-permissive environment, with no

[51] Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR). Lin Taiying, "Analysis of the Protection of Electronic Information In The Gulf War," *China Astronautics and Missilery Abstracts*, Vol. 2, No. 3, 1995, 28.

[52] Albert, Chase, Pollpeter, and Valko, "China's Preliminary Assessment of Operation Iraqi Freedom," *Chinese Military Update*, Vol. 1, No. 2, July 2003, 1.

[53] U.S. Department of Defense, *National Defense Strategy* (Washington DC: Pentagon, 2008), 22 and Department of Defense, *Quadrennial Defense Review* (Washington DC: Pentagon, 2010), 31-32.

degradation of services. This has created an expectation of availability, especially among more junior service members who have never conducted operations in an information-denied environment. Operational commanders who lose access to information that they have grown accustomed to having tend to suffer from immediate information paralysis and a loss of confidence in the decisions made.[54]

NEC2 systems have continually pushed back the fog of war since their widespread adoption starting in the 1970s, providing an ever-expanding view of the battlefield and the forces located therein. The danger is that in an information-denied environment, whether due to internal or external factors, this hard-fought battlespace awareness will be lost. Worse yet, the paralysis that accompanies the loss of regularly available information may become debilitating. As Colonel Campen notes, "the fog of war quickly descends on the human … both the strongest and the weakest link in the system."[55]

Recommendations

As previously mentioned, Joint Pub 6-0 recognizes that military communications are comprised of two key elements: people and hardware. These recommendations are provided with the acknowledgement that leadership, like warfare, is the most human of endeavors. Similarly, in a discussion on the effects of information technology, some issues will inherently reflect technical issues, while others reflect leadership. Similar to the repeating of familiar "lessons learned" after operations, only through continual reflection and focus can qualitative adjustments be made to the military that are necessary to wage, and win, future war.

[54] Interview with Prof. Stephen Downes-Martin, U.S. Naval War College, April 16, 2012.

[55] Alan Campen, "Information Technology – Servant, Not Master, of Operational Art," *SIGNAL Magazine*, June 2000, 31.

First, limit the level of access to information that is definitively tactical in nature. Leaders at the strategic and operational level are managing concerns that differ in both scope and scale from the tactical commander, necessitating a focus on information that is broader in character. Providing unlimited access to streaming, real-time battlefield ISR feeds risks saturating leaders with unwanted information, which can lead to negative impacts on decision-making as well as micromanagement. Place systematic blocks in the network that filters tactical data, which *by default* only displays the level of information appropriate to the level of the user. This will electronically mimic the role that people play in filtering the information that a commander receives, while retaining the ability to view tactical data if it is deemed necessary. While all leaders want unlimited access to any information that might prove valuable, there is precedent for this course of action. During Kosovo operations, the Predator feeds became such a distraction that they were shut off in Pentagon spaces with the exception of the watch floor.[56] The feeds were available, but required deliberate actions to access, deterring natural human tendencies.

Second, conduct operational-level exercises that demonstrate realistic degradation of information technology sources. Leaders are taught that forces should "train like they fight," though exercises rarely employ the realistic capabilities of perceived adversaries. The military must remain agile concerning future wars, fighting the assumption that forces will retain unfettered access to space, cyber, and information systems during a conflict. Purposefully degrading access to heavily relied-upon information sources during exercises will force leaders to make decisions in an information-denied environment, reinforce the importance of decentralization, and provide an opportunity to identify areas of friction in existing plans.

[56] Interview with LtCol Donald Holloway at the U.S. Naval War College, April 17, 2012.

Third, increase focus on leadership development with emphasis on information management and the decentralized execution of commander's intent. The next conflict is likely to look very different than insurgent warfare in a desert region, reinforcing the importance of focusing on abstract issues that can help leaders succeed in the future. Consider modification of the Officer Professional Military Education Policy (CJCSI 1800.01D) to ensure students enrolled in JPME institutions received focused training on NEC2 and information systems. Through JPME, provide leaders with an awareness of the benefits and limitations of NEC2, and more importantly, how to leverage and manage the level of information that is appropriate for the assigned position within a command. Train leaders in critical-thought, adaptability, and agility. Leaders should leverage the strengths of each level of war, reinforcing the importance of communicating intent up the chain of command while providing a vision and mission down the chain. Doing so will inherently reduce the reliance on the continuous stream of tactical information that has become the norm over the past twenty years, with the additional benefit that leaders will be prepared for reduced situational awareness.

Conclusion

History continues to prove that the next war is unlikely to represent what was either expected or prepared for, and "the convenience [of NEC2] won't be there in a quick-fighting war."[57] NEC2 is simply another high-tech tool available to operational commanders. Ultimately, how NEC2 is used during a conflict is a question of leadership. The unchecked centralization of execution, potential decision-making errors, and physical vulnerabilities of NEC2 should be acknowledged and countered through training and doctrine.

[57] West interview.

