An Occasional Paper of the
Center for Naval Warfare Studies

The Implications of

NETWORK-CENTRIC WARFARE

for United States and Multinational Military Operations

by
Professor Henry Kamradt
and
Commander Douglas MacDonald, RN

Decision Support Department
Occasional Paper 98-1
31 December 1998

United States Naval War College

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
31 DEC 1998		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Implications of Network-Centric Warfare for United States and Multinational Military Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval War College,Newport,RI,02841**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**60**	

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The development of information technology has revolutionized both society and the way it conducts business. Companies that have been able to adapt to and exploit these fundamental changes have prospered; those that have not have often been left behind. The United States Navy's network-centric warfare (NCW) concept is based on the premise that the networking of sensors, weapons, and information systems, if coupled with appropriate operational concepts, tactics, and organizational structures, will likewise revolutionize the capabilities of the military. It will, it is claimed, fundamentally change the nature of war.

In theory, a common, comprehensive, and comprehensible near-real-time view of the battlefield will enable a new and faster form of warfare characterized by the concepts of "speed of command" and "self-synchronization." Speed of command enables our forces to act, and react to enemy actions and changing vulnerabilities, so quickly and effectively that we "lock out" all possible alternate enemy strategies, forcing capitulation or stopping enemy actions before they begin. Comprehensive knowledge of the battlefield also allows self-synchronization--the ability of forces to organize from the bottom up. Bottom-up organizations are perceived as being better able to adapt to the dynamic, fast-paced, complex, fluid nature of military operations, and better able to rapidly exploit opportunities and enemy vulnerabilities.

The network-centric warfare architecture will consist of three separate, but related, systems of systems--a sensor grid, an engagement grid, and an information backplane. The United States is progressing well with the individual component equipment that will form the architecture; Information Technology 21 (IT-21), the Global Broadcast System (GBS), Global Command and Control System (GCCS) , Link 16 and Cooperative Engagement Capability (CEC) are the principal examples. Many of these are already in the fleet or will be so in the near future. However integration of these systems with each other and legacy systems has been slow and is expected to be expensive.

- GCCS is composed of several mission applications built to a single, common operating environment and networked to support the sharing, displaying, and passing of information and databases. Essentially it is a joint planning net for force coordination at the operational level.

- Links 11 or 22 and 16 are NATO-standardized communication links suitable for transmission of digital information.

- CEC links geographically dispersed sensors of differing capabilities with all potential firing platforms. Such sensor netting makes each shooter’s combat system "think" that every asset in the data link is that unit’s own sensor, making engagements on remote track data possible.

- IT-21 is the United States Navy’s concept to take advantage of increased processing power, networking capabilities, and software enhancements in IT, using commercial

off-the-shelf (COTS) technology, for warfighting.

It is reasonable to expect that there will be some improvements to the NCW architecture by 2010, particularly in the areas of information technology, C4ISR, information management, and information security. Regardless of improvements, some important issues are likely to remain.

- Bandwidth will remain a limitation, especially for small mobile platforms that are heavily dependent on satellite communications (SATCOM).

- Software, which continues to grow in size and complexity at a rate commensurate with the growth in computer capacity, is a major risk area. As complexity increases, so too does the cost, in time and money, of a single line of code (SLOC). This relationship of size and complexity to cost is highly unfavorable.

- IT capabilities available through COTS will be increasingly market driven and the Department of Defense (DOD) is only a very small portion of the market. Industry is investing heavily, but not in some of the military's areas of interest such as multilevel security and reliability. DOD will be expected to fund DOD unique requirements.

- COTS IT is a double-edged sword. It offers an opportunity to upgrade systems much more rapidly than would be otherwise but brings with it serious concerns about reliability, security, and configuration management.

- Large networks and tight security are uneasy bedfellows. No system is 100 percent secure, though such protection features as data encryption and firewalls can increase the degree of difficulty that the 'hacker' must overcome to breach security.

The Intelligence Surveillance and Reconnaissance (ISR) system is a vital component of the NCW sensor grid. While the ISR system is usually thought of in terms of the high-technology hardware that collects much of the raw data, its most vital component is the group of intelligence analysts who take raw information from a number of disparate sources and compile it into a coherent picture. Collecting information, integrating it, and turning it into a product that someone can use is a monumental task. This processing is still expected to be heavily dependent on people. Without evaluation and analysis by trained human beings there is only data--no information, no intelligence--only data: and a lot of it too.

ISR is not a panacea. It has limitations both technological and human. Technology will remain limited by the laws of physics; there are things (like enemy intent) that it can rarely tell us; it is not omnipresent; it is not immune to countermeasures, destruction, or spoofing; it is highly dependent on communications throughput; and it depends on people making good decisions and doing good analysis. While new sensors and systems will improve ISR over the next decade, they will not eliminate any of these systemic problems.

To avoid information overload, intelligent information management must be developed. The process by which the human mind vets, filters and correlates data must be automated to handle the quantity of data anticipated. The magnitude of this task has been recognized, although it has not been matched with appropriate funding or level of effort.

DOD's steadily increasing dependence on a global information environment heightens its vulnerability to a growing number of increasingly sophisticated threats. There are other areas where IT-21 philosophy weakens security, even if known COTS software operating systems are protected by encryption, the efficacy of the code may be weakened because the hacker has some knowledge of the data inside the firewall. DOD is moving toward a layered defense with damage limitation in mind though it has yet to be seen if this approach will satisfy the National Security Agency (NSA).

Objectively, it is impossible to know what the impact of network-centric warfare on United States naval operations will be without conducting much more research and many more experiments. Until we agree on what we are talking about, develop specific NCW concepts of operations and supporting organizational structures, and field associated hardware that is mature enough to test, there are no objective means to confirm or refute the assertions made on behalf of NCW.

Subjectively a bit more can be said. While ultimately the smart application of information technology to warfare may be revolutionary, the process of moving from a "platform-centric" to a "network-centric" navy will be evolutionary. Will the evolutionary process continue to the point where the Navy no longer recognizable as the same species it is today? Perhaps, but progress will be slow. As a result, the impact of NCW on the Navy between now and 2010 is unlikely to be extreme. Why?

- The conceptual difference between NCW and how the Navy has traditionally tried to operate is not as great as has been supposed.

- Technological improvements and systems integration are likely to be slower and more expensive than anticipated.

- The overall potential of NCW, even in its ultimate form, is probably overstated.

The technology that will support NCW has been in evolving and improving for decades. Just as the basic technologies are not new**,** the key precepts of NCW--the synergy of networked forces, speed of command, delegation of authority, local coordination, networking of sensor and database information--are not new. Additionally, the precepts of delegation of authority, direct local coordination (self-synchronization), individual initiative based on a clear understanding of commander's intent, and command by negation are, once again, not radical departures for those who have operated under the Composite Warfare Commanders (CWC) concept.

There is no doubt that gradual maturation of technology has improved the power, efficiency and effectiveness of United States forces in conventional warfare scenarios,

particularly at the tactical level. But at the conceptual level, the practical differences are hard to pinpoint.

However, the costs and technical challenges of integrating systems into a coherent network are not trivial. Finances alone will probably dictate the speed at which progress has will be made, and that speed may not be as fast as envisioned. In particular, system integration is likely to be a challenge. The current teething problems with integrating CEC into the Aegis Baseline 6 and the Advanced Combat Direction System (ACDS) are indicative of the types of problems that need to be solved in building the NCW architecture.

Technology is a key component of the success of the United States military, but technology itself is not a panacea. Even if the ambitious technical and organizational goals implied by NCW proponents are achievable, because of the innate nature of people and technology, it is unlikely that the fundamental nature of war will change. War in the future will still be a two-sided contest with intelligent and dedicated opponents on each side. Neither side is likely to sit still and let the other win. Neither side is likely to accept that all of its strategic options have been foreclosed. It has always been a mistake to underestimate the power of human ingenuity when faced with an intractable dilemma and an incentive to solve it. We should expect our potential adversaries to look at what we do and how we do it, and to attempt to develop clever and sometimes unexpected counters.

NCW is essentially about information. The power of NCW depends on the collection, processing, and dissemination of actionable information. It relies on an extremely complex network of interoperable subnets and systems, working as they are expected to in order to meet its potential. Large networks are theoretically fairly robust; however, nodes that are both unique and critical can be highly lucrative targets. In the case of NCW, a potential adversary might attempt to work against any or all of the three NCW grids (sensor, information, engagement), the connectivity that binds them together, or the information technology that underpins them all.

Just as our dependence on overhead sensors has not gone unnoticed, our growing dependence and fascination with information technology has been well documented. We should expect that potential adversaries are looking for ways to exploit it. There are main three ways that we may be increasing IT vulnerability:

- By moving toward an open architecture information infrastructure.
- By moving toward COTS.
- By moving toward rapid upgrades.

The notion of information superiority is probably an invalid, and potentially dangerous. The amount of information each side is able to disseminate is not the key to success; the critical measure of performance is the ability to move that information needed to accomplish the operational objectives of the commander. It is not clear how United States forces using high-tech sensors, communications, and information systems can achieve information dominance

against an indigenous, entrenched opposition that can meet most of its needs with very simple means or carefully selected, commercially available technology or services.

The end of the Cold War and the associated uncertainty about the role of the military have led to major reductions in defense funding. To reduce spending without reducing capability, the United States is betting heavily on precision targeting and high technology-weapons that are highly dependent on information superiority to be effective. However, to train and equip our forces as if we expect nearly perfect information, and then not be able to obtain it will lead to disaster. If we expect war to be chaos and train and equip with that expectation, any information we can obtain will serve as a force multiplier.

Multinational operations will enjoy varying degrees of interoperability with the United States. First-rate partners will achieve full connectivity, assuming security concerns can be assuaged, although full integration of many systems may still be costly and time consuming. Low-end partners could achieve basic connectivity with portable arrangements. It is the command structure that is likely to prevent the full benefits of NCW from being realized. Future coalitions are likely to enjoy military supremacy; therefore, the possible benefits of unity of command are likely to be subordinate to the political requirement for parallel national command.

AIM

The aim of this paper is to assess the implication of NCW on United States military operations conducted with allied or coalition partners at about the year 2010. It is directed to non-U.S. readers who may not be intimately familiar with the NCW vision, C4ISR, or computer technology

SCOPE

JV 2010 notes the importance of integrating United States forces with allied and coalition partners because it is expected that nearly all force deployments in the future will be associated with multinational operations.[1] This paper will focus initially on the impact of NCW on United States national operations. NCW is intended for joint operations, but because it is a naval vision the paper will have a naval bias. Taking these findings forward, the paper will then investigate the impact of the United States concept of NCW in an allied and coalition environment.

METHOD

Because NCW is a maturing vision at the time of writing, there is relatively little documented material available to research. However, much information has been gleaned during numerous visits to research laboratories, both civil and military. The views of United States and foreign defense staffs have also been sought. A full list of sources is at Annex B.

1. General J. M. Shalikashvili, *Joint Vision 2010* (Washington, D.C.: Chairman Joint Chiefs of Staff, n.d.), p. 9.

PART I -- UNITED STATES NCW OPERATIONS

THE U. S. REQUIREMENT FOR NCW

The Global Security Environment

The drive toward revolutionary military concepts, including NCW, is based on the United States position relative to the global security environment. Currently, the United States enjoys relative security. The threat of global war has receded, and the United States is not now confronted with a "peer competitor"–a hostile power of similar strength and capability–nor is it likely to have one in the near future. Given the military power of the United States, it is also unlikely that any regional power or coalition could amass sufficient conventional strength to defeat it. Despite this "strategic pause," the complexity of the current world has probably increased, and the future is no more certain than it has ever been. There are still near-term conflicts that the nation must remain ready for while it prepares for uncertainties about the "what", "where", and "how" of future security challenges.

Between now and 2010 the military challenges that confront the United States are significant but not intractable. In the near term there is a possibility that military forces may be called to thwart regional aggression in Eastern Europe, the Middle East, or Korea. Beyond these serious, but manageable, contingencies, the proliferation of advanced technology, such as ballistic missiles (BMWs) and weapons of mass destruction (WMD), whether for state or terrorist use, is also of concern. It is also possible that organized crime and the drug trade may embroil United States forces, as may involvement in failing states.[2] However, none of these challenges pose a direct threat to the survivability of the United States homeland. Even the possibility of "wild card" scenarios and asymmetric threats would be unlikely to threaten United States survivability directly, although they might easily undermined United States influence in some regions of the world.[3] The real nub of the security dilemma for the United States is the unpredictability of the threat[4] and the expectation that regardless of the source, it must be addressed.

While the United States has every reason to be confident of it's capabilities to deal with near term conventional threats, it can not necessarily afford to sit back and ignore major changes to technological and/or social realities that could have an fundamental impact on the nature of war.

It is the confluence of having the luxury of time to reflect on future security requirements, the need to maintain the technological edge that has been such an important factor in past military success, and the reductions in the military budget that is driving the United States' interest in revolutions in military affairs. It is hoped that such an RMA will help maintain force

2. William S. Cohen, Secretary of Defense, *Report of the Quadrennial Defense Review* (May 1997), Section 2, pp. 3-5.

3. William S. Cohen, Secretary of Defense, *Annual Report to the President and Congress 1998,* <http://www.dtic.mil/execsec/adr98/msg.html> 6 March 1998, Chapter 1, p.3.

4. Admiral J. Paul Reason, *Sailing New Seas,* Newport Paper 13 (Newport, R.I.: Naval War College Press, 1998), Part 1, pp.5-6 (available online at http://www.ncw.navy.mil/npapers/np13/np13toc.htm).

effectiveness while improving efficiency and reducing the associated costs.

United States National Security Strategy

United States national security strategy is driven by its national interests and constrained by available resources.[5] United States national interests fall into three categories. First in priority are vital interests--those of overriding importance to the survival, security, and territorial integrity of the United States. Second are important interests--those that do not affect national survival, but do affect national well-being and the general character of the world. Third are humanitarian interests--those situations where the United States feels compelled to get involved because its the "right thing to do." The decision to use United States military power and the extent to which it is used will depend on the perceived importance of the threatened interests, and whether the costs and risks are commensurate with the potential payoff. United States vital national interests include:

a. Protecting the sovereignty, territory, and population of the United States.

b. Preventing the emergence of hostile regional coalitions or hegemonies.

c. Ensuring uninhibited access to key markets, energy, and resources.

d. Deterring and, if necessary, defeating aggression against United States allies and friends.

e. Ensuring freedom of the seas, airways, and space, and security of communication.