General Dempsey, Chairman of the Joint Chiefs of Staff, recently noted that his number one priority for his term as Chairman is leader development. Now is the time, during a period of fiscal austerity and on the heels of two protracted, relatively low-intensity conflicts, to focus attention and resources inward in order to develop leaders who will emerge well-trained and well-equipped to meet the challenges of future wars.

Bibliography

Albert, Chase, Pollpeter, and Valko. "China's Preliminary Assessment of Operation Iraqi Freedom," *Chinese Military Update*. Vol. 1, No. 2, July 2003.

Begley, Sharon. "I Can't Think," *Newsweek.* Feb 27, 2011.

Bolia, Robert; Vidulich, Michael; and Nelson, W. Todd. "Unintended Consequences of the Network-Centric Decision-Making Model: Considering the Human Operator." Air Force Research Laboratory, 2006.

Botti, S and Iyengar, S.S. "The Psychological Pleasure and Pain of Choosing: When People Prefer Choosing at the Cost of Subsequent Satisfaction," *Journal of Personality and Social Psychology*. Issue 87, 2004.

Campen, Alan. "Information Technology – Servant, Not Master, of Operational Art," *SIGNAL Magazine.* June 2003.

Clark, Wesley K. *Waging Modern War*. New York, NY: Public Affairs Group, 2002.

Clausewitz, Carl von. *On War*. New Jersey: Princeton University Press, 1989.

Cohen, Eliot A. *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime.* New York, NY: Anchor Books, 2003.

Davis, Alan D. "Filtering and Trust as Tools for the Operational Commander in the Information Age," JMO Research Paper, Naval War College, 2006.

Davis, Joshua. "If We Run Out of Batteries, This War is Screwed," *Wired*. Issue 11.06, June 2003.

Fitton, Robert A. "A Perspective on Doctrine: Dispelling the Mystery," *Military Review*, Issue 65, 1985.

Franks, Tommy. *American Soldier*. New York: Harper Collins, 2004.

Heuer Jr., Richards J. *Psychology of Intelligence Analysis*. Langley: U.S. Central Intelligence Agency, 1999.

Kolenda, Christopher D. "Transforming How We Fight: A Conceptual Approach." *Naval War College Review*, Spring 2003.

Lambeth, Benjamin. NATO's Air War For Kosovo: *A Strategic and Operational Assessment.* Arlington: RAND, 2001.

Mahnken, Thomas G. *Technology and the American Way of War Since 1945.* New York, NY: Columbia University Press, 2008.

Maloney, Sean. Command of the Sea: NATO Naval Planning 1948-1954. Annapolis: U.S. Naval Institute Press, 1995.

McCaskill, Ryan. "Network-Enabled and Leader-Centric Command and Control (C2): The Dangers of Digital Decision Making*."* *JMO Research Paper*, Naval War College, 2011.

Miller, Michael G. "Thinking About Second and Third Order Effects: A Sample (And Simple) Methodology," *IO Sphere*, Summer 2006.

Ricks, Thomas. "Live Video Feed of Afghan Fighting Had Questionable Effect," *Washington Post*. March 26, 2002.

Rosenberg, Barry. "Technology and Leadeship," *Armed Forces Journal*. http://www.armedforcesjournal.com/2007/07/2786772/. Retrieved April 27, 2012.

Singer, P.W. "Tactical Generals: Leaders, Technology, and the Perils of Battlefield Micromanagement." *Air & Space Power Journal*, Vol. 23, No. 2, Summer 2009.

Taiying, Lin. "Analysis of the Protection of Electronic Information in the Gulf War," *China Astronautics and Missilery Abstracts.* Vol. 2, No. 3, 1995.

Tokar, John A. "Logistics and British Defeat in the Revolutionary War." *Army Logistician*, Vol. 31, No. 5, 1999.

U.S. Department of the Army. "ES2: Every Soldier is a Sensor," *Association of the United States Army Discussion Paper*, No. 5, August 2004.

U.S. Department of Defense. *Command and Control Implementation Plan, Version 1.0.* Washington, DC: Pentagon, 2009.

U.S. Department of Defense. *Command and Control Joint Integrating Concept Final Version 1.0.* Washington, DC: Pentagon, 2005.

U.S. Department of Defense. *Joint Publication 3-0, Joint Operations*. Washington, DC: Pentagon, 2011.

U.S. Department of Defense. *Joint Publication 3-13, Information Operations.* Washington, DC: Pentagon, 2006.

U.S. Department of Defense. *Joint Publication 6-0, Joint Communications Systems.* Washington, DC: Pentagon, 2010.

U.S. Department of Defense. *National Defense Strategy*. Washington, DC: Pentagon, 2008.

U.S. Department of Defense. *Quadrennial Defense Review*. Washington, DC: Pentagon, 2010.

Vego, Milan N. *Joint Operational Warfare.* Newport, RI: Naval War College Press, 2007.