National Military Strategy

The basic challenge for the United States armed forces is to shape and respond in the current near term while concurrently preparing for the future. The DOD strategy to ensure United States military superiority has four main parts:

a. Force modernization that incorporates cutting-edge technology.

b. Exploiting the Revolution in Business Affairs to reengineer DOD infrastructure.

c. Hedging against unlikely, but significant, future threats while constrained by limited resources.

d. Exploiting the RMA.

5. William S. Cohen, Secretary of Defense, *Annual Report to the President and Congress 1998,* <http://dtic.mil/execsec/adr98/msg.html>, 6 March 1998, Chapter 1, pp. 4-5.

Joint Vision 2010

JV 2010 is considered to be the conceptual template for joint operations and warfighting in the future. The future capabilities it envisions are intended to guide warfighting requirements and procurement, and to focus technological development. JV 2010 proposes four new operational concepts: dominant maneuver, precision engagement, focused logistics, and full-dimensional protection, supported by the overarching enablers of technological innovation and information superiority. While the integration of new technologies with innovative operational concepts is viewed as important, information superiority as is considered to be the key to the success of JV 2010.

Information Superiority

Information superiority is defined as "the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[6] Once achieved, information superiority should facilitate total battlespace awareness, allow commanders to employ widely dispersed forces to engage the enemy, enhance force protection, and tailor the logistics flow to meet the requirements of the moment. Improved intelligence collection and assessment, as well as modern information processing and command and control capabilities, are pivotal to the achievement of information superiority. DOD is working to provide a complementary, secure, and open C4ISR network architecture. The six principal components of the evolving C4ISR architecture for 2010 and beyond are:

a. A robust multisensor information grid providing dominant awareness.

b. Advanced C2 capabilities, faster and more flexible than the enemy's.

c. A sensor-to-shooter grid.

d. An IW capability to deny an adversary awareness or unimpeded use of forces.

e. A joint communications grid with adequate capacity, resilience, and networking.

f. An information defense system to protect C3 from interference or exploitation.

6. Ibid. Chapter 13, p. 2

THE VISION OF NETWORK CENTRIC WARFARE

The vision of network-centric warfare (NCW), first presented in United States Naval Institute *Proceedings*, elaborates and expands on the importance of information superiority to the future of warfare.[7] It is important to note that information superiority and network-centric warfare are not synonymous. Information superiority is a necessary, but not sufficient, precursor for NCW. The NCW vision is to create and exploit information superiority by coupling sensors, command and control (C2), and shooters to a network in order to increase greatly combat power[8] and to create a well-informed but geographically dispersed force. The enabling elements are: a fully netted information service with access to all appropriate information sources; weapons with adequate reach, precision, and speed of response; and a C2 process that includes high-speed, automated tactical decision aids to aid in the assignment of resources to needs, and the coupling of integrated sensors to shooters.

Information technology is undergoing an all-encompassing shift from stand-alone to networked computing. The emergence of network-centric computing is most obvious in the explosive growth of the Internet, Intranets, and Extranets. These networks allow information to be created, distributed, and easily exploited across the global computing environment. The power of network-centric computing comes from information-intensive interactions between very large numbers of heterogeneous computational nodes; the power of the network is proportional to the square of the number of such nodes. The assumption is that value is derived from the content, quality, and timeliness of the information moving on the network and that this value increases as information moves toward 100 percent relevant content, 100 percent accuracy, and zero time delay.

There is no doubt that United States society and business have witnessed sweeping changes brought about by huge advances in networked IT. Companies that have been able to evolve their organizations and processes to exploit information technology have gained tremendous competitive advantages, particularly in transaction-heavy regimes. The NCW hypothesis is that many of the changes in the way we make wealth are directly transferable to the way we make war. The theory is that the benefits that information technology has provided to business, when combined with new doctrine, tactics, and organization, have the potential to change the fundamental nature of warfare.

NCW advocates expect to draw power from three phenomena: the shift in focus from the platform to the network, the shift from directed action to self-synchronization, and a vast increase in the speed of decision making. Through networking of sensors and weapons, the creation of common operational and tactical pictures, and the rapid dissemination of critical information on the task at hand, NCW hopes to achieve two effects that will, in turn, significantly improve the efficiency, effectiveness and power of United States forces. The first is speed of command; the second is self-synchronization.

---

7. Vice Admiral A. K. Cebrowski and J. J. Gartska, "Network Centric Warfare: Its Origin and Future," Naval Institute *Proceedings*, January 1998, p. 29

8. The Joint Staff, J6, *Observations on the Emergence of Network-Centric Warfare*, <http://www.dtic.mil/jcs/j6/education/warfare.html, p. 1.

Speed of Command

Speed of command is the ability to observe, decide, command, and act far more quickly than the enemy. It has three parts:

- Developing a substantially better understanding of the battlefield, through the use of improved sensors, powerful networks, improved display technology, and sophisticated modeling and simulation.

- Using that knowledge to quickly and precisely mass effects against the adversary.

- Exploiting the shock of closely coupled events to foreclose possible enemy courses of action, ultimately "locking out" enemy options and disrupting his strategic plans.

Self-Synchronization

Self-synchronization is the ability of an informed force to organize and synchronize complex warfare activities from the bottom up. The organizing principles are unity of effort, clearly articulated commander's intent, and carefully crafted rules of engagement. Self-synchronization is enabled by a thorough knowledge of one's own forces, enemy forces, and the operating environment.[9] The premise is that very high levels of situational awareness will allow forces to coordinate at the local level and respond rapidly enough to take advantage of fleeting opportunities. Traditional military operations utilize top-down, directed synchronization to achieve the required fires and level of mass. Because each element of the force has a unique operating rhythm, combat at the operational level is reduced to a step function, which takes time and provides opportunity to the enemy. After the initial engagement there is an operational pause, and the cycle repeats. In contrast, bottom-up organization is hypothesized to enable self-synchronization, in theory the step function becomes a smooth curve, and combat moves at a higher speed. The "Observe-Orient-Decide-Act (OODA) Loop" hypothetically vanishes, and the enemy is denied the advantage of ones own operational pause. Such speed of action might "lock-out" alternative enemy strategy and "lock-in" success.

NCW Architectural Requirements

NCW requires an operational architecture with three critical elements: a sensor grid, an engagement grid, and a high-performance information grid that provides a "back-plane" for computing and communications. Sensor grids can quickly generate high levels of battlespace awareness when coupled with appropriate filters, analysis, and processing. Engagement grids will exploit this awareness to deliver weapons (or effects) precisely where and when they are required. The information grid enables the operational architecture of sensor and engagement grids. Many key elements of these grids are already in place or soon will be available; however,

9. Captain W. Gravell, “The Offensive Punch - Network-Centric Warfighting,” *Surface Warfare*, March/April 1998, p. 14.

their full integration into a more powerful fighting system is only partially complete. If NCW is to be carried forward, appropriate funding and training will be required to allow for the co-evolution of technology, organization, and doctrine.

THE EVOLUTION OF THE REVOLUTION

The fundamentals of NCW–the systems, doctrine, and organization that will form the foundation of NCW–have been evolving for some time. The immediate forerunner to NCW was the "System of Systems" (SofS) concept, which advanced the synergistic interaction of sensors, C2, and precision, integrating them into a highly capable fighting force.[10] Initially NCW architecture will comprise a number of systems that are already in the fleet or will be in the near future: these include the Global Command and Control System (GCCS), Links 11, and 16, and the Cooperative Engagement Capability (CEC).[11] Each of these key components is briefly described below.

GCCS

GCCS is composed of several mission applications built to a single common operating environment and networked to support sharing, displaying, and passing of information and databases. Essentially it is a joint planning net for force coordination at the operational level. The GCCS infrastructure consists of a client-server environment incorporating UNIX-based servers (being replaced by Windows NT), and client terminals as well as personal computer (PC) terminal workstations, operating on a standardized local area network (LAN). The GCCS infrastructure supports a communications capability providing data-transfer facilities among workstations and servers. The Secret Internet Protocol Router Network (SIPRNET) provides connectivity between GCCS sites. This layer of the Defense Information Systems Network (DISN) carries classified data up to United States SECRET and is NOFORN, or United States proprietary. Remote user access is also supported via dial-in communications servers, or via telnet from remote SIPRNET nodes.[12] At sea the bearer is normally a satellite channel. Because of the demand on military constellations, this will normally be by commercial means, such as INMARSAT, for destroyers and below.

Tactical Data Links

Links 11, 22, and 16 are NATO-standardized communication links suitable for transmission of digital information. Current practice is to describe a tactical digital information link (TADIL) by its standardized message formats and transmission characteristics. TADILs interface two or more command and control or weapons systems via a single or multiple network architecture and multiple communication media for exchange of tactical information. Link 11 (TADIL-A) is a secure, half-duplex, netted digital data link utilizing parallel transmission frame characteristics and standard message formats at either 1,364 or 2,250 bits per second (BPS). It is normally operated in a roll-call mode, under the control of a net control station, to exchange digital information among airborne, land-based, and shipboard systems. Link 16 (TADIL-J) is a

10. U.S. JCS (J6 C4 Systems Directorate), *Mission Orientated, Warrior Focused,* <http://www.dtic.mil/jcs/j6/j6_old.html>, 1 June 1998.

11. Admiral William A. Owens, "The Emerging System of Systems," Naval Institute *Proceedings*, May 1995, p. 39.

12. U.S. CJCS, *The Global Command and Control System*, http://spider.osfl.disa.mil/fbsbook/fbsbook.html, 2 June 1998.

secure, high-capacity, jam-resistant, nodeless data link that uses Joint Tactical Information Distribution System (JTIDS) transmission characteristics and protocols, conventions, and fixed-length message formats.[13] The systems are line of sight and are carried on UHF or microwave channels.

Cooperative Engagement Capability

The Cooperative Engagement Capability (CEC) links geographically dispersed sensors of differing capabilities with all potential firing platforms C and fuses data from multiple sensors to develop a composite track of engagement quality. Such sensor netting makes each shooter's combat "think" that every sensor serving the data link is that unit's own. Accordingly, engagement using remotely provided track data is possible. In addition, the ability to develop composite tracks means that every participating unit has a real-time and in theory, identical, picture of the battlespace.. With the addition of the airborne element, the CEC surveillance window will be dramatically increased.[14] Because targets are illuminated from different directions the opportunity to capture stronger aspects is maximized. This creates a level of battlespace awareness that surpasses anything that can be created with stand-alone sensors. With CEC target tracking is more continuous, engagement depth is increased, the ability to detect and track targets in the presence of jamming is improved, and the ability to detect targets with lower-than-average radar cross sections is better than is possible with a stand-alone sensor.

IT-21

Information Technology for the 21st century (IT-21) is a USN concept that takes advantage of increased processing power, networking capabilities, and software enhancements of IT, using commercial off-the-shelf (COTS) technology, for warfighting. This ranges from using PCs and the Windows NT operating system, to Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) message packaging. [15] The Navy is building a communications and networking backbone that will support the rapid exchange of information between naval and joint platforms. The majority of the fleet should be fitted by 2002, and the rolling seven year program should be complete by 2005; [16] The total cost will be $6.6 billion.[17] New doctrine and organizations also are being developed to allow the Navy to take full advantage of these changes.[18]

---

13. U.S. Defense Technical Information Center, *Tactical Digital Information Link,* <http://www.dtic.mil/doctrine/jel/doddict/data/t/05737.html>, 2 June 1998.

14. John H. Dalton, Secretary of the Navy, *Posture Statement* (1998), Section VIII, pp. 66-67.

15. The Internet is a network of computer local area networks (LANs) throughout the globe that can be accessed by PCs using modems and standard telephone lines. It provides access to a vast amount of data; indeed, many of the references for this paper are taken from Internet sources. However, it has shortcomings for military use; only about 80 percent (assessments vary) of E-mail is ever received; there is no confirmation of receipt; routing is by a basic protocol that breaks down at peak times, and security is easily compromised by hackers. Intranets are private Internet systems; an example is the SIPRNET. Although 'Metcalfe's Law' illustrates the potential power of the Internet, Metcalfe is also quick to point out its increasing fragility. As Intranets grow in size, they will also suffer in the same way. A more comprehensive explanation of the Internet based on Metcalfe's work is at Appendix I.

16 Rear Admiral D. Mayo, *BandwidthBaseline Assessment Memo,* <http://copernicus.hq.mil/crwg98/briefs/brown_bag.pdf>, p, 22.

17. Ibid, p.29

18. John H Dalton, Secretary of the Navy, *Posture Statement* (1998), Section VI, p.41.

Other Legacy Systems

The systems listed above are some of the more critical command and control elements that will form the foundation of NCW. However, there is a plethora of legacy systems on which to build; many of them provide duplicate and redundant capability. This is because in the past, combat support information for operations, intelligence, personnel, logistics, engineering, finance, and medical purposes were, in general, only available through unique, mission-specific stovepipes sponsored by a single service.[19] Such a stovepiped architecture hinders the integration of information into an overall warfare picture. DOD has recognized this shortcoming and established the Defense Information Infrastructure (DII) to revolutionize information exchange across the DOD area of responsibility, by maximizing the benefit of IT while reducing the burden on staffs and the expertise required to use it. [20] Accordingly a joint vision was developed for the services known as the "C4I for the Warrior" (C4IFTW) program. C4IFTW is a commitment to a broadly connected joint system that provides total battlespace information with a focus on the warfighter's perspective. The Global Combat Support System (GCSS) is the final piece of the C4IFTW concept. It uses the same tools, approach, methodology, and integration processes in providing combat support information as are used by the GCCS in providing command and control and intelligence information. These two systems and the Defense Messaging System (DMS) and the Defense Information System Network (DISN) are the key elements of the DII.[21]

19. U.S. Defense Information Systems Agency (DISA), *Global Combat Support System (GCSS)* [Online] Available, <http://www.disa.mil/line/gcss.html>, 28 January 1998.

20. U.S. Defense Information Systems Agency, *DISA Master Plan 6.0,* <http://www.disa.mil/diimp/diimp-2.html>, 27 June 1997.

21. U.S. Defense Information Systems Agency (DISA), *Global Combat Support System (GCSS)* [Online] Available, <http://www.disa.mil/line/gcss.html>, 28 January 1998.

NCW REALIZABLE BY ABOUT 2010

It is reasonable to expect that there will be improvements to the NCW architecture by 2010. Although 2010 is eleven years in the future, and several years beyond the period covered by the current Program Objectives Memorandum (POM), it is fairly easy to identify new systems that might reasonably be operational by 2010. The POM gives details of proposed acquisitions and anticipated funding over the start of the next decade. The elements of NCW that might be available by 2010 will either take advantage of commercially driven improvements in technology or their long-lead-time research, development, or procurement items will already be funded in the POM. The following sections detail what might reasonably be expected in the areas of information technology, C4ISR, information management, and information security

IT Expectations.

There have been dramatic improvements in IT over the last two decades, but the advances in hardware, software and artificial intelligence have been at vastly differing rates. [22] Computing power has grown almost exponentially, software improvements have been significant; and artificial intelligence (AI) has made only modest progress in comparison. This increase in power will improve capability, but the improvement will be limited by software. Over a decade ago there were great expectations for expert and knowledge-based software in C3 systems, which have not come to pass.[23] Neural networks then became the next great hope, but they have yet to mature and reach the fleet.

> Hardware. Silicon based IT has increased in capacity and speed while the unit cost has dropped. While these gains will eventually be limited by the laws of physics, new laser technology is providing the next generation of hardware, one that will offer improvements measured in orders of magnitude. Vertical Cavity Surface Emitting Lasers (VCSELs) are poised to be cheaper and faster, use less power, and be more versatile than silicon chips. One can transmit data at 6 gbps; and packed closely together, a 10 x 10 array boasts an aggregate rate of 600 gbps.[24]
>
> Software. While software grows in size and complexity at a rate commensurate with the growth in computer capacity, it is a major risk area. As complexity increases, so too does the cost, in time and money, of a single line of code (SLOC). This relationship of size and complexity to cost (illustrated in Figure 1) is highly unfavorable. Cases of software failures, delays, and cost overruns are legion, particularly when sophisticated or cutting-edge applications are involved. An example is the United Kingdom's civil air traffic control center; in early 1996 the in-service date was delayed by a year because of software faults.[25] The system, potentially the most advanced in the world, is manufactured by the

22. Dr Randall Shumaker Naval Research Laboratory, "Presentation," *NCW Workshop 1 Research Memorandum 98-1*, (Newport RI: DSD, USNWC, 1998), p. 4.

23. Ronald E. Wright, "The Potential Application od Neural Networks and Neurocomputers in C3I," in *Science of C2: Coping with Complexity*, ed. Stuart E Johnson and Alexander H Levis (Fairfax, VA.: AFCEA International Press, 1988), p. 164.

24. Steve G Steinberg, VCSELs, *Wired*, February 1998, p. 77.

25. *Aviation Week and Space Technology*, 5 February 1996, p. 23.

US firm Lockheed Martin; however after a further eighteen-month delay it is still not in service. If the current software checks uncover further faults the project could be abandoned and a simpler, though less effective, system procured instead.[26] To produce complex software with improved reliability and an affordable price, improvements of the same order of magnitude as the changes from machine code to high-level language to subroutines are needed. For now, it is frequently necessary to limit or scale back functionality or eliminate desired capability in order to achieve affordable and reliable software.

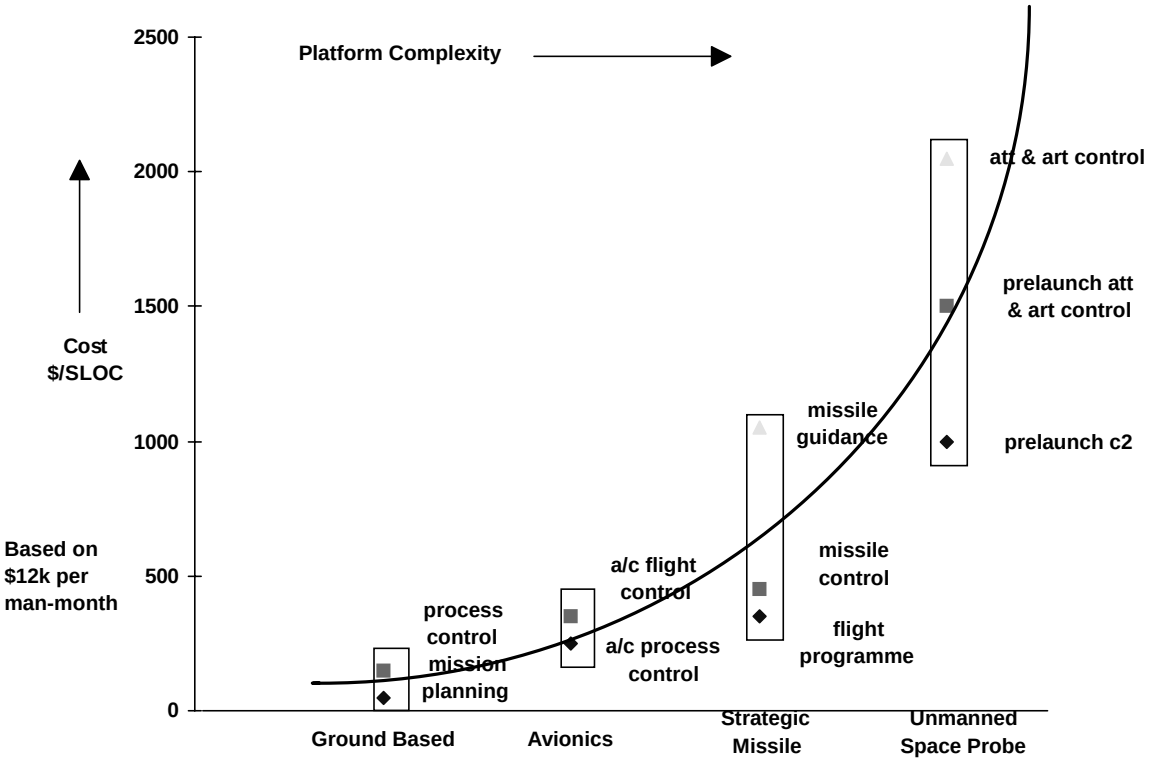

Figure 1 - Software Development related to Size, Complexity and Cost[27]

Commercial Off-the-Shelf (COTS). IT capabilities available through COTS will be market driven, and the DOD is only a very small portion of the market. Industry is investing heavily in IT development, but not in some of the military's prime areas of interest, such as multilevel security and reliability. If these are a DOD requirement, industry will expect the department to fund improvements. This could negate some of the cost benefits of COTS.[28] Ultimately, COTS IT is a double-edged sword. It offers an opportunity to upgrade systems much more rapidly than would be possible through the traditional military research and development process, but it brings with it serious concerns about reliability, security and configuration management.

26. Arthur Leathley and Jason Nisse, "Axe poised over air traffic computer," *The Times,* 25 June 1998, p. 2.
27. Source, Institute for Defense Analysis, January 1991.
28. "Feds, industry at odds over data, duties," *Federal Computer Week,* 10 November 1997, p. 1.

Network Security. Large networks and tight security are uneasy bedfellows. No system is 100 percent secure though such protection features as data encryption and firewalls can increase the degree of difficulty that the hacker must overcome. Indeed it may be so great that the intruder may consider the effort and time required outweigh any benefit gained. Nevertheless, reports of successful intrusion into systems connected to the Internet are legion. This is compounded by the increasing size of software which precludes economical auditing of programs that contain code written abroad for unauthorized features.

C4

As discussed above, IT-21, GCCS, Link 16, and CEC are all funded programs that will be in place well before 2010. They are likely to be in service until well after that date. In order to achieve the promise of NCW, the initial focus for further investment is directed at establishing the "information back-plane".[29]

Communications. DISN provides a secure, wideband, multimedia, flexible, and fully integrated global network. It transports voice, video, and data by terrestrial and satellite means and a fiber-optic secure network is in the final stages of construction in the United States. To leverage commercial satellite technology and provide a mobile, secure, global communications capability, an Enhanced Mobile Satellite Service (EMSS) program has also been initiated. The DOD has programmed $90.3 million from FY 1999 through FY 2003 for this.[30] Military satellites will carry the Global Broadcast System (GBS) which has a tremendous capacity; some 24 mbps on the downlink, or more than 300,000 times the capacity of a normal 72-baud RATT broadcast. The uplink from individual platforms will be far more limited, however. The broadcast will be channelized; for example high command, intelligence, and weather traffic might each carried on a separate one.

These communications pipes will be the bearers for the information back-plane. An architecture of internets, SIPRNETS and special compartmented information (SCI) nets will carry traffic up: and the GBS will carry traffic down to forces in-theater. However, as IT-21 is based on Windows NT, DOD systems will be hostage to the commercial sector in terms of quality, maintenance, reliability, and obsolescence. Further, in the past, seamless connectivity offered the enemy opportunities to detect and localize transmitters or interfere with communications, there is no indication that this will change in the future.

---

29. One of the great difficulties that must be overcome in funding C4ISR programs is producing a quantifiable assessment of its worth in the Cost and Operational Effectiveness Assessment (COEA) process. The Defense Information Systems Agency (DISA) is supporting the use of the "Federation" model to improve joint, theater-level, C4ISR analysis. U.S. Defense Information Systems Agency (DISA), C4ISR Model "Federation," <http://www.disa.mil/D8/html/navy-study.html>, 22 April 1998.

30. Honorable Jacques S. Gansler, "Statement," U.S. Congress, House, Committee on National Security, *Overview of the Under Secretary of Defense for Acquisition and Technology*, <http://www.acq.osd.mil/ousda/testimonies/hnsc_redraft.html>, 26 February 1998.

Bandwidth will continue to be a limitation, especially for small mobile platforms that are heavily dependent on SATCOM. Table 1 contains an unclassified estimate of bandwidth capacity of a variety of tactical platforms over the next thirty years. The limits on how much data can be moved are physical; however, network architecture and preprocessing might enable us to update information much more efficiently. For example, if common databases are held by all network participants, it will be necessary to transmit only changes to the data, drastically reducing the amount of bandwidth required. The bottom line is that using both military and commercial satellites, DOD assesses that it will have sufficient bandwidth for its needs.[31]

Bearer	1998	2000	2010	2020
Fiber-optic	622 Mbps	2.5 Gbps	80 Gbps	500 Gbps
Satcom (large platform)	10 Mbps	45 Mbps	45 Mbps	45 Mbps
Satcom (small platform)	1.5 Mbps	10* Mbps	20* Mbps	20* Mbps
RF (line of sight)	45 Mbps	155 Mbps	155 Mbps	155 Mbps
RF (over the horizon)	64 Kbps	64 Kbps	64 Kbps	64 Kbps

* Uplink 1.5 Mbps

Table 1 - Typical Platform Communication Capability

Intelligence Surveillance and Reconnaissance (ISR)

The Intelligence Surveillance and Reconnaissance (ISR) System will form an important component of the network-centric warfare sensor grid. The current United States ISR system is a loosely confederated "system of systems." It consists of a wide variety of space-based sensors, unmanned aerial vehicles, manned strategic and tactical reconnaissance aircraft, and other intelligence gathering sources and methods, including human intelligence. Its job is to collect, evaluate, and disseminate intelligence in a format that is useful to the end user, whoever that may be. While the ISR system is usually thought of in terms of the high-technology hardware that collects much of the raw data, its most vital component is the group of intelligence analysts who take raw information from a number of disparate sources and compile it into a coherent picture.

Component sensors of the ISR system are capable of providing near-real-time electro-optical, infrared, and synthetic aperture radar-based photography and of intercepting a wide variety of electromagnetic emissions. When properly tasked and focused, ISR is capable of providing a tremendous amount of knowledge about the enemy, and potentially, a tremendous advantage on the battlefield.

It is not the purpose of this paper to describe in detail the performance of each component of the ISR system. Classification restrictions alone would preclude it. It is, however, worth

31. Rear Admiral D. Mayo, *Bandwidth Baseline Assesment Memo*, <http://copernicus.hq.navy.mil/crwg98/briefs/brownbag_bam.pdf>, p. 22.

highlighting a few of the additions to the ISR system that are expected by 2010 and have been reported in open sources. While many of these upgrades represent considerable improvements in capability, they will not eliminate any systemic limitations.

Space Based Infrared Satellite. The Space-Based Infrared Satellite network (SIBRS) is intended to replace the Defense Satellite Program (DSP) missile warning systems with an infrared network that provides better target discrimination and better global coverage, and is able to relay warnings much more quickly when short-range missiles are launched. The network will consist of both high and low orbital satellite constellations. It will have a small number of geosynchronous and highly elliptical orbiting satellites, complimented by an estimated twenty four "SBIRS-low" vehicles. SIBRS-low is estimated to be able to discriminate between missiles and decoys and to hand off trajectory data to national and theater TMD. The first SBIRS will be orbited in 2004 and the last in 2007.[32] There is some discussion of integrating SBIRS-low into CEC. [33]

Future Imagery Architecture. The National Reconnaissance Office (NRO) is also planning for the Future Imagery Architecture (FIA). FIA will replace today's large and complex NRO spacecraft with a constellation of more numerous, smaller satellites that can provide improved revisit times. This will make it more difficult, but still not impossible, for adversaries to work around satellite schedules. The current network of two or three optical imaging satellites of the KH-11 type and two Lacrosse imaging radars.[34] NRO had planned to begin orbiting the new constellation in 2003 or 2004 but has delayed the start due to budgetary considerations. NRO appears to be looking at an evolutionary system of three or four satellites rather than a revolutionary system of ten or twelve that could provide the United States military with dramatically improved revisit times and worldwide coverage. However, the new plans are also coming under fire form some critics who believe the agency is not going far enough. FIA is designed to operate until about 2020. There are also separate plans for a new signals intelligence (SIGINT) constellation which, like FIA, would be populated by a larger number of smaller satellites. The system is scheduled to come on line in the latter part of the next decade.[35]

Tactical Space Based SAR/MTI. The Defense Advanced Research Project Agency (DARPA) and NRO are looking at developing a network of approximately twenty small satellites carrying a sensor combining SAR and a moving target indicator (MTI). The sensor would be able to spot moving targets on the ground, ranging from columns of vehicles to isolated mobile missile launchers. The satellites are intended to supplement (and eventually replace) Joint-STARS airborne radar by looking well beyond the aircraft's range. However, the satellites will not have the aircraft's acuity, so initially they will be

32. "Spectrum Astro to Bid for SBIRS-Low," *Aviation Week & Space Technology*, 13 April 1998, p. 58.

33. Christopher J. Castelli, "Four Advanced Descriminator Options Need to Be Studied," *Inside the Navy*, 29 June 1998, p. 5.

34. Craig Covault, Eavesdropping Satellite Parked Over Crisis Zone, *Aviation Week & Space Technology*, 18 May 1998, p. 30.

35. Joseph C. Anselmo, Imagery Satellite Costs Prompt NRO Delay, *Aviation Week & Space Technology*, 25 May 1998, p. 24.

used more for cueing other sensors than tracking and target identification.[36]

Manned Aircraft. The United States also operates a large assortment of specialized manned reconnaissance aircraft carrying a diverse spectrum of sensors. These include the E-2 Hawkeye, E-3 AWACS, E-8 Joint STARS, the EC/RC-135 family, the U-2, the EP-3, the RC-7, and others. In addition to collecting intelligence, some of these platforms, particularly the E-3 and the E-8 have important battle management functions. While the United States Air Force would like to transition many of these to UAVs and then satellites, the majority of these aircraft will be around for the foreseeable future.[37] Most of them have received, or will shortly receive, upgrades particularly in the area of providing useful real-time information directly to the warrior. For example, the U-2 has recently completed a reengineering designed, among other things, to equip the aircraft with MTI radar to enable it to track moving vehicles and data link the tracks back in real time. The ultimate goal is to find, fix, track, identify, and engage anything of military significance on the surface of the earth in real time.

Unmanned Aerial Vehicles. Manned aircraft and satellites will be augmented with a new generation of UAVs, although, because of escalating costs they may not be available in the numbers once envisioned. The Predator UAV has operated successfully in Bosnia and the Middle East providing a variety of real-time tactical intelligence to the theater commanders. Its primary sensors are SAR and EO/IR. Predator is, however, limited to relatively low-threat areas because of its flight profile and nonstealthy radar characteristics. Predator's range limitations also prohibit it from self-deploying from the United States and it has a relatively short on station time. By 2010 Predator will be augmented by two new long-range UAVs, Darkstar and Global Hawk. Darkstar is a long-range very-low-observable (VLO) platform. It will be capable of operating in high-threat air defense areas and will carry either an electro-optical package or a low-probability-of-intercept SAR that was originally developed for the A-12. It will begin integrating into the force in 1999.[38] Global Hawk is a long-endurance platform designed to taxi, takeoff, and fly autonomously using GPS and a ring-laser inertial navigation system. The vehicle is designed to operate at altitudes up to 65,000 feet, with a 14,000 nautical mile ferry range and an on station time of more than 40 hours.[39] Global Hawk's primary sensor will be SAR/ISAR, but it is capable of carrying other sensors, and because of its long endurance time and high patrol altitude is an excellent communications relay platform.

Sensor Technology. Aside from the platforms themselves there are other ISR-related technologies being explored. These include:

- Moving target exploitation, which allows semiautomatic target recognition from

36. David A Fulghum, "Small Recon Satellites Win 1999 Budget Funding," *Aviation Week & Space Technology*, 9 February 1998, p. 28.

37. "ISR Sees Problems Ahead," *Air Force Magazine*, April 98, Page 23.

38. David A. Fulghum, "Darkstar Beats Problems, Scores Successful Flight," *Aviation Week & Space Technology*, 6 July 98, p. 25.

39. "Teledyne Ryan's Global Hawk Begins Taxi Tests," *Aviation Week & Space Technology*, 3 November 1997, p. 38.

video.

- Better "geolocation sensors" to improve the targeting accuracy of GPS guided weapons.
- New multispectral and hyperspectral imagery that allows extraction of more data from time-lapsed imagery. [40]

ISR Systems Integration. While much is being done to improve systems and sensors, the major emphasis is on integrating available systems to create an all-encompassing, seamless architecture. Virtually all military platforms and personnel generate data that can help supply the intelligence network with an updated, real-time database depicting the battlefield in detail. Collecting this information, integrating it, and turning it into a usable product (i.e. actionable information) is a monumental task. Today, this process is highly dependent on well trained analysts and it is expected to remain so for the foreseeable future. Because of the huge amount of raw data that we can produce, analysts can easily be saturated if they try to look at all of it. Unless the system is cued to the collection priorities of the end-user, analyst overload and the endemic stovepiping of the intelligence community can cause critical information and important events to go unnoticed until it is too late.

Information Management

Information management is a perennial problem. Broadcast overload, inefficient message distribution codes, and information missed because the reader is awash in it, are all too common in military operations.[41] With the ability to transmit vastly increased quantities of data, the risk of inundating friendly forces with unessential information is great. To avoid information overload, intelligent information management must be developed. Broadcast filters, search engines, and word recognition will help, but as seen with the Internet and spell checkers, they employ rudimentary techniques that provide narrowly correct answers, but often in the wrong context. The ability of the human mind to intelligently vet, filter, and correlate data must be automated to handle the quantity of data anticipated. The magnitude of this task has been recognized, although it has not been matched with appropriate funding or level of effort. Only $13 million has been appropriated over the next period; a sum which barely scratches the surface of the task at hand.[42] Some progress is being made however. For example the Decision Support System, a component of the Tactical Decision Making Under Stress (TADMUS) program, integrates track data collected by the Aegis combat system into an easy to understand, intuitive display of track history to aid Tactical Action Officers in making target engagement decisions. Decision aids of this type may eventually help collection managers and operational commanders evaluate and integrate all-source data in near-real-time on the battlefield.

40. "ISR Sees Problems Ahead," *Air Force Magazine*, April 98, p. 26
41. Vice Admiral J. O. Tuttle, "C3, An Operational Perspective," in *Science of C2: Coping with Complexity* ed. Stuart E Johnson and Alexander H Levis (Fairfax, VA: AFCEA International Press, 1988), p.3.
42. Capt R Lee USN, DISA, "Telephone Interview," 18 June 1998.

Military IT Security and Vulnerability.

DOD's steadily increasing dependence on a global information environment heightens its vulnerability to a growing number of increasingly sophisticated IT threats. While most reports of successful "hacks" are into unclassified military networks, there are unconfirmed claims of intrusion into classified systems;[43] National Security Agency (NSA) exercises such as "Eligible Receiver" illustrate how hackers might disable military information systems.[44] The wider the net and the greater its connectivity, the greater the risk of compromise. As noted above, there are areas where the IT-21 philosophy weakens security. For example, one of IT-21's most formidable challenges is multilevel security. Ideally, information at all classification levels will be accessible through a common PC, however, because of concerns over the adequacy of current multilevel security software and procedures, NSA may not accredit envisioned systems. If not, IT-21 may have to revert to a system for each security level. Nonetheless, protecting the DII against physical, electronic, and cyber threats is one of DOD's highest priorities. It is moving toward a layered defense with damage limitation in mind[45] with a strategy based on the following areas:

Protection of Systems and Networks. This seeks a layered defense of the DII through trusted operating systems, databases, access controls, and application security. It has a budget of $72 million from FY 1999 to FY 2003. Complementing this, a further $34 million has been allocated over the same period for the development and testing of COTS products.

Intrusion Detection and Monitoring. DOD has programmed $58 million from FY 1999 through FY 2003 to develop advanced attack sensing and warning tools. This will include network intrusion detection systems, virus and malicious code detection, audit reduction, host sensors, integrity verification mechanisms, indications and warning capabilities, and attack sensing and analysis efforts.

Reaction and Recovery. The department programmed $30 million from FY 1999 through FY 2003 to provide continuous cover from computer emergency response teams.[46]

43. George I. Seffiers, "Hackers Claim Heist of Sub-Tracking Software", *Defense News*, 27 April –3 May 1998, p. 4.

44. Bill Gertz, "Computer hackers could disable military," *Washington Times*, 16 April 1998, p. 1.

45. Capt Dan Galik USN. "Defense in Depth: Security for NCW," *CHIPS*, April 1998, pp. 4 – 7.

46. William S. Cohen, Secretary of Defense, *Annual Report to the President and the Congress* 1998, <http://www.dtic.mil/execsec/adr98/msg.html>, 6 March 1998, Chapter1, p. 3.

THE IMPLICATIONS OF NCW FOR UNITED STATES MILITARY OPERATIONS

The irony of the Information Age is that it has given new respectability to uninformed opinion.

Reporter John Lawton at the American Association of Broadcast Journalists

What will the impact of Network Centric Warfare on United States Naval Operations be? Will the integration of information technology with robust communications and new precision weapons enable revolutionary operational concepts? Will NCW change the nature of war?

Objectively, it is impossible to answer any of these questions. There are several major difficulties with evaluating the impact of NCW in the near term. Most of them stem from the fact that the vision itself is not yet sufficiently mature to evaluate. There is currently no agreed-upon lexicon; key terms, including "NCW" itself, mean radically different things to different people. There is no agreement on scope or applicability; some feel that NCW will be applicable to all levels of warfare, others only to the tactical level, and still others feel that the impact of NCW is so radical that it will erase the boundaries between the strategic, operational, and tactical levels of warfare altogether. Finally, it is very difficult to develop measures of effectiveness that allow a cost-benefit analysis on the value of information in terms of lives, dollars, time, and equipment. Until we agree on what we are talking about, develop specific NCW concepts of operations and supporting organizational structures, and field more hardware that is mature enough to test, there will be no objective means to confirm or refute the assertions made on behalf of NCW.

Subjectively, a bit more can be said. While ultimately the results of the smart application of information technology to warfare may be revolutionary, the process of moving from a "platform-centric" to a "network-centric" Navy will be evolutionary. Will the evolutionary process continue to the point where the Navy is no longer recognizable as the same species it is today? Perhaps, but progress will be slow; the impact of NCW on the Navy between now and 2010 is unlikely to be extreme. Why? First, the conceptual difference between NCW and how the Navy has traditionally tried to operate is not as great as has been supposed. Second, technological improvement and systems integration are likely to be slower than anticipated. Third, the overall potential of NCW is probably overstated.

"Platform-Centric" Warfare: Myth or Reality?

The conceptual distance between the Navy's present approach to doing business and that implied in the NCW vision is not as great as it is claimed to be. As noted earlier, much of the technology that will support NCW has been in evolving and improving for decades as the Navy worked to refine its tactics and correct deficiencies in its capability. Link 11 led to Link 16, JOTS to GCCS-M, and New Threat Upgrade Remote Track Launch-on-Search (RT-LOS) to CEC. Precision weapons have likewise evolved slowly, from the laser-guided bombs and radar

guided antiship weapons of the 1970s to the growing family of precision ordnance entering service today. Just as the basic technologies are not new, the key precepts of NCW--the synergy of networked forces, speed of command, delegation of authority, local coordination, and networking of sensor and database information--are not new to the Navy, nor to warfare in general.

Historical Naval Networks

Despite assertions to the contrary, the United States Navy of today does not take a "platform-centric" approach to *operations*, and it has not done so for some time. For example, the Navy's approach to strategic Anti-submarine warfare (ASW) during the Cold War, the Integrated Undersea Surveillance System (IUSS), consisted of a networked collection of fixed sensors, mobile towed arrays, and shore-based processing and fusion stations supported by national space-based assets, maritime patrol aircraft, and submarines--hardly a platform centric approach. On a more fundamental level, the Navy's basic unit of issue, the carrier battle group, is a symbiotic network of sensors, communications, weapons, and other resources designed to provide a specific set of required capabilities to the CINC. While many of the battle group's components are capable of autonomous operations in some mission areas, generally speaking none are expected to depend solely on their indigenous resources. In turn, the battle group is often a node within a larger network. Many of the capabilities of the modern battle group are not contained "within the lifelines" of the ships, submarines, and aircraft that constitute it. Generally, it is supported by a variety of fleet, theater, and national assets to achieve the required overall capability set that is required by the mission.

Composite Warfare Commander

Just as the paradigm of networking forces to create synergy is not fundamentally new, the precepts of delegation of authority, direct local coordination (self-synchronization), individual initiative based on a clear understanding of the commander's intent, and command by negation are not radical departures for those who have operated under the Composite Warfare Commander concept (CWC). CWC, which was developed in the 1970s to deal with the complex and fast paced command and control realities of a modern multithreat war at sea against the Soviets, featured all of the above characteristics. CWC recognized that a modern battle at sea would develop too quickly and be too complex for any single individual to exert positive control throughout. This was particularly true of the air battle, due not only to the speed of the threat but also to the intense jamming expected from the strike force. It was expected that this jamming would significantly degrade the tactical picture and our ability to talk to one another, especially via long-haul communications. To cope with the expected pace and chaos of the air battle, tactics, techniques, and procedures were developed that relied on clearly articulated commander's intent, wide dissemination of standardized procedures, control by negation, and loose coordination directly between elements at the tactical level.

CWC was supported by a "sensor grid" of airborne, shipborne, and occasionally ground-based radar, with support from national queuing sensors, and by an "engagement grid" consisting of a group of platforms connected by Link 11, Link 4A, Link 14 and a variety of voice circuits.

Conceptually, it was network-centric. Could the sensors, weapons, computers, and data links have been more reliable and effective? Absolutely. Could the system integration have been better? Probably. Were there things that could have been done better or differently if the technology had been there? Undoubtedly. Was the total system approach adequate? We never had the misfortune of having to find out.

There is no doubt that gradual maturation of technology has improved the power, efficiency, and effectiveness of United States forces in conventional warfare scenarios, particularly at the tactical level. Precision guided weapons allow a few missiles or aircraft to destroy reliably targets that required hundreds of aircraft and thousands of aircrewmen fifty years ago. CEC, once it becomes operational, will enable us to better defend ourselves against some very difficult airborne threats. Link 16 allows us to maintain a better, more reliable, and more secure tactical picture to better coordinate both defensive and offensive operations. But will the combination of all these incremental improvements lead to a fundamentally different concept of how to approach war between now and 2010? Maybe, but the practical differences are hard to pinpoint.

Rate Of Change And System Integration

While the conceptual gap between "platform-centric" and "network-centric" may not be great as supposed, the cost and technical challenges of integrating our systems into a more coherent network are not trivial. Finances alone will probably dictate the speed at which we can move ahead and in the current fiscally constrained environment, that speed may not be as fast as envisioned. For example, based on current budget plans it will be 2004 before all United States Navy ships are equipped to IT-21 baseline standards, 2005 before IT-21 compliance is reached at critical shore commands, and perhaps as late as 2008 for non critical commands, including such places as the Naval War College.[47]Vice Admiral Cebrowski while serving as N6 stated that he was very uncomfortable with the state of IT-21 funding for shore-based assets, with the FY 00 POM showing an approximately $500 million shortfall in that area.[48]

> CEC Case Study . From an integration standpoint IT-21 compliance is, relatively speaking, straightforward. Other system integration problems will not be as benign. The current teething problems with integrating CEC into the Aegis Baseline 6 and the Advanced Combat Direction System (ACDS) are probably more indicative of the problems that need to be solved in building the NCW architecture. During at-sea testing over the past year there have been severe problems with the Aegis combat system and how it integrates with CEC. The problems have been so serious that CINCLANTFLT refused to allow HUE CITY (CG-66) and VICKSBURG (CG-69) to deploy with the JOHN F. KENNEDY battle group.[49] This decision could not have been made lightly in an era of tight operating schedules and overburdened resources. Correcting the problems

47. Christopher J. Castelli, "NUTWELL: IT-21s Program Fairly Well Off, Despite cuts in POM-00," *Inside the Navy,* 29 June 1998, p. 1.

48. Ibid.

51. Thomas Duffy, "Surface Warfare Officials Agree on Plan to Fix CEC, Aegis Integration Problems," *Inside the Navy,* 20 July 1998, p. 1.

will potentially require a two-year reengineering of Aegis Baseline 6 Phase 1 and the way it integrates with data links and CEC. The fix involves substantial portions of Aegis hardware and software as well as the way in which Aegis, CEC, and data links share information in the combat system.

There are several layers of problems. Integrating the modified software needed to run the COTS hardware into the Aegis Command and Decision Display area has been more challenging than expected. There have been difficulties in the CEC software itself. Finally, there have been difficulties in integrating CEC, Aegis, ACDS, and JTIDS.[50] For example, CEC, Aegis and ACDS use different data transfer rates, which causes problems with contact identification (ID) integrity across the network; track numbers that appear in one place in one system may be elsewhere in another. There have also been problems reported with the interface between identification friend or foe (IFF) and fire control, which can lead to track ID conflicts as well.[51]

RADM George Hutchings, the program executive officer for theater air defense and surface combatants, has recently said, "There are a number of things we're trying to solve; the first is the basic computer program. We have put a lot of COTS into this computer program, particularly in the Command and Decision display areas. That has been more challenging than we figured." At this juncture there is no firm estimate of how much it will cost to integrate CEC or how long it will take.

In order to address quickly the Aegis/CEC problem, the Navy formed a tiger team consisting of officials from the Program Executive Office for Theater Air Defense and Surface Combatants and industry representatives from Lockheed Martin and Raytheon, the manufacturers of CEC and Aegis, respectively. In a 22 June 1998 letter to program managers the panel chair, RADM Paige stated, "the last six months have brought a keen awareness of the scope of the challenge related to interoperability as we move towards highly integrated, networked systems."[52]

Joint System Integration. The point is well taken. Given the Navy's interoperability problems among systems that were designed to perform similar functions, using similar sensor inputs (radar), by a single service (and sometimes a single program office), it would be reasonable to expect even more problems when the network extends into systems designed by other services and, in some cases, for completely different functions. For example, PEO TAD/SC is looking at the feasibility of integrating CEC with the twenty-four satellites of the planned Space Based Infra Red-Low Earth Orbit (SBIRS-Low) constellation. The idea is to use SBIRS-Low as a space based link for extending the CEC footprint out to 1,000 kilometers. This would give the Navy theater wide theater missile defense the discrimination distance it needs for the types of threat missiles

50. Ibid.
51. "U.S. Navy to Test Aegis Upgrade Integration on Cruisers," *Defense News*, 26 July 1998.
52. Roman Schweizer, "Navy Scrambling to Fix Two Cruisers, Aegis -CEC Integration," *Inside the Navy*, 29 Jume 1998, p. 1.

predicted to be operational in the 21st century.[53] Integration of a space based infrared detector with an air and ground based radar network has the potential for some extremely "interesting" issues. Even less ambitious joint integration efforts, like the integration of CEC into AWACS, are likely to be expensive if not perplexing. The Air Force has estimated that adding CEC to the thirty two aircraft of the AWACS fleet will cost approximately $540 million even if everything goes as planned.[54] Linking CEC and Patriot Data Link (PDL) will probably be at least as expensive, if not more. Similar figures for each of the dozens of systems to be tied together to achieve "seamless connectivity" across all warfare areas and levels of command add up to a great deal of money.

There is no reason to believe that integration problems will be limited to United States Navy-designed combat systems. In fact, the evidence points to the contrary. A recently completed command and control exercise run by USACOM showed that even with all the joint communications pieces now available, the warfighting picture may still not come into clear focus. Systems tested included GCCS, JMCIS, the Tactical Combat Operations System (TCOS), and the Contingency Theater Automated Planning System (CTAPS). A number of interoperability issues were noted, including the inability to exchange overlays; vaguely defined and nonstandard geospatial accuracy requirements, which caused positional differences between systems; nonstandard symbology; and an inability to automatically deliver the Air Tasking Order beyond CTAPS.[55]

Interoperability problems are probably not insurmountable, and they are certainly not being neglected, but they can be insidious. In all probability, the more complex the network and its components become, the more difficult (and expensive) these problems will be to detect (in time) and correct. Fixing them will require time, patience, money, and, to quote RADM Paige, "a solid foundation of programmatic and technical data to drive our plans."[56] Ultimately, it may be necessary to curb expectations and ambitions and prioritize our requirements for networking to focus on areas where it really makes a difference. Explicit recognition of this reality can be seen in the statement of General George Krulak, then Commandant, Marine Corps, who flatly asserted that digitization of the battlefield is too expensive for the Marines. Krulak insisted that it is simply not affordable and predicted that the Army will also find it too expensive for units larger than brigades or divisions.[57]

---

53. Christopher J. Castelli, "Four Advanced Descriminator Options Need to be Studied," *Inside the Navy*, p. 29 Jume 1998, p. 5.

54. Thomas Duffy, Navy, "Air Force Agree on CEC/AWACS Plan, Decision Pending Joint Staff Study," *Inside the Navy*, 18 May 1998, p. 3.

55. Thomas Duffy, "Atlantic Command Exercise Reveals Flaws in Joint C2 Concepts," *Inside the Navy*, 25 May 1998, p. 21.

56. Roman Schweizer, "Navy Scrambling to Fix Two Cruisers, Aegis-CEC Integration," *Inside the Navy*, 29 June 1998, p. 1.

57. Paul Mann, "Idle Icon," *Aviation Week & Space Technology*, 25 May 1998, p.19.

NCW Potential

We have discussed how the Navy operates today, and how it is not dissimilar from the way we would like to operate in a network-centric environment. The "speed bumps" likely to be encountered along the way, such as funding shortages and overly ambitious software engineering dreams, have also been addressed. Let us take a look at the absolute potential for NCW if all the components--sensors, communications nets, information data bases, weapons, doctrine, tactics, and an appropriately flexible logistics system--are put in place.

As noted earlier, there is little argument that technology, including information technology, has had an impact on the way we wage war. Modern command and control, collection, and weapon systems have had a tremendous on impact on the efficiency and effectiveness of the military in some scenarios. No doubt at the tactical level the introduction of technologies like CEC and Link 16 will help solve some longstanding combat deficiencies. Likewise, most would agree that technology has plenty of room for improvement in many areas. Target identification, short-duration mobile targets, and battle damage assessment, remain as very challenging problems.

Virtually everyone would also be willing to stipulate that the goals of NCW--a more comprehensive operational picture, better and more timely tactical situation awareness, better interoperability, the ability to act or react as quickly as necessary to thwart enemy options, and the ability to concentrate force (effects) on the targets that really matter--are fundamentally "good things" in war. But, even if we assume for a moment that the ambitious technical and organizational goals implied by NCW proponents are achievable, will they alter the fundamental nature of war? Will having enough information, in the right places, at the right times, change war from an incredibly complex, chaotic, and confusing battle of human wills to a comprehensible mechanistic process? Will we be able to use "dominant battlespace awareness" to apply power with such precision and effect that it will "lock out" all options for the enemy? Can we eliminate uncertainty? In light of the nature of technology and the nature of human beings, it seems unlikely.

> Technological Limits. There are limits to what technology can do, even in the future. Frequently, it will not alert us to enemy intent. It cannot help distinguish between civilians and combatants in such places as Somalia, Vietnam, the Occupied Territories of the Middle East, or Chechnya.[58] It cannot destroy a chemical weapons plant in the middle of a "baby-milk factory" without causing collateral damage. It cannot violate the laws of physics; it cannot see through mountains, buildings, or far into the ocean's depths. This is not to say that technology is without value. It is a key component of the success of the United States military, but it is not perfect. The United States can still be surprised. The nuclear explosions in India, the recent attacks against our embassies in Kenya and Tanzania, and the Somali counterattack against United States solders are somber testaments to this reality. Important information can still be hidden. Eight years after the Gulf War cease fire the exact status of Iraqi weapons of mass destruction is still

58. In Chechnya the Russians resorted to explosive sniffing dogs to try and determine who had been handling weapons or explosives. Russian Army Lessons Learned from the Battle of Grozny.

unknown—although a team of United Nations inspectors and a considerable portion of the United States ISR capability focused on the problem for most of that time.

The Nature of War

There are indeed great changes that are occurring with civilian and military technologies. But our view in the Marine Corps is that these changes will only allow us to improve our capabilities, they will not alter the fundamental nature of war.

LtGeneral Paul K. VanRiper, USMC[59]

War in the future will still be a two-sided contest, with intelligent and dedicated opponents on each side. Neither side is likely to sit still and let the other win. The history of war is replete with examples of action and reaction, move and countermove, technology and counter-technology. It has always been a mistake to underestimate the power of human ingenuity when faced with an intractable dilemma and an incentive to solve it. If we accept that history is still relevant in the information age, we should expect our potential adversaries to look at what we do and how we do it, and then attempt to develop clever and sometimes unexpected counters. For example, there has been considerable reaction to the performance of the United States-led coalition in Desert Storm. During the Gulf War the United States demonstrated the capability of destroying many of Iraq's command and control bunkers and hardened aircraft shelters. Since the end of the war, the Iranians, Libyans and other Middle Easterners have been digging much deeper to survive United States airstrikes in future conflicts. Burying vital facilities can serve as an effective counter to United States superiority in ISR, stealth, and PGMs. While it is often possible to locate these shelters, it can be very difficult to determine who or what is in them, and many of them would be very hard to destroy.[60]

NCW is essentially about information. The power of NCW depends on the collection, processing, and dissemination of actionable information. It relies on an extremely complex network of interoperable subnets and systems working more or less as they are expected to. Large networks are theoretically fairly robust; however, if they contain nodes that are both unique and critical, those nodes can be highly lucrative targets, and a successful attack opens up the entire network to defeat. In the case of NCW a potential adversary might attempt to work against any or all of the three grids (sensor, information, engagement), the connectivity that binds them together, or the information technology that underpins them all.

59. LtGen Paul K. Van Riper, "Information Superiority," *Marine Corps Gazette*, June 1997

60. The harder of these targets are beyond the capabilities of conventional weapons to destroy. Current tactics focus on cutting the power, water, ventilation and blocking the entrances to such facilities; a time and weapons consuming task. Iran is being assisted by the North Koreans who have considerable experience with underground shelters. At present Korea is estimated to have many of their most important airbases, missile production, and nuclear power sites deep underground. "Slipup Spoils Coverage of Missile Test," *Aviation Week and Space Technology*, 3 August 1998, p. 24

Indian' Nuclear Tests Case Study

India's recent success in hiding preparations for nuclear tests from United States ISR assets is representative of a successful attempt to defeat the sensor grid. Prior to the May 1998 tests the Indian government went to great lengths to deny unambiguous information on the upcoming detonations. They reportedly employed a simple deceptive strategy based on avoiding activity during overflight windows and on creating a diversion to attract the attention of United States (and Chinese) resources. They also transferred the test control system underground. Knowledge of United States satellite capabilities was based on common scientific knowledge and on data that the United States had provided to India in 1995 to convince it of the capability of overhead systems to monitor their nuclear program. [61] India may also have used its own INSAT Earth observation satellites to help determine how to avoid detection from space. India apparently charted the path of United States reconnaissance satellites, and scientists and technicians coordinated their preparations to avoid telltale activity at times when it would be vulnerable to detection. In addition, shortly before the scheduled detonation a strategic deception was carried out at a missile test range thousands of miles away. The object was to convince United States intelligence analysts that the Indians were going to conduct a test flight of the Agni intermediate-range ballistic missile; as a result United States assets focused on the missile launch area, not the nuclear site, until it was too late. In the words of an Indian Defense Ministry source, "Astronomy, common sense, and a basic knowledge of the space environment has enabled us to beat the best technology money can buy." [62] [63]

Information Technology (Where No Man Has Gone Before).

> *"The history of IT can be characterized as the overestimation of what can be accomplished immediately and the underestimation of the long term consequences."* [64]
>
> Paul Strassman,

Just as our dependence on overhead sensors has not gone unnoticed, our growing dependence upon and fascination with information technology has been well documented. We should expect potential adversaries to look for ways to exploit it. As noted in a recent RAND study for Project Air Force, there are few if any potential adversaries whose militaries and societal well-being rely as heavily on high-technology information systems as that of the United

61. Frank Gaffney Jr. "The Real failures of Intelligence," *Washington Times*, 19 May 1998, p 21.

62. Rahul Bedi, "Indian Success Casts Doubt Over U.S. Reconaissance, As Nuclear Test Preparations Avoid Detection," *Janes Defense Weekly*, 20 May 98, p. 5.

63. To some extent the failure was also due to the inability to focus resources and analysis on everything at once. Unambiguous warning information that was detected by the systems was either not seen or not recognized by analysts for what it was prior to the tests. Admiral David Jeremiah, appointed by CIA Director George Tenet to head an inquiry into "intelligence failure," said that, "U.S. satellites produce too much information for the overworked and inexperienced analysts." Tom Rhodes, "CIA in Disarray After Nuclear Tests Debacle," <http://www.sunday-times.co.uk/news/pages/tim/98/06/04/timfgnusa03001.html?1944438>, 4 June 98.

64. Paul Strassman, *Information Payoff: The Transformation of Work in the Electronic Age*, New York: Free Press, 1985, p. 199.

States does, and that dependence is growing.[65] It would stand to reason that the United States is therefore more vulnerable to disruption of its information systems than most adversaries would be. Several trends are likely to increase that vulnerability in the near term:

- Movement toward an open architecture information infrastructure. While this is important for the sake of future system interoperability, it means that potential adversaries may also have an easier time interfacing with that technology.

- Movement toward COTS. There is major shift in favor of COTS hardware and software in military information, command and control, and even weapons control systems. This allows the military to take advantage of the advances in commercial-sector information technology without having to finance the parallel development of that technology. Used judiciously, COTS can both save money and improve capabilities. There is a cost, however: a loss of direct control over the manufacture and development of hardware and software involved. It may prove very difficult to assess fully the weaknesses of systems that are based on proprietary hardware and software, which the military did not have a role in developing and does not have a license to examine or alter. Additionally, adversaries can acquire the technology just as easily and could learn just as much (or more) about it.

- The trend toward rapid upgrades. Commercial products change very rapidly, often without notice or documentation. This aggravates the problem of not knowing what one's code is doing and creates a configuration management nightmare. Problems which where fixed in earlier configurations can reappear along with totally new ones in a future release. Nonstandard hardware and interfaces may also prove to greatly complicate the logistics of supplying repair parts. Finally, it may be very difficult to understand what a series of minor changes could do to the performance of the system as a whole.

Many of the problems that have dogged the introduction of a new technology to military operations have been caused by attempts to introduce technology that is not yet mature enough to be either effective or reliable in combat. It is hard to argue that commercial off-the-shelf information software is mature, by any standard. We certainly do not yet fully understand the vulnerability or fragility of these systems. COTS software is the one technological arena in which we have absolutely no technological advantage; our adversaries have access to virtually the same technologies and the same information about them that we do.[66] While the reality of the budget will drive us to use more and more COTS IT, we need to be extremely cautious about how and where we use it in military systems.

65. Glenn Buchan, "Information War and the Air Force: Wave of the Future? Current Fad?" Project Air Force Issue Paper, RAND Corporation, March 1996.

66. In some cases they know far more about it since much of the actual code for programs like NT is written overseas--and U.S. military users are not licensed to even look at it.

The Utility of Speed of Command.

It is extraordinarily difficult to assess the value of speed of command. At the tactical level for systems such as CEC, "speed of command" is both important and achievable, because the rule set is relatively simple to define. Operationally, speed of command is much harder to achieve, because the decision-making process is much more complex; the potential tradeoffs are more subtle and do not lend themselves to a quantitative evaluation or automated processes. For example, how does one automate the choice between a course of action that may be effective but could result in high friendly or neutral casualties, and one that is less effective, but lower in risk to one's own forces? At the strategic level, achieving speed of command becomes even more difficult. While the military may want to move quickly to lock-out enemy options, politicians may be limited by diplomatic or other constraints. Strategic decision making may be measured in days and weeks.[67] Even single changes to rules of engagement may take many hours, despite cavalier abbreviations of the process.[68] In the many cases where the United States enjoys overwhelming force, the military may wish to move as quickly as possible to secure rapid, unconditional surrender. On the other hand, political strategists may wish to move more slowly--to employ a 'shoot-look-shoot' approach in order to retain international respectability.

It also seems that the utility of increased speed of command is greatest if the saving in time is large relative to the speed of implementation of the command. Clearly of value for missile defense, it is less apparent for forces maneuvering on the ground where the radius of action is only tens of miles in a day. Likewise with logistics: the instantaneous reordering of munitions once expended gains one little if the supply train takes two weeks and the buildup prior to the campaign took six months. Clearly, if organic supplies and ready-use ammunition can sustain action, this is not a problem; however, for an operation of any size, logistics is a major limitation. If the operation is prescripted so that the logistics pipeline can be accurately "focused" to the needs of the campaign, there is no room for fog and friction.

Self Synchronization.

Self-synchronization seeks to avoid the loss of combat power that can result from top down command and direction; yet it requires carefully crafted commander's intent and ROE. In fact there are models that dispute the fundamental assumption and show that particular hierarchical architectures have been faster than a fully connected, self-synchronous one.[69] While the network notion may be well suited to naval C2, the land commander operates in a different environment and with different forces, which mean significantly different requirements for C2. A subjective assessment of United States C2 is that command direction is detailed and verbose, consuming all available bandwidth. Other nations with smaller communications pipes tend to issue more succinct orders, delegate more, and encourage initiative. It may be that because of the risk of information overload modern communications may force a return to this style of

67. General H. Norman Schwarzkopf, *It Doesn't Take a Hero,* (New York: Bantam Books, 1992), p. 325.

68. Admiral Sir John Woodward, *One Hundred Days,*(London: Harper Collins, 1992), pp. 156 - 158.

69. Berndt Brehmer, "Distributed Decision Making in Dynamic Environments" in *Proceedings of the 1998 C2 Research and Technology Symposium* (Monterey, CA: Naval postgraduate School, July 1998), pp.590-595.

command, but these benefits would not stem from NCW.[70]

Information Superiority??

Finally, there is the notion of information superiority itself. One of the keystones of NCW and JV 2010 is the assumption/assertion of information superiority, even information dominance. This is probably an invalid and potentially a dangerous assumption. Information dominance is hard to define or measure as an operational objective, particularly in the complex military-political situations that are typical in the post Cold War era.[71] The amount of information each side is able to disseminate is not the key to success; the critical measure of performance is the ability to move that information needed to accomplish the operational objectives of the commander. In light of those objectives, information requirements could be extremely modest. How do United States forces using high-tech sensors, communications, and information systems achieve information dominance against an indigenous, entrenched opposition that can meet most of its needs with means as simple as smoke signals or drums, or carefully selected commercial technology?

The United States experience in Somalia and the Russian experience in Chechnya are both excellent examples. In Somalia the warlords had very simple command and control requirements and had unique means of providing for them. As a result the United States could do very little to prevent them from getting the sorts of information they needed to do their job. In Chechnya the Russians were surprised at the degree to which the Chechens used cell phones, Motorola radios, improvised TV stations, and the Internet to win the information war.[72] In both of these cases, simple command and control requirements and equally straightforward communications methods thwarted a technologically superior force. The knowledge and minimal technology that allowed them to do so was largely taken from the public domain, and it is beyond anyone's ability to control.

CONCLUSIONS

It is not clear that NCW will conceptually revolutionize warfare. However, the programs being pursued under the rubric of network-centric warfare will add to United States military capability. By 2010 the foundation of a network of sensors, C2, and shooters will be in place, a network faster and better than what is presently available and that should help provide an unprecedented standard of situational awareness. However, progress toward NCW will be slower than advertised, and the full vision is not likely to be realized until well after 2010. System integration will be both technologically challenging and expensive, in a time when defense budgets are shrinking.

Even when the NCW architecture is complete, technical limitations can be expected. The

70. Kuhn, Lt Cdr James K, *NCW: the end of Objective Oriented C2*, (Unpublished Research Paper, U.S. Naval War college, Newport, RI: 1998), p. 16.

71. Glenn Buchan, "Information War and the Air Force: Wave of the Future? Current Fad?" Project Air Force Issue Paper, RAND Corporation, March 1996.

72. Russian Army Lessons Learned from the Battle of Grozny.

comprehensive sensor grid will have gaps. ISR will remain fragile in some environments, particularly underground, underwater, and on land against moving targets. Assessment of enemy intent will continue to be a perplexing problem. Inadequate information management is likely to remain a major weakness; prioritization and multilevel security are prickly problems yet to be resolved. Without intelligent filtering, editing, and distribution, huge amounts of information will overload command centers. Great advances in hardware are being made, but much more powerful software than can be affordably compiled is needed to carry forward the vision of NCW.

Speed of command will increase at the tactical level, but shifting the scale to the operational level is exponentially more complex. In addition, operations that unfold with extreme speed may be unattractive to strategists in circumstances that call for a measured approach. Assuming speed of command can be achieved, speed of *implementation* will be a major limitation, particularly for ground forces and bulk logistic supply. "Self-synchronization" if not taken literally, is no more than commander's intent, delegation, and initiative. Unless enormously complex direction covering all eventualities is issued, synchronizing from the bottom up may be counter productive, especially if the networked force is subjected to unequal stress.

To some extent, the dye has been cast. The end of the Cold War and the associated uncertainty about the role of the military have led to major reductions of defense funding. To try to reduce spending without reducing capability, the United States is betting heavily on precision targeting and high-technology weapons that are highly dependent on information superiority However, as illustrated above, information superiority is likely to be difficult to define, hard to obtain, and hotly contested. Terms such as "information dominance" and "total battlespace awareness" need to be used cautiously, and our expectations of what technology can do for us need to be tempered with historical reality. To train and equip forces to expect very nearly perfect information, and then not be able to obtain it will lead to disaster. On the other hand, if we expect war to be chaos and train and equip with that expectation, any information we can obtain will serve as a force multiplier. Colonel T. X. Hammes, in a recent *Proceedings* article, stated the case very eloquently:

> *The information revolution notwithstanding, war will continue to be nasty, brutish, and not subject to business rationale. As professionals, we must recognize the fundamental nature of war, develop concepts for fighting in that environment, and then develop the systems to support our concepts of fighting. The sequence is important. If we base our concept of war on uncertainty and train to deal with fog and friction then perfect knowledge makes us more effective. But if we base our concept of war on perfect knowledge and then cannot attain that perfection in every fight, we will lose."*[73]

73. Col. T.X. Hammes, "War Isn't a Rational Business," U.S. Naval Institute Proceedings, July 1998, p. 25.

PART II - MULTINATIONAL NCW OPERATIONS

COMBINED MILITARY OPERATIONS

One of the key elements in the DOD strategy that cascades from the United States National Security Strategy is "the demonstrated capability to form and lead effective military coalitions."[74] These may be based on formal alliances or ad hoc coalitions. In general, alliances can provide the tightest political and military structures, whereas coalitions enjoy somewhat looser ties. However, allied and coalition operations are similar in that several independent sovereign states combine to pursue a joint cause. The form that this relationship takes will have significant impact on the method of combined operations. Furthermore, the relationship will be dictated principally by the political will of the members rather than by military expedience. Accordingly, the potential impact of NCW on the operation will be subordinate to political requirements. Some member states may offer only political support, like Iceland's participation in NATO. Others may assign military forces where varying elements of command may be either retained nationally or delegated to the operation's C2 structure.

Alliances

The United States is a member of several alliances, whereby signatory states are bound by international treaty to participate in security or defense organizations that obligate military action in collective defense. One such alliance is NATO. For "Article V" operations NATO has an "integrated" C2 structure already established wherein United States forces would operate within and for the allied organization, under the operational command (OPCOM) of the Major NATO Commander (MNC).[75] Interoperability agreements (standardization agreements or STANAGs) seek to ensure equipment compatibility; they are reasonably successful for C3 but less so for some logistical requirements. The final important element of the alliance is training; frequent exercises range from small-scale procedural ones to large-scale freeplay scenarios. With the de facto transformation of NATO into a security organization that conducts non-Article V operations, nations tend to surrender much lesser degrees of command. For example the United Kingdom and France have delegated only tactical control (TACON) of their forces to NATO in the Balkans.[76] Other alliances, such as the Southeast Asia Treaty Organization (SEATO), remain extant but their security organizations have ceased to exist. Accordingly, they have no established C2 structure; any equipment compatibility that exists is a result not of design but of arms sales; and there are no exercise programs.

Partnerships

A lower level of interoperability is typified by the Partnership for Peace (PfP) and by the

74. William S. Cohen, Secretary of Defense, *Annual Report to the President and Congress 1998*, <http;//www.dtic.mil/execsec/adr98/msg.html>, 6 March 1998, Chapter 1, p. 7.

75. Colonel Anthony J. Rice, *C2 in Coalition Warfare*, (Carlisle Barracks, PA: U.S. Army War College, 1996), p. 18.

76. Ibid. The definition of types of command is detailed in the glossary to Joint Pub 3-0, *Doctrine for Joint Operations.*

United States and South American annual UNITAS exercise. Here there is no established C2 structure and almost no equipment compatibility. However, there has been some degree of integrated training.

Coalitions

These are ad hoc arrangements with no established C2 structure, varying degrees of equipment compatibility, and by definition, no long-term prior training. Future coalition operations might draw heavily on alliance infrastructures as seen during the operations against Iraq during 1991. Here the coalition C2 structure was a mix of "parallel" and "lead nation" arrangements, a mix that was driven by the political concerns of the participating nations.[77] Coalition operations are also conceivable wherein C2, interoperability, and expertise must be built from scratch; Because of downsizing of United States forces, in such cases, coalition efficacy may depend on partners pulling their weight. In other scenarios partners may be required only for cosmetic purposes in order to afford the operation a degree of international legitimacy.

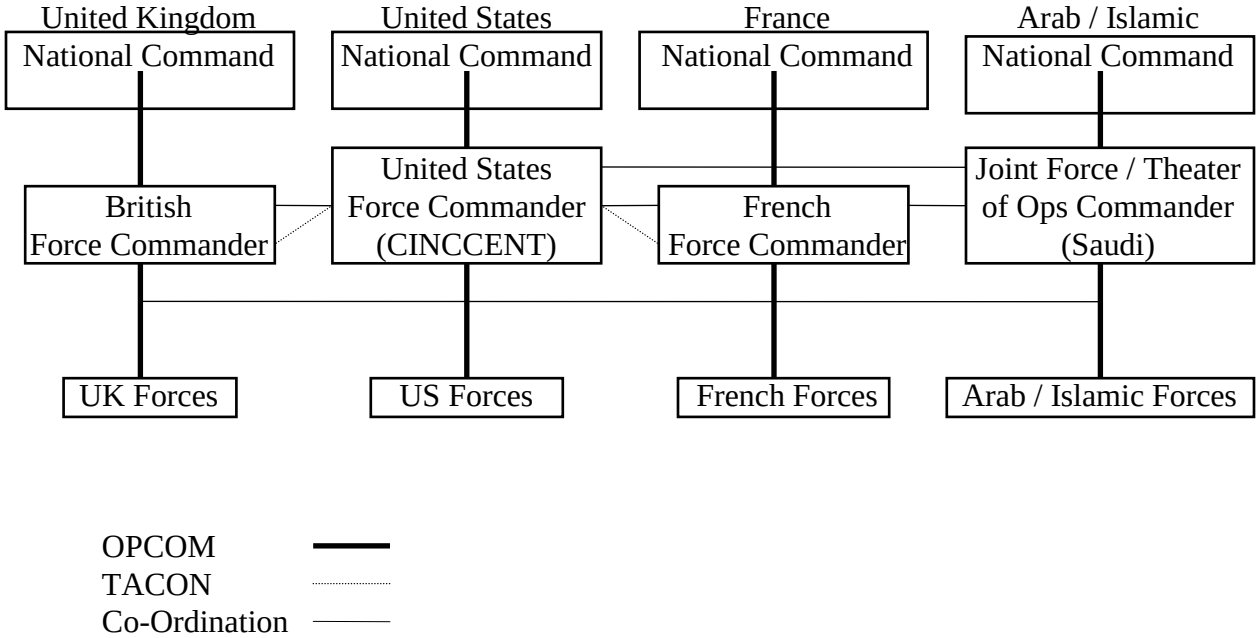

Figure 2 - Desert Storm Coalition Command Relationships

Clearly there can be a multitude of variations, and NCW will impact on each in a slightly different way. To illustrate the spectrum of possibilities compare the more capable members of an alliance (NATO) to an ad-hoc coalition. However, in either case, a multinational operation involving United States forces within the 2010 time frame is very likely to enjoy overwhelming superiority in force. While unity of command will remain important and could produce delegation of OPCOM against a major threat, against a weaker adversary political sensibility will

77. U.S. Department of Defense, *Conduct of the Persian Gulf War: Final Report to Congress*, (Washington, D.C: U.S. DOD, 1992), p. 58.

probably predominate and the United States might only expect TACON of other nations' forces. In short, for high-intensity wars C2 will probably be integrated; a challenging military situation increases the importance of unity of command, and the political will to support it can be expected. With an overwhelming military advantage or for lower-intensity operations, C2 will probably be "parallel" but with the United States as the "lead nation."

C4ISR OPERATIONS

The C4ISR Architecture Working Group identified six inhibitors to efficient multinational C4ISR operations; policy, equipment, information management, technology, culture, and training.[78] Policy and doctrine have not kept pace with technology or with how coalition operations are executed. Defense sales focus on stand-alone equipment, not on an integrated operational capability incorporating C4ISR. Current methods for information management, release criteria, and security labeling are not conducive to multilevel access and dissemination to coalition partners. The increasing pace of technological change in the United States without the adoption of a common standard makes it difficult for coalition partners to keep up and technology has impacts across the whole spectrum of C4ISR. Cultural differences mean different perceptions of purpose, authority, and standing; for example some nations may not accept female commanders. Lastly, combined training is required because it is fundamental to achieving efficient military capability.

All these inhibitors can be addressed, but with differing expectations of success. The degree to which they can be resolved depends on whether the nations are in an alliance or a coalition. Clearly, it is impractical to achieve a high level of interoperability and training with members of an ad hoc coalition not yet even identified. Also, the United States will be wary of supplying technologically advanced equipment to potential partners whose continued alignment is uncertain, like Iran before the fall of the shah. These are also applicable to NCW. The inhibitor most easily addressed is equipment connectivity; the ones that give the greatest difficulty cascade from multinational command relationships.

C4I Equipment Interoperability

Noting the difficulty in quantifying the benefits of improving C4, some nations seem content to rely on a simple architecture with limited capacity, while others surge ahead with vastly increased sophistication and capacity. The United States, as the largest and most capable partner in any future multinational operation, will probably be the "lead nation." It has unilaterally developed its DII with little regard for, or dialogue with, potential partners and has yet to develop a concept of operations for coalition operations in an IT-21 environment.[79] A possible base line for Multinational information exchange is shown at Figure 3.

78. C4ISR Architecture Working Group, White Paper - *Multinational Force C4ISR Operations*, 11 December 1997.

79. Cdr. Jon Greene USN (SACLANT) , *Allied Interoperability Issues,* <http://copernicus.hq.navy.mil/crwg98/briefs/index.html#topWG_IT-21_Greene_v4.ppt>, May 1998.

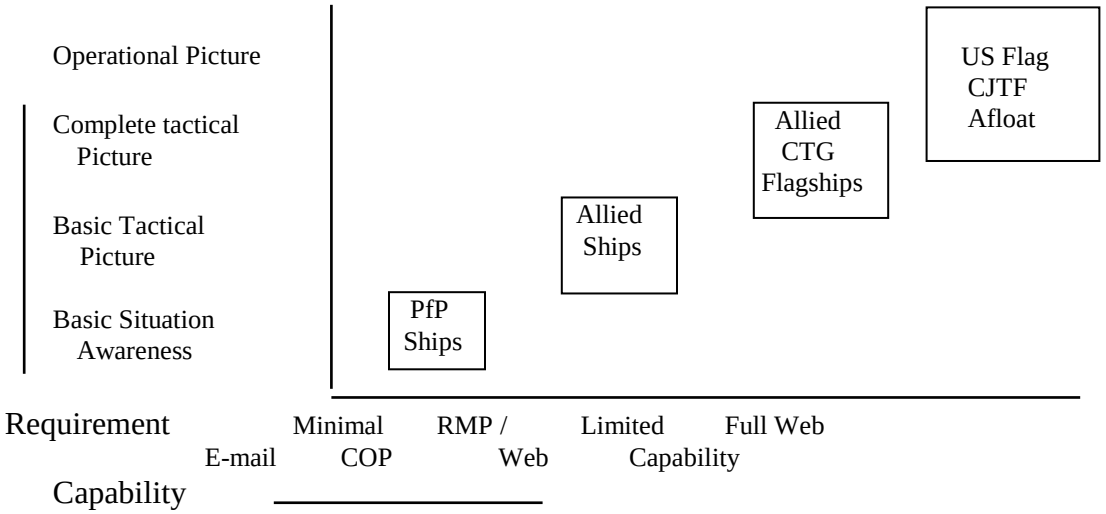

Figure 3 - Multinational Information Exchange[80]

The AIWG. Interoperability is being addressed by a subgroup of the Copernicus Requirements Working Group (CRWG), the Allied Interoperability Working Group (AIWG). The AIWG was quick to point out that without the participation of the United States National Security Agency (NSA), progress on fundamental security issues would be severely hampered. The AIWG identified four main issues: IT-21 connectivity, information exchange, information security and cryptography, and interoperability with legacy systems.[81]

IT-21 Connectivity. The United States will review existing IT-21 plans with a view toward allied interoperability requirements and will investigate the possibility of establishing multifunctional gateways for IP data exchange between nations. Options for implementation of IP will be sought that address a roaming capability to help allied units joining a local U.S. afloat network without a national reach-back requirement. Allied access to the SIPRNET will also be investigated.

Information Release. Changes in technology are incorporated into equipment and operational concepts much more rapidly by the United States than by allies. In contrast, the majority of allies require a concept from which their acquisition process proceeds. Allies accept that they tend to follow U.S. trends and programs, but if they are to respond with interoperable equipment of their own in a timely fashion, early release of U.S. operational concepts is needed.

80. Ibid.

81. Minutes of the CRWG 98 Allied Interoperability Working Group <http://copernicus.hq.navy.mil/crwg98/briefs/alliedwg.doc>, 14 May 1998.

Information Security and Cryptography. Nations will explore with their respective national security agencies the adoption of risk management versus risk avoidance. Risk management is the present United States trend. Restrictions that preclude allied 'over the air' rekeying of crypto, crossdecking equipment and the use of commercial equipment should be reviewed to seek more flexible procedures.

Interoperability with Legacy Systems. The issue of maintaining interoperability with legacy systems is complex, particularly because technological progress varies greatly between nations. While connectivity may be achieved, the basic designs of the systems connected may be incompatible. For example, if the geographic grids in two systems are based on separate reference systems, they might be able to communicate, but the information they display will be inconsistent.

NATO Interoperability

NATO strives to achieve interoperability between the forces of its members. Nevertheless, the vast majority of equipment procurement is under national control, with only some, most notably important headquarters C4 hardware, purchased through NATO infrastructure funding. Notwithstanding the unilateral American procurement strategy for C4I, the Joint Staff has sought to bring NATO along, sponsoring an annual Joint Warrior Interoperability Demonstration (JWID). The objectives for the last exercise in the series, JWID-98, were:

a. To connect GCCS systems to the SHAPE Virtual Command Center (VCC) and MCCIS.

b. To provide an integrated common operational picture (COP) at different levels of command via a single PC.

c. To integrate e-mail and formatted messages

d. To use data labeling (dB and HTML) to segregate data based on different labels, identifying security caveats and levels of sensitivity.

e. To connect LANs to common wide area networks with different classification levels.

f. To connect national systems to VCC.

g. To explore the Windows NT operating system and investigate whether it can provide security features that overcome current concerns.

h. To achieve automatic file translation to HTML.

i. To connect collaborative planning tools and web front ends to the VCC.

Binational Agreements

The United States has bilateral agreements with other countries, for example the United Kingdom, on equipment trials to prove compatibility. Work is in hand on exchanging information in a classified IT environment and achieving interoperability with United States IT-21 and the U.K. Joint Battlespace Digitization (Maritime) programs. Forthcoming trials will aim to achieve interoperability between the SIPRNET / Tactical Internet Protocol Net (TIPNET), and the GCCS-M. [82] Connectivity, to be achieved through firewalls and "mail guards," may enable Web browsing while preventing transmissions not cleared for release. For immediate operational requirements the theater commander could waive security concerns, as occurred during exercise Rim of the Pacific (RIMPAC) 98.[83] However, before the United States and U.K. nets can be connected in the long term, the NSA and GCHQ must accredit the security features of the system.

Ad Hoc Coalitions.

A much more basic degree of connectivity can be achieved with little difficulty. This could be accomplished by transferring cryptographic equipment and operators as is done to the other nations during the South American exercise UNITAS. A more up-to-date method would be to supply PCs connected to the net by IRIDIUM cell phones. [84]

Rules of Engagement (ROE)

ROE serve the political-military purposes of national operations. If OPCOM is delegated to the force commander, then he may expect to use joint ROE. An example is the MNC's ROE system, where all alliance forces under NATO command use the same rules. If anything less is delegated, command is through the national chain, and ROE can be fragmented in the joint force. With different national interpretations on things as basic as self-defense, there is considerable risk that multinational cooperation will be stressed. For example, should one nation's forces take the first hit because the protecting force could not fire? Should escalation occur because an ally shoots first and preempts the overall plan?

The definitions of anticipatory self-defense and hostile intent cause the most difficulty in forming joint ROE.[85] The mechanics for achieving common ROE -- or even common offensive ROE, leaving defensive rules to national authorities -- are readily conceivable.[86] However, the operational requirement is likely to always be subordinate to the political one, and though legal criteria should cascade from international law, nations reserve the right to use their own interpretations. While it would be advantageous to have common ROE, it may be difficult to

82. Cdr M. Jim Dale RN (CNO/N60Q), *US/UK IP NET TRIAL*, 1 July 1998.

83. Gregory Slabodkin, "Navy hosts exercise without coalition WAN," *Government Computer News*, 3 August 1998, p.6.

84. C4ISR Architecture Working Group, "White Paper - Multi National Force C4ISR Operations," 11 December 1997.

85. Eric S. Miller, *Interoperability of Rules of Engagement in Multinational Maritime Operations* (Alexandria, VA: CNA, October 1995), p. 5.

86. Ibid, pp. 19-23.

achieve; in any case, multinational forces will, as a practical matter, deploy with loosely similar ones. Achieving a well defined and universally agreed statement of the coalition's strategic and political war aims might not be possible.[87]

Weapon Control

CEC has not been released to other friendly nations, although the Japanese are trying to acquire it.[88] By 2010 it may be in the United States' national interest to share this technology or it may have been developed elsewhere. If either transpires, it will cause ticklish problems for multinational C2. A unit of one nationality detecting a target may control the engagement of a firing unit of another nationality. Clearly, to optimize the employment of CEC, there should be unity of command so as to allow this; however, this issue will be hostage to the command and ROE arrangements noted above. If OPCOM is delegated there will be less of a problem than if only TACON is offered. In the Cold War scenario, procedures were developed to allow one nation to order the targeting and firing of tactical nuclear weapons, such as depth bombs. Likewise, procedures to smooth over the different release criteria for antisubmarine torpedoes have been evolved. Naval gunfire and close ground support present similar difficulties that have been resolved.

THE IMPLICATIONS OF NCW FOR MULTINATIONAL MILITARY OPERATIONS

The impact of NCW on multinational operations is similar to its implications for U.S. operations, tempered by national considerations. Notwithstanding interoperability and connectivity issues, it is the political shape of the multinational command structure that will likely prevent the utility of NCW from being realized throughout the force. While the United States may draw some benefit from self-synchronization, some nations who operate normally with a greater degree of delegation and top-down direction may not see any difference. The one great advantage that NCW may achieve, if IFF Mode 4 is not available to the multinational force, is a reduction in fratricide, through an improved awareness of friendly dispositions.

CONCLUSIONS

Multinational forces will face the same interoperability problems that face United States forces. Connectivity is achievable with direct system links for the more sophisticated allied nations and simpler stand-alone solutions for members of ad hoc coalitions. The major hurdle with both is the willingness of respective NSAs to authorize multilevel security. While allied nations will overcome doctrinal and equipment differences, the United States is unlikely to transfer this technology to potential coalition partners unless it is certain of their allegiance and stability.

Notwithstanding the ability to communicate at some level, many of the potential benefits of NCW are unlikely to be fully realized in multinational operations for political reasons. In many instances multinational force unity of command will take a back seat to the need to retain a strong national command linkage. Ultimately, scope, the pace, direction, and intensity of the

87. General H. Norman Schwarzkopf, *It Doesn't Take a Hero* (New York: Bantam Books, 1992), p. 386.
88. Frank Wolfe, "Japanese Want CEC, but YEN Problems May Prevent Buy", *Defense Daily*, 16 July 1998.

battle will continue to be determined by the sensibilities of individual national political leaders rather than by speed of command or self-synchronization.

APPENDIX I
THE INTERNET

The Internet links many types of computers by a communication network that offers almost global coverage. [89] It uses standard protocols to enable different types of computers to communicate to each other and sends information in "packets" to make maximum efficiency of the connecting network. The World Wide Web provides a means to access the Internet.

There are three kinds of computers on the Internet. Client computers, often PCs, are the users' means of access. Server computers print, file, mail, process, retrieve, and do various other jobs for clients. Lastly router computers move digital data around the world between clients, via servers. Routers establish what clients and servers are operating and the optimum route to connect them with respect to cost or time. Internet computers are connected by various means. Optical fiber is the best; a loom can carry data thousands of kilometers at billions of bits per second (BPS). However, the most common connection is via telephone circuits using modems at only thousands of BPS. The Internet carries digital data in "packets", strings of bits in standard formats that specify addresses, originator, length, sequence, protocol and check sum, together with message data. The actual functioning Internet is a network of the networks of Internet Service Providers (ISPs), of which there are more than 3,700 in North America alone.

The major Internet protocols are:

a. The Internet Protocol (IP) which specifies the format of data packets.

b. The Routing Information Protocol (RIP) which establishes connectivity and route.

c. The Transmission Control Protocol (TCP), which allows large blocks of information to be broken up into streams of small sequentially numbered packets. TCP controls how these packets are sent, based on the capacities of the sender, receiver, and network.

d. Domain Name System (DNS) protocols are used by name servers to update the easy-to-remember names of networks and computers, like <web.mit.edu>, and to resolve those names when asked into current addresses.

f. The File Transfer Protocol (FTP), which specifies how directories of files are named and moved among client and server computers.

g. Mail Transfer Protocols (MTP), used by clients to send and receive electronic messages (e-mail) through mail servers, which store, copy, distribute, and forward them to their destinations.

The world wide web comprises three protocols:

a. Uniform Resource Locators (URLs), like http://www.company.com/dir/file, a standard

89. Dr Robert Metcalfe, *The Internet*, <http://www.com-web.com/metcalfe.htm>, April 98.

way of specifying a type of web document, the DNS name of the server where it is found, and the location of the document on the server's disk.

b. Hyper-Text Markup Language (HTML), a standard format for web documents that allows them to make references, hyperlinks using URLs, to other web documents.

c. Hyper-Text Transfer Protocol (http) uses DNS to resolve URLs and uses TCP/IP to download HTML documents from servers to client browsing software.

Intranets are internal information systems built using TCP/IP/Web technology for use within an organization. Most Intranets do not use the Internet but private routers, circuits, and servers. This overcomes the lack of security, delay, and down time of the Internet, which is not robust enough for corporate use. If Intranets are connected to the Internet it is through firewalls that limit or sift information transfer. Extranets are applications of TCP/IP/web technologies to corporate information systems for use externally by customers. As these private nets grow, they tend to suffer from same problems that beset the Internet.

INTERNET FRAGILITY

Routing. Routing tables have to be laboriously prepared. They are not dynamic in real time and therefore not robust. In 1996 an ISP crashed, losing Internet access for all 400,000 of its users for thirteen hours. The cause was a typographical error in a routing table that propagated to other routers. By far the word's largest ISP, America Online, lost its routers, denying Internet access to all of its then 6.2 million users for nineteen hours. By contrast, in 1997 a tiny ISP inadvertently created some erroneous routing information that propagated to a larger ISP and then to an even larger one. It eventually infiltrated the Internets' major inter-ISP exchange points (NAPS). Up to 40 percent of the Internet's traffic was lost for up to seven hours. Another issue is that if too many packets show up at a router at about the same time, the ones arriving after its memory is full are discarded. Packets are also discarded if routers become so busy that while attempting to route, they deny message traffic. Packet losses routinely reach 30 percent during busy hours. There are now 50,000 routes in the Internet and routing tables just passed ten megabytes.

Response Time and Priority. The Internet has a huge capacity but when demand is high it slows down significantly. The "stop" button is pressed as patience runs out waiting for downloads at peak times. There is no method of prioritizing e-mail, either by the urgency of its content or the importance of the sender.

Security. The open architecture of, and ease of access to, the Internet do not lend themselves to efficient security. Information passes through each computer in the network. Web browsers can incorporate security features that control entrance of active participants, impose passwords, and certify specific sites, but they have limited efficacy. There is no effective control over content, and users download files at peril of being infected by the latest virus. Reports of hacking outnumber those of detection and prosecution; however those intrusions that have been

discovered give an indication of the breadth and depth to which hackers can infiltrate.[90] There are Web pages devoted to hacking news,[91] and bulletin boards where the latest tools and attacker freeware are posted.[92]

REMEDIAL ACTION

Slow and insufficient servers cause delays. Unfortunately, traffic and Web load are unpredictable. As capability improves, increases in bandwidth are eaten up by new features -- improved graphics, for example. The http 1.0 protocol makes very inefficient use of TCP/IP, opening and closing many TCP connections per Web page. However, http 1.1 is being deployed now and promises substantial improvement, fewer packets, and faster response.

Bandwidth. The capacity of the network will be vastly increased with the use of fiber-optic communication between fixed sites, and further increased by wave division multiplexing. Satellite capacity will increase with the advent of IRIDIUM but this increase will be insignificant compared with the huge capacity of fiber optics. Intelligent data management will also help ease bandwidth limitations, by passing only data that has changed. For example, if passing video, only the pixels that change will be transmitted.

Information Management. The Internet is already awash in content, and too much information is nearly as bad as none at all. Search engines are being developed to help users find what they want, but to date they are very basic tools; discrimination and flexibility are both poor.

90. Pamela Ferdinand, "Argentine Pleads Guilty to Hacking U.S. Networks", *The Washington Post*, May 20 1998, p. 23.

91. Antionline, "How 'mercs and crackers like him break into governmental servers", <http://www.antionline.com/SpecialReports/mercs/how.html>, 21 July 1998.

92. Leslie N Weiner, "statement" *Attack methods and Defense Techniques*, Defense Technology Seminar 1998, MIT Lincoln Laboratory.

Annex A
LIST OF ABBREVIATIONS

ACDS	Advanced Combat Direction System
AI	Artificial Intelligence
AIWG	Allied Interoperability Working Group
ASROC	Anti-Submarine Rocket
ASW	Anti-Submarine Warfare
ATACMS	Army Tactical Missile System
ATM	Asynchronous Transfer Mode
AWACS	Airborne Warning and Control System
BM	Ballistic Missile
BPS	Bits per second
CEC	Co-operative Engagement Capability
CINC	Commander-in-Chief
CINCLANTFLT	Commander-in-Chief Atlantic Fleet
COEA	Cost and Operational Effectiveness Assessment
COP	Common Operational Picture
COTS	Commercial Off The Shelf
CRWG	Copernicus Requirements Working Group
CSS	Command Support System
CTAPS	Contingency Theater Automated Planning System
CWAN	Coalition Wide Area Network
CWC	Composite Warfare Commander
C2	Command and Control
C3	C2 and Communications
C4I	C3, Computers and Intelligence
C4ISR	C4I, Surveillance and Reconnaissance
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DMS	Defense Messaging System
DNS	Domain Name System
DOD	Department of Defense
FTP	File Transfer Protocol
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GCHQ	Government Communications HeadQuarters

HARM	High-speed Anti-Radiation Missile
HTML	Hyper-Text Markup Language
HTTP	Hyper-Text Transfer Protocol
ID	Identification
IFF	Identification Friend or Foe
IP	Internet Protocol
IT	Information Technology
IT-21	Information Technology for the 21st Century
IUSS	Integrated Undersea Surveillance System
IW	Information Warfare
JMCIS	Joint Maritime Command Information System
JOTS	Joint Operational Tactical system
JTIDS	Joint Tactical Information Distribution System
JV2010	Joint Vision 2010
JWID	Joint Warrior Interoperability Demonstration
LAN	Local Area Network
MNC	Major NATO Commander
MTP	Mail Transfer Protocol
NATO	North Atlantic Treaty Organization
NCW	Network-Centric Warfare
NSA	National Security Agency
OODA	Observe Orient Decide Act
OPCOM	Operational Command
OPCON	Operational Control
PC	Personal Computer
PEO TAD/SC	Program Executive Officer, Theater Air Defense & Surface Combatants
PfP	Partnership for Peace
POM	Program Objectives Memorandum
RAT	Radio-Automatic-Teletype
RF	Radio Frequency
RIMPAC	Rim of the Pacific
RIP	Routing Information Protocol
RMA	Revolution in Military Affairs
ROE	Rules of Engagement

SATCOM	Satellite Communications
SBIRS - Low	Space Based Infra Red-Low Earth Orbit
SCI	Secret Compartmented Information
SIPRNET	Secret Internet Protocol Router Network
SLOC	Single Line of Code
SofS	System of Systems
STANAG	Standardization agreements within NATO
TACOM	Tactical Command
TACON	Tactical Control
TADIL	Tactical Digital Information Link
TCOS	Tactical Combat Operations System
TCP	Transfer Control Protocol
UHF	Ultra High Frequency
URL	Uniform Resource Locators
VCC	Virtual Command Center
VCSEL	Vertical Cavity Surface Emitting Lasers
WMD	Weapons of Mass Destruction
www	World Wide Web

Annex B
RESEARCH METHODOLOGY.

In addition to the literature search conducted in support of this paper visits were conducted to the following U.S. Navy and Joint Staff orgainizations. The views presented in this paper do not necessarily reflect those of the individuals interviewed.

Central Intelligence Agency
OPNAV N816
OPNAV N84
OPNAV N6
Joint Staff J 6 OSD
Naval Research Laboratory
Massachuesets Institute of Technology Lincoln Laboratory
John Hopkins Applied Physics Laboratory
Space and Air Warfare Systems Center, San Diego
Naval Warfare Assessment Station, Corona
Naval Post Graduate School
United Kingdom Embassy
Naval Doctrine Command

There were also two Network Centric Warfare workshops held in support of this project. One in Newport and one in Washington, DC at the U.K. Embassy. Attendees included representatives of :

OPNAV N41
OPNAV N513
OPNAV N6
OPNAV N816
OPNAV N816
Naval War College
Office of Naval Intelligence
Central Intelligence Agency
Joint Staff J6
Naval Research Lab
Naval Doctrine Command
Naval Underwater Warfare Center
MIT Lincoln Lab
Applied Physics Lab

Annex C
BIBLIOGRAPHY

Aviation Week & Space Technology (New York; McGraw-Hill).

Brehmer, Berndt. "Distributed Decision Making in Dynamic Environments," *Proceedings of the1998 C2 Research and Technology Symposium.* Monterey, California: Naval Postgraduate School, July 1998.

Buchan, Glenn. *Information War and the Air Force: Wave of the Future? Current Fad?* Project Air Force Issue Paper. RAND Corporation, March 1996.

Cebrowski, Vice Admiral Arthur K. and John J. Garstka, *Network-Centric Warfare: Its Origin and Future*, U.S. Naval Institute *Proceedings*, January 1998.

Cohen, William S, Secretary of Defense, *Annual Report to the President and the Congress 1998.* http://www.dtic.mil/execsec/adr98/msg.html, 6 March 1998.

Report of the Quadrennial Defense Review, May 1997.

Conetta, Carl and Charles Knight. *Dueling with Uncertainty: the New Logic of American Military Planning*. Commonwealth Institute Cambridge, Mass. http://www.comw.org/pda/bullyweb.html,February 1998.

C4ISR Architecture Working Group. White Paper: Multinational Force C4ISR Operations. 11 December 1997.

Dale, Cdr. M. Jim RN (CNO/N60Q). *US/UK IP NET TRIAL*, 1 July 1998.

Dalton, John H, Secretary of the Navy. *Posture Statement*, 1998.

Defense Daily.

Defense News.

Federal Computer Week.

Ferdinand, Pamela. "Argentine Pleads Guilty to Hacking United States Networks.", *The Washington Post*, 20 May 1998.

Galik, Capt. Dan, USN. "Defense in Depth: Security for NCW." *CHIPS*, April 1998

Gansler, Hon. Jacques S. "Statement." United States Congress, House, Committee on National Security, *Overview of the Under Secretary of Defense for Acquisition and Technology*. http://www.acq.osd.mil/ousda/testimonies/hnsc_redraft.html, 26 February 1998.

Gertz, Bill. “Computer Hackers Could Disable Military.” *Washington Times,* 16 April 1998.

Gilder, George, *Metcalfe’s Law and Legacy*. http://www.forbes.com/asap/gilder/telecosm4a.htm, 13 September 1993.

Government Computer News.

Gravell, Captain W. “The Offensive Punch - Network-Centric Fighting.” *Surface Warfare*, March / April 1998.

Hammes, Col. T.X.. “War Isn’t a Rational Business.” Naval Institute *Proceedings*, July 1998)

Inside the Pentagon's *Inside the Navy*.

Jane’s Defense Weekly, 20 May 1998.

Johnson, Stuart E and Alexander H Levis, ed., *Science of C2: Coping with Complexity*, (Fairfax, VA: AFCEA International Press, 1988)

Kuhn, Lt Cdr James K, *NCW: the end of Objective Oriented C2*, (Unpublished Research Paper, United States Naval War college, Newport, RI: 1998)

MacDonald, Cdr D. and Kamradt, H.D. *NCW Workshop 1 Research Memorandum 98-1*, (Newport RI: DSD, USNWC, 1998)

Marine Corps Gazette. June 1997

McDonald, Chris. “The Security Implication of IT-21”, *CHIPS,* April 1998.

Metcalfe, Dr. Robert. *The Internet.* http://www.com-web.com/metcalfe.htm, April 1998.

Miller, Eric S. *Interoperability of ROE in Multinational Maritime Operations*. Alexandria, Va: Center for Naval Analysis, 1995.

Naval Studies Board, National Research Council. *Technology for the USN and MC 2000-2035, Vols. I-IX*. Washington D.C: National Academy Press, 1997.

Nature.

Owens, Admiral William A, *The Emerging System of Systems.* Naval Institute *Proceedings*, May 1995.

Reason, Admiral J. Paul. *Sailing New Seas.* Newport Paper 13. http://www.nwc.navy.mil/press/npapers/.np13toc.htm, 21 April 1998.

Rice, Colonel Anthony J. *C2 in Coalition Warfare.* Carlisle Barracks, Penn.: United States Army War College, 1996.

Schwarzkopf, General H. Norman. *It Doesn't Take a Hero.* New York: Bantam Books, 1992.

Seffiers, George I. "Hackers Claim Heist of Sub-Tracking Software." *Defense News,* 27April – 3 May 1998.

Sessions, Sterling D. and Carl R. Jones. *Interoperability; A Desert Storm Case Study.* Washington D.C.: National Defense University, 1993.

Shalikashvili, General John M. *Joint Vision 2010.* Washington, D.C.: Chairman, Joint Chiefs of Staff, n.d.

Strassman, Paul. *Information Payoff: The Transformation of Work in the Electronic Age.* New York: Free Press, 1985.

New York Times.

Weekly Defense News. (Worldwide).

Thomas, Timothy L. "The Mind Has No Firewall." *Parameters,* Spring 1998.

United States Defense Information Systems Agency, *DSIA Master Plan 6.0.* http://www.disa.mil/diimp/diimp-2.html, 27 June 1997.

Global Combat Support System (GCSS). http://www.disa.mil/line/gcss.html, 28 January 1998.

United States Defense Information Systems Agency (DISA). *C4ISR Model "Federation."* http://www.disa.mil/D8/html/navy-study.html, 22 April 1998.

United States Defense Technical Information Center. *Tactical Digital Information Link* http://www.dtic.mil/doctrine/jel/doddict/data/t/05737.html, 2 June 1998.

United States Department of Defense. *Conduct of the Persian Gulf War: Final Report to Congress*. Washington D.C.: United States GPO, 1992.

United States Department of State. *Treaties in Force.* http://www.acda.gov/state/tifjan97.pdf.

United States CJCS. *Joint Pub 3-0 Doctrine for Joint Operations.* Washington D.C.: CJCS, 1995

United States CJCS. *The Global Command and Control System.* http://spider.osfl.disa.mil/fbsbook/fbsbook.html, 2 June 1998.

United States CNO (N6, Space, IW & C2 Directorate). *Copernicus.* http://copernicus.hq.navy.mil/, May 1998.

United States JCS (J6 The C4 Systems Directorate), *Mission Orientated, Warrior Focused.* http://www.dtic.mil/jcs/j6/j6_old.html, 1 June 1998.

Washington Post.

Weiner, Leslie N. "Statement." *Attack methods and Defense Techniques*. Defense Technology Seminar 1998, MIT Lincoln Laboratory.

Wired.

Woodward, Admiral Sir John. *One Hundred Days.* London: Harper Collins, 1992.

Washington Times. 19 May 1998